IBM SOA
Policy Gateway Pattern

目次

第 1 章 SOA Policy の概要 1
SOA Policy アーキテクチャー 1
SOA Policy ライフサイクル 5
ポリシー標準 5

第 2 章 パターンの概要 9

第 3 章 IBM SOA Policy Gateway Pattern 入門 11
パターンのダウンロードおよびインストール . . . 12
インストールされたパターンの検証 13
ユーザー・アクセスの構成 15

第 4 章 パターン、パーツ、およびスクリプト・パッケージ 17
パターン 17
SOA Policy Gateway Basic Runtime Sample . . . 18
SOA Policy Gateway Governance Master 20
SOA Policy Gateway Basic Runtime 22
SOA Policy Gateway Advanced Runtime 24
パーツ 27
DB2 Enterprise パーツ 27
DB2 Enterprise HADR Primary パーツ 30
DB2 Enterprise HADR Standby パーツ 34
WSRR スタンドアロン・サーバー・パーツ . . . 36
WSRR デプロイメント・マネージャー・パーツ 38
WSRR カスタム・ノード・パーツ 40
スクリプト・パッケージ 42
スクリプト: SOA Policy Gateway 2.0.0.0 - DataPower Domain 42
スクリプト: SOA Policy Gateway 2.0.0.0 - Promotion 44
スクリプト: SOA Policy Gateway 2.0.0.0 - Sample 46
スクリプト: SOA Policy Gateway 2.0.0.0 - Security 49

第 5 章 IBM SOA Policy Gateway Pattern による作業. 53
パターン構成およびパターン前提条件の計画 . . . 53
IBM SOA Policy Gateway Pattern のための DataPower の構成 55
IBM SOA Policy Gateway Pattern パターンのセキュリティー 55
サンプルのための LDAP の構成 63
パターンのデプロイ 64
SOA Policy Gateway Basic Runtime Sample パターンのデプロイ 65
SOA Policy Gateway Governance Master パターンのデプロイ 66
SOA Policy Gateway Basic Runtime パターンのデプロイ 68
SOA Policy Gateway Advanced Runtime パターンのデプロイ 69
デプロイメントの検証 71
シナリオ: パターンにさらにランタイムを追加する 71
IBM SOA Policy Gateway Pattern の複製とカスタマイズ 72
複数の DataPower ドメインを伴うデプロイ . . . 73
サンプル・アプリケーション 73
サンプルの WSRR 成果物の概要 75
サンプル・テスト・ケースの実行 76
サンプル・アプリケーションの拡張 82
サンプルの追加の学習 86
DataPower サンプル・ドメイン 87

第 6 章 デプロイしたインスタンスを扱う作業 97
デプロイしたインスタンスの管理 97
WSRR への接続 - Business Space 98
WSRR への接続 - サービス・レジストリー・コンソール 99
初回使用時の Business Space の構成 100
パターンのデプロイメント後の構成 101
サンプル・アプリケーションの LDAP の設定変更 101
DataPower 証明書の DN 値の認証 101
LTPA 鍵の変更. 102
WSRR トラストストアからの DataPower 証明書の削除または追加 102
ポリシー適用ポイントの構成 103
SOA Policy Gateway Basic Runtime パターンによる作業 105
SOA Policy Gateway Advanced Runtime パターンによる作業 105
Basic Runtime パターンおよび Advanced Runtime パターンで作成される DataPower オブジェクト 106
サービスの作成およびガバナンス. 107
ポリシー 108
新しいポリシーのオーサリング 114
ポリシーの管理. 115
ポリシーのライフサイクルの管理. 116
サービスに接続されたポリシー 116

第 7 章 トラブルシューティング . . . 117
デプロイメントの問題のトラブルシューティング 117
デプロイされたインスタンスの問題のトラブルシューティング 120
診断情報の収集. 121

第 8 章 保守およびサポート 123
緊急フィックスのカタログへの追加 123
緊急フィックスの適用 124

第 9 章 付録. 125
特記事項 125
プログラミング・インターフェース情報 . . . 127
商標 127
IBM へのコメントの送付 127

第 1 章 SOA Policy の概要

ポリシー管理は、構造化された一貫性のある方法でポリシーを管理する上で、重要な役割を果たします。ポリシーは、あらゆるサービス指向環境において、より良いガバナンスを有効にするために使用できます。サービス指向アーキテクチャー (SOA) プラクティスは、ビジネスで主要なサービスを識別し、そのビジネスの重要なサービスをフォーカスする上で役に立ちます。ポリシーを追加することで制御点が加えられ、ビジネスと情報技術に俊敏性が付与されます。その結果、SOA はより使いやすくなり、プロジェクトに要するコストの削減によりビジネス・ユーザーの効率 (time-to-value) を改善し、SOA ソリューションの採用を促進します。

ポリシーは独立したエレメントであり、各種サービスを含む 1 つ以上のリソースに適用できます。ポリシーおよび関連付けられたメタデータの (特に分散環境における) 割り当ては、さまざまな実施ポイントおよび決定ポイントで行われます。

SOA Policy アーキテクチャー

SOA Policy アーキテクチャーでは、「ポリシー・オーサリング・ポイント (PAP) (Policy Authoring Point (PAP))」「ポリシー実施ポイント (PEP) (Policy Enforcement Point (PEP))」、「ポリシー決定ポイント (PDP) (Policy Decision Point (PDP))」、「ポリシー情報ポイント (PIP) (Policy Information Point (PIP))」、および「ポリシー・モニタリング・ポイント (PMP) (Policy Monitoring Point (PMP))」の相互作用について説明します。このパターンでは、PAP は WSRR を使用して実現され、PEP は WebSphere® DataPower® を使用して実現されます。

基本的なポリシー・アーキテクチャーの編成と、それらのキーポイントの定義は、以下のとおりです。

- **ポリシー・オーサリング・ポイント (Policy Authoring Point)** - ポリシーのオーサリング、ポリシーの管理およびガバナンスと、ポリシーのリソースへの割り当て、および実行時のポリシー結果の管理を行うためのポリシー機能を提供します。ポリシーを格納するためのリポジトリーが含まれます。このパターンでは、WSRR を使用して実現されます。
- **ポリシー実施ポイント (Policy Enforcement Point)** -「ポリシー実施ポイント (Policy Enforcement Point)」は、ミドルウェアで実行される機能ポイントであり、以下を行います。
  - ポリシーを実施します。
  - 実施ポリシーの更新を受け取り、その準備をします (使用するために変換します)。
  - 「ポリシー・モニタリング・ポイント (Policy Monitoring Point)」に対して実施メトリックを提供します。
  - 「ポリシー管理ポイント (Policy Administration Point)」および「ポリシー・モニタリング・ポイント (Policy Monitoring Point)」に対して実施ポリシーの結果と分析を提供します。

– ポリシーが実際に適用され、実施される対象を、ライフサイクル・ステージに応じて変更します。
  - 設計の間は、サービス・レジストリーとリポジトリー自体が実施ポイントになります。
  - 実行時には、通常、サービス・プロバイダーをコンシューマーと結び付ける、基礎となる中間 (ミドルウェア) システムによってポリシーが実施されます。

このパターンでは、このポイントは WebSphere DataPower を使用して実現されます。

- **ポリシー決定ポイント (Policy Decision Point)** -「ポリシー決定ポイント (Policy Decision Point)」は、参加者の要求を、関連するポリシーや規約、および属性に対して評価します。許可、適格性、または妥当性検査の決定を表示し、算出された結果を提供します。
- **ポリシー情報ポイント (Policy Information Point)** -「ポリシー情報ポイント (Policy Information Point)」は、「ポリシー決定ポイント (Policy Decision Point)」に、LDAP 属性情報や、ポリシー決定を行うために評価する必要のある情報を持つデータベースからの結果などの外部情報を提供します。
- **ポリシー・モニタリング・ポイント (Policy Monitoring Point)** - アーキテクチャー全体に対する詳細なポリシー・モニタリング機能を提供する機能コンポーネント。例えば、分散環境におけるポリシーの概要など。以下が含まれます。
  – モニタリング・ポリシーの更新を受け取り、その準備をします (使用するために変換します)。
  – リアルタイム収集と統計分析をキャプチャーして表示します。
  – 「ポリシー実施ポイント (Policy Enforcement Points)」などの各種リアルタイム収集機能によってフィードされたデータを、相関、分析、および視覚化します。
  – ポリシー実施ポイントの分散ネットワークの管理や、これらの実施状況に可視性を提供する管理コンソール。
  – モニタリング・ポリシーの指定に従って、ロギング、測定の集約、および重要なイベントの強調表示を行います。
  – 「ポリシー管理ポイント (Policy Administration Point)」および「ポリシー実施ポイント (Policy Enforcement Point)」にモニタリング・ポリシーの分析を提供します。

  注: このパターンには、モニタリングは含まれません。

コンシューマーとプロバイダーはいずれもミドルウェアと対話し、ミドルウェアはリポジトリーおよび任意のモニタリング・ソフトウェアと対話します。

SOA Policy アーキテクチャーと連動する方法

3 ページの図 1 に SOA Policy のアクション可能パターンのフローを示し、その下に説明を記載します。

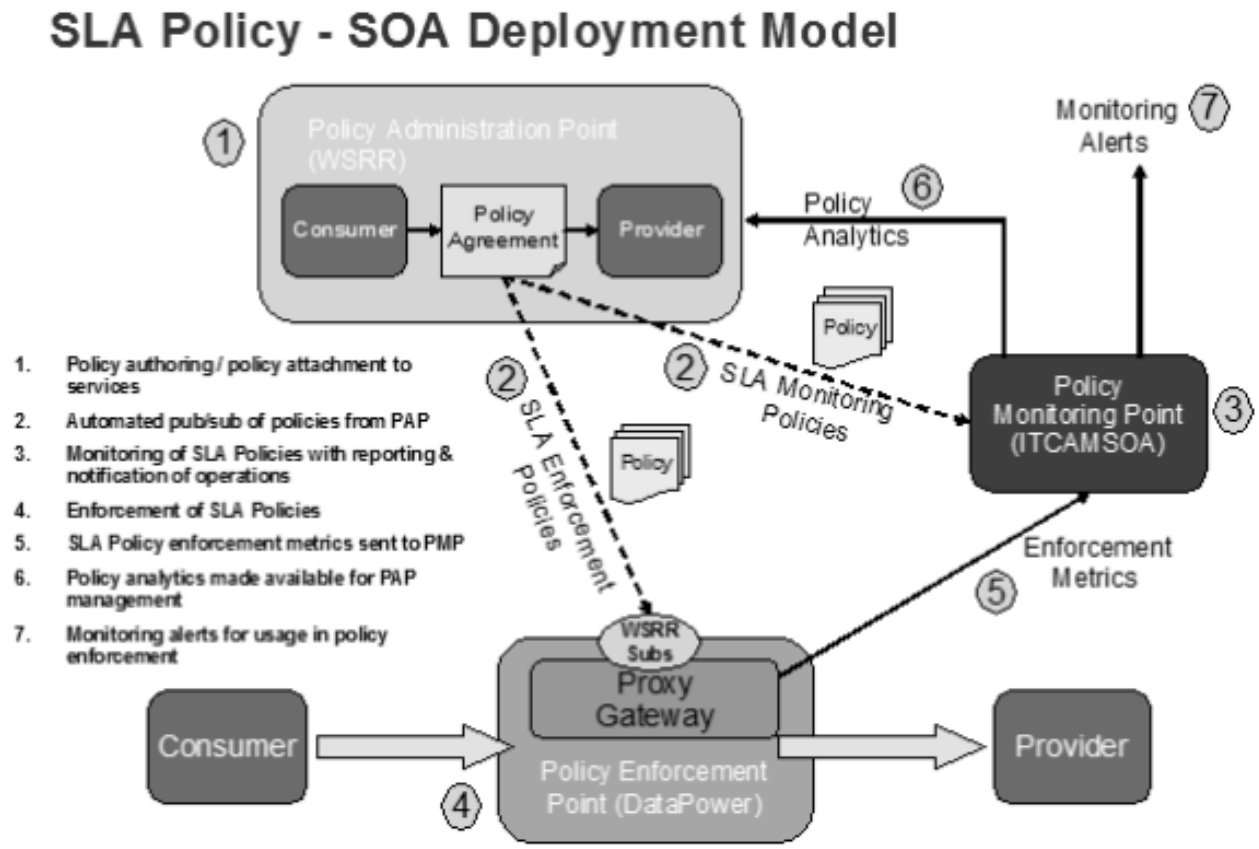


図 1. サービス・レベル・アグリーメント (SLA) ポリシー - SOA デプロイメント・モデル

1. ポリシーがオーサリングされ、そのポリシーを必要とするサービスに添付されます。通常、これは以下の順序で行われます。
   a. サービス・セットがサービス・リポジトリーにロードされるか、作成されます。これは「ポリシー・オーサリング・ポイント (Policy Authoring Point)」の一部です。
   b. 必須のポリシー・セットが、ポリシー・ライフサイクルを使用して「ポリシー・オーサリング・ポイント (Policy Authoring Point)」に作成されます。
      1) ポリシーは、これらのポリシーを必要とするサービスに、必要に応じてサービス、操作、またはエンドポイントのレベルで添付されます。
2. 「ポリシー・オーサリング・ポイント (Policy Authoring Point)」から「ポリシー実施ポイント (Policy Enforcement Points)」および「ポリシー・モニタリング・ポイント (Policy Monitoring Point)」に対する自動化されたポリシーのパブリッシュ/サブスクライブ。

   注: ITCAM for SOA を使用したモニタリングは、このパターンには含まれません。
   a. セットアップの一環として、ITCAM for SOA は WSRR からモニタリング・ポリシーにサブスクライブします。これは 1 回だけ行われます。

b. セットアップの一環として、ポリシーが実施されるサービス・トランザクションがある WebSphere Data Power® アプライアンスごとに、プロキシー・ゲートウェイが作成されます。これは 1 回だけ行われ、必要に応じて追加または変更されます。

c. セットアップの一環として、アプライアンスの各プロキシー・ゲートウェイは、それぞれが担当するサービスの WSRR からポリシーにサブスクライブします。これは 1 回だけ行われ、必要に応じて追加または変更されます。

d. セットアップの一環として、クラスター内の他のアプライアンスとポリシーを共有できるように、WebSphere DataPower が構成されます。これは 1 回だけ行われ、必要に応じて追加または変更されます。

e. ITCAM for SOA は、パブリッシュされたモニタリング・ポリシーをダウンロードします。

f. ITCAM for SOA は、ポリシーをシチュエーション・ポリシーと呼ばれる内部表現に変換します。

g. WebSphere DataPower は、トランザクションを担当するサービスの WSDL をダウンロードします。

h. WebSphere DataPower は、WSRR から通知を受けたときに、担当するサービスのポリシーをダウンロードします。

i. WebSphere DataPower は、ポリシーを SLM オブジェクトの形式で内部 WebSphere DataPower 表現に変換します。

3. 操作のレポート作成および通知による SOA ポリシーのモニタリング:

a. モニタリング・ポリシーは、ITCAM for SOA シチュエーション・ポリシーでアクティブです。

b. ITCAM for SOA は、モニタリング情報を受け取り、その情報をワークスペースに配置します。

注: このパターンでは、モニタリングは提供されません。

4. SOA Policy の実施

a. 実施ポリシーは、各種 WebSphere DataPower アプライアンスでアクティブです。

b. WebSphere DataPower は、サービス・トランザクションを受け取り、そのコンシューマー・サービスとプロバイダー・サービスのポリシーを適用します。

5. 「ポリシー実施ポイント (Policy Enforcement Point)」は、「SOA ポリシー実施 (SOA Policy Enforcement)」の統計を「ポリシー・モニタリング・ポイント (Policy Monitoring Point)」に送信します。

注: このパターンには、モニタリングは含まれません。

6. 「ポリシー・モニタリング・ポイント (Policy Monitoring Point)」は「ポリシー・オーサリング・ポイント (Policy Authoring Point)」にモニタリング・イベントを送信します。

a. イベントは、「ポリシー・モニタリング・ポイント (Policy Monitoring Point)」からモニターされる必要がある「ポリシー・オーサリング・ポイント (Policy Authoring Point)」でセットアップされます。これは 1 回だけ行われ、必要に応じて追加または変更されます。

b. シチュエーション・ポリシーが True に評価されると、イベントは「ポリシー・モニタリング・ポイント (Policy Monitoring Point)」から「ポリシー・オーサリング・ポイント (Policy Authoring Point)」にプッシュされます。

注: このパターンには、モニタリングは含まれません。

7. アラートのモニタリング:
   a. シチュエーション・ポリシーは定期的に実行され、ポリシーの指定に従って操作可能アクションを実行します。デフォルトでは、5 分ごとに実行されます。

SOA Policy ライフサイクル

メディエーション・ポリシーは、SOA Policy ライフサイクルを使用して制御されます。このライフサイクルは、ポリシーが最初に識別されたときから、ポリシーが実動環境にデプロイされて、ポリシーが最終的に不要になって非推奨になるときまでです。

SOA ポリシー・ライフサイクルにおけるライフサイクルの遷移と状態について詳しくは、IBM® WebSphere Service Registry and Repository バージョン 8.0 インフォメーション・センター - SOA ポリシー・ライフサイクルを参照してください。

ポリシー標準

Web テクニカル・コミュニティー・グループである W3C および OASIS は、Web サービスに適用可能なポリシーを定義するための要件を提供する標準を作成してきました。

- **WS-Policy**: Web Services Mediation Policy 1.0 ドメインでは、サービスのメディエーション要件を記述するための一連のポリシー・アサーションが定義されています。
- **Web Services Policy 1.5 - Framework**: Web サービス・ベースのシステムにおけるエンティティーのドメイン固有の機能、要件、および一般的な特性に関するポリシーを表すフレームワークおよびモデルを定義します。

ドメイン固有のポリシー・アサーションを定義する仕様の例は、以下のとおりです。

- WS-MediationPolicy
- WS-SecurityPolicy
- WS-ReliableMessaging および WS-ReliableMessagingPolicy
- WS-SecureConversation
- WS-Security
- WS-Transactions
- WS-Trust

WS-MediationPolicy について詳しくは、ftp://public.dhe.ibm.com/software/solutions/soa/pdfs/WSMediationPolicy1.6-20120124.pdfを参照してください。

WS-Policy データ・モデルには、以下のようなものがあります。

- **ポリシー**: 「ポリシー・オルタナティブ」の順不同のコレクション。
- **ポリシー・オルタナティブ**: 「ポリシー・オルタナティブ」は、「ポリシー・アサーション」の集合です。
- **ポリシー・アサーション**: 個々の設定 (例えば、要件や機能など) を表します。
- **ポリシー・パラメーター**:「ポリシー・アサーション」の不透明なペイロード。
- **ポリシー・サブジェクト**: ポリシー式をバインドできるエンティティー。これは WS-PolicyAttachment 文書で使用されます。

以下の 図 2 の例では、WS-Security および WS-SecurityPolicy で定義されたアサーションを使用したセキュリティー・ポリシーの式を示しています。

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

行 (03-07) は、メッセージ本文に署名するための 1 つのポリシー・オルタナティブを表しています。

行 (08-12) は、メッセージ本文を暗号化するための 2 つ目のポリシー・オルタナティブを表しています。

行 (02-13) は `ExactlyOne` ポリシー演算子を示します。ポリシー演算子は、ポリシー・アサーションをポリシー・オルタナティブにグループ化します。上記のポリシーの正しい解釈は、Web サービスの呼び出しでメッセージ本文に対して署名または暗号化のいずれか一方を行いますが、両方は行わないということです。

図 2. Web Services Policy をセキュリティー・ポリシー・アサーションと共に使用

7 ページの図 3 は、ポリシー定義を示しています。

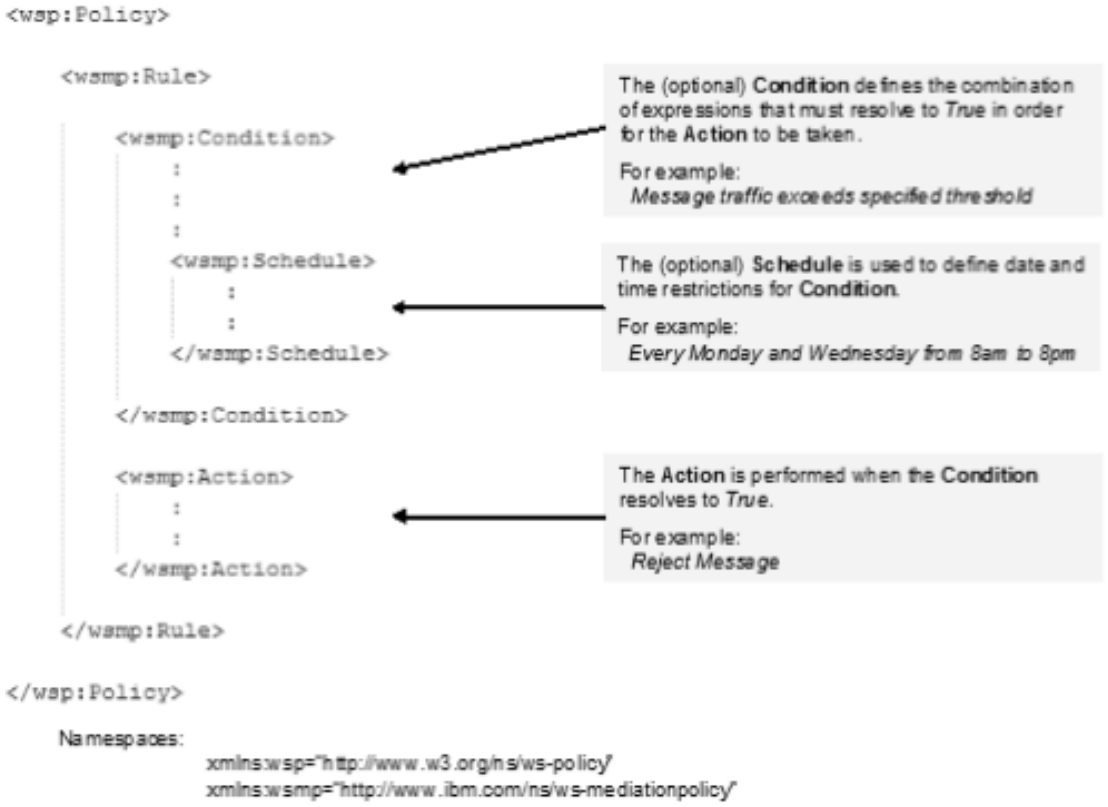


図 3. ポリシー構造の概要

ポリシー添付

ポリシー添付文書の役割は、一連の WS-Policy ポリシー・セットを実施するために、Web サービス添付ポイントなどの特定のサービス添付ポイントに関連付けることです。

例えば、Web サービス・プラットフォームは、以下に基づく添付ポイントをサポートできます。

- WSDL Element URI 1.1 要素
- WS-Addressing 要素

構文は、以下に示すように WS-PolicyAttachment 仕様で定義されています。

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


    </wsp:AppliesTo>
    <wsp:Policy>


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

図 4. WS-PolicyAttachment 仕様

WSRR は、SLA モデルで適切なポリシー添付を獲得するための REST インターフェースを提供します。ポリシーが適用されるコンシューマーとプロバイダーのペア

に関する情報は、WS-PolicyAttachment 形式で ESB に渡されます。構文は、WS-PolicyAttachment: Message Content Filters 仕様で定義されています。

ポリシーは、プロバイダー・サービスに対してのみ指定することも、特定のコンシューマーとプロバイダーのペアや、匿名コンシューマーに対して指定することもできます。匿名コンシューマーによって、他のポリシーが適用されないコンシューマーに対してのみ適用されるデフォルト・ポリシーを定義する方法が提供されます。

7 ページの図 4 で、<wsp:AppliesTo> セクションには、ポリシーが適用されるドメイン固有のポリシー・サブジェクト (プロバイダー) と、それに続けてポリシーを適用するコンシューマー・コンテキスト・フィルター (コンシューマー) が入ります。次に、<wsp:Policy> セクションで、ポリシー (複数可) が宣言または参照されます。

第 2 章 パターンの概要

IBM SOA Policy Gateway Pattern は、ポリシー適用ポイントとポリシー管理ポイントを提供する、仮想システム・パターンのセットです。ポリシー管理ポイントを提供する仮想システム・パターンは、複数層アーキテクチャーで WSRR をプロビジョンして、実動環境とステージング環境を実現します。ポリシー適用ポイントを提供する WebSphere DataPower アプライアンスでは、仮想システム・パターンのデプロイメント時にドメインが作成されます。

ポリシーの例は、多くのサービス指向アーキテクチャー (SOA) 環境にあります。サービスのプロデューサーとコンシューマーは、設計フェーズ中に、サービスの機能、パフォーマンス、および特性について合意します。これを行うために、サービス・レベル定義 (SLD) とサービス・レベル・アグリーメント (SLA) を使用できます。本パターンにより、SLD と SLA のポリシーの定義を、効率的に管理、定義、統制、および活用された仕方で行うことができます。本パターンで使用するポリシー・タイプには、以下のものが含まれます。

- **メディエーション・ポリシー** -
  - 拒否 - 定義したレートを上回るレートで届いた要求を拒否するか、制限します。
  - ロギング - サービスの呼び出し時にポリシー適用ポイントによりログ・メッセージを作成します。
  - 変換。
  - 妥当性検査 - サービス定義に照らして、サービス呼び出しの妥当性検査を行います。
  - ルーティング - メッセージに基づいて、特定のエンドポイントに経路指定します。
- **セキュリティー・ポリシー**: サンプルでは、XACML アクセス制御セキュリティー・ポリシーの適用方法が示されています。現時点で、これらのガバナンスはポリシー管理ポイント内で実施されません。

IBM SOA Policy Gateway Pattern パターンには、以下の仮想システム・パターンが含まれます。

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

これらの 4 つの仮想システム・パターンが組み合わさって機能し、複数ステージのサービス・ガバナンス環境を実現します。また、IBM SOA Policy Gateway Pattern は、パターンのデプロイメント時にガバナンス環境に対して、構成された複数の DataPower ドメインをプロビジョンする機能も提供します。組み合わされて、以下のデプロイメント・トポロジーが提供されています。

- スタンドアロン・デプロイメント

- パイロット・デプロイメント
- フル実動デプロイメント

SOA Policy について詳しくは、 1 ページの『第 1 章 SOA Policy の概要』を参照してください。

デプロイされる仮想システム・パターンは、ITCAM for SOA バージョン 7 によるモニターが組み込まれるように手動で構成することができます。これにより、イベントの基本モニターを実施し、ポリシー・サポートを拡張してモニター・ポリシーを含めることができます。モニター・ポリシーを使用すると、イベント・シチュエーションをポリシー・オーサリング・ポイント (PAP) 内に定義し、サービス定義に添付することが可能になります。こうして、イベント・シチュエーションの発生時にモニターを機能させることができます。

関連概念:

1 ページの『第 1 章 SOA Policy の概要』
ポリシー管理は、構造化された一貫性のある方法でポリシーを管理する上で、重要な役割を果たします。 ポリシーは、あらゆるサービス指向環境において、より良いガバナンスを有効にするために使用できます。 サービス指向アーキテクチャー (SOA) プラクティスは、ビジネスで主要なサービスを識別し、そのビジネスの重要なサービスをフォーカスする上で役に立ちます。 ポリシーを追加することで制御点が加えられ、ビジネスと情報技術に俊敏性が付与されます。 その結果、SOA はより使いやすくなり、プロジェクトに要するコストの削減によりビジネス・ユーザーの効率 (time-to-value) を改善し、SOA ソリューションの採用を促進します。

22 ページの『SOA Policy Gateway Basic Runtime』
SOA Policy Gateway Basic Runtime には、 スタンドアロンとして使用することもデプロイ済み SOA Policy Gateway Governance Master パターンに統合して使用することもできる、 ランタイムを提供するための簡単な手段が備わっています。 SOA Policy Gateway Basic Runtime パターンは、 パターン内でプロビジョンされる WSRR ランタイム・サーバーと通信するように構成された、 DataPower ドメインのデプロイメントをサポートします。

18 ページの『SOA Policy Gateway Basic Runtime Sample』
SOA Policy Gateway Basic Runtime Sample は、SOA Policy Gateway Basic Runtime に、 このリリースで現在サポートされるポリシーを示すサンプル・インターフェースおよびアプリケーションをプロビジョンします。

20 ページの『SOA Policy Gateway Governance Master』
SOA Policy Gateway Governance Master パターンは、 サービスとポリシーのオーサリングおよび管理のための、クラスター化されたガバナンス環境を提供します。 この環境は、WSRR のデフォルトのガバナンス有効化プロファイルが構成されてプロビジョンされます。 デフォルトのガバナンス有効化プロファイルは、ステージングと実動の 2 つのプロモーション・ターゲットをサポートします。

24 ページの『SOA Policy Gateway Advanced Runtime』
SOA Policy Gateway Advanced Runtime には、さらに可用性の高いオプションが含まれており、SOA Policy Gateway Governance Master と共に使用する必要があります。

第 3 章 IBM SOA Policy Gateway Pattern 入門

このパターンでは、WSRR における管理されたポリシーとサービス定義を利用しつつ、WebSphere DataPower を使用してメッセージを制御します。このセクションのトピックを読めば、このシナリオで網羅される範囲、ビジネスでこのシナリオに従うのが良い理由、関係するユーザー・ロール、および本製品で提供される機能の概要を理解できます。

始める前に

IBM IBM SOA Policy Gateway Pattern を IBM PureApplication System または IBM Workload Deployer アプライアンスで使用することができます。

手順

IBM SOA Policy Gateway Pattern を使用するには、以下のステップを実行します。

1. IBM SOA Policy Gateway Pattern をダウンロードし、インストールします。Passport Advantage®からのパッケージのダウンロードについて詳しくは、12 ページの『パターンのダウンロードおよびインストール』を参照してください。
2. オプション: ユーザー・アクセスを構成します。詳しくは、15 ページの『ユーザー・アクセスの構成』を参照してください。
3. パターンを構成し、デプロイします。
   a. WSRR のための、インポートされた仮想システム・イメージのライセンスに同意します。
   b. DB2® Enterprise に関するすべてのご使用条件に同意します。
   c. パターンをデプロイします。
      1) デプロイメント・トポロジーを決めます。詳しくは、IBM WebSphere Service Registry and Repository バージョン 8.0 インフォメーション・センター - デプロイメント・トポロジーを参照してください。
      2) スタンドアロン・デプロイメント・トポロジーを使用する場合は、プロモーションを構成しないで、単一の Basic Runtime パターンをデプロイします。
      3) その他のトポロジーの場合は、最初に SOA Policy Gateway Governance Master パターンをデプロイします。これにより、サービスとポリシーのためのガバナンス環境を備えることができます。
      4) Governance Master パターンが正常にデプロイされた後、必要なランタイム環境のタイプを選択します。テスト環境またはステージング環境の場合は通常、Basic Runtime で十分です。実動環境の場合は、Advanced Runtime 環境を選択します。ランタイムは、Governance Master のガバナンス有効化プロファイルのプロモーション構成で登録できます。プロモーション・オプションには、実動、ステージング、またはプロモーションなし (手動のプロモーション構成用) などがあります。

      詳しくは、64 ページの『パターンのデプロイ』を参照してください。

d. デプロイメントを検査します。 71 ページの『デプロイメントの検証』を参照してください。

e. WSRR 環境をセキュアにします。WSRR のセキュリティーの計画と構成について詳しくは、IBM WebSphere Service Registry and Repository バージョン 8.0 インフォメーション・センターを参照してください。

f. プロビジョンされた DataPower ドメインを構成します。詳しくは、 56 ページの『セキュリティー管理』を参照してください。

4. デプロイしたインスタンスを使用します。詳しくは、 97 ページの『第 6 章 デプロイしたインスタンスを扱う作業』を参照してください。

パターンのダウンロードおよびインストール

IBM Workload Deployer バージョン 3.1.0.2 または IBM PureApplication System で使用する IBM SOA Policy Gateway Pattern は、パスポート・アドバンテージからダウンロードするためにパッケージされています。

始める前に

CI9G9ML.tar.gz ファイルに使用できる 10 GB のスペースと、解凍したファイル用にさらに 10 から 14 GB があることを確認してください。

CI9G9ML.tar.gz ファイルは、Linux または Microsoft Windows を実行しているシステムにダウンロードする必要があります。また、パターンをインストールする前に、Java™ Runtime Environment (JRE) Version 6 をインストールしておく必要もあります。このバージョンの Linux 用は、次のアドレスからダウンロードできます。
http://www.ibm.com/developerworks/java/jdk/linux/download.html。

このタスクについて

IBM SOA Policy Gateway Pattern は CI9G9ML.tar.gz ファイルにパッケージされています。このアーカイブには、Open Virtual Archive (OVA) ファイル、スクリプト・パッケージ・ファイル、およびパターン定義ファイルが含まれています。

手順

IBM SOA Policy Gateway Pattern イメージをパスポート・アドバンテージからダウンロードするには、以下のステップを実行します。

1. 次のパスポート・アドバンテージ Web サイトにアクセスします。パスポート・アドバンテージ。
2. 使用するイメージ、スクリプト・パッケージ、およびパターンが含まれる、アーカイブ・ファイルをダウンロードします。このファイルの名前は CI9G9ML.tar.gz です。
3. Linux 上のターミナル、または Windows 上のコマンド・プロンプト・ウィンドウを開き、CI9G9ML.tar.gz ファイルがダウンロードされたディレクトリーにナビゲートします。
4. CI9G9ML.tar.gz ファイルの内容をローカル・ファイル・システムへ解凍します。Linux では、解凍コマンドは次のとおりです。 Linux では、解凍コマンドは次のとおりです。

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

Windows では、追加でアーカイブ解凍ソフトウェアを使用して、CI9G9ML.tar.gz の内容を解凍します。

5. Linux システムでは、解凍した以下のファイルに実行権限があることを確認してください。
   - chmod a+x installer/installer
   - chmod a+x installer/deployer.cli/bin/deployer
   - chmod a+x installer/deployer.cli/bin/3.1.0.2-20120531075842/deployer
6. 次のように installer ディレクトリーに移動します。

```
cd installer
```

7. IBM SOA Policy Gateway Pattern をクラウド・アプライアンスにインストールするには、インストーラーを実行します。コマンドの名前は、installer.bat (Microsoft Windows の場合) または installer (Linux の場合) です。 次のコマンドを入力します。installer -h *<host>* -u *<username>* -p *<password>* ここで、<host> はクラウド・アプライアンス、username と password はクラウド管理者の資格情報です。以下に例を示します。

```
./installer -h apiliwd.rchland.ibm.com -u cbadmin -p cbadmin
```

8. プロンプトが出されたら、IBM SOA Policy Gateway Pattern のライセンスに同意します。
   a. Microsoft Windows の場合: ご使用条件に同意した後、ターミナルで改行された行に >>> と表示された場合は、quit() と入力して Enter キーを押します。ステップ 7 を繰り返します。
9. パターンがインポートされます。 各パターンがインストールされるたびに、メッセージがインストーラーに表示され、正常にインストールされたことが示されます。以下に例を示します。

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

タスクの結果

パターンとスクリプトがロードされ、仮想システム・パターンが作成されます。

注: IBM SOA Policy Gateway Pattern で使用される適切なバージョンの仮想システム・パターンが既にカタログに存在する場合、それは上書きされません。

次のタスク

IBM Workload Deployer アプライアンスまたは IBM PureApplication System でのライセンスに同意します。

インストールを検証するには、『インストールされたパターンの検証』を参照してください。

インストールされたパターンの検証

パターンが正常にインストールされたことを検証し、パターンの使用に必要なライセンスに同意することができます。

始める前に

12 ページの『パターンのダウンロードおよびインストール』のすべてのステップが完了していることを確認します。

このタスクについて

パターンのインストール後、パターンのインストールを検証できます。仮想イメージを使用する前に、それに必要なライセンスに同意する必要があります。

手順

IBM SOA Policy Gateway Patternのインストールを確認するには、次のステップに従います。

1. パターンがインストールされているホストの IPAS コンソールまたは IWD コンソールにログインします。
2. `Catalog -> Virtual Images` にナビゲートして、DB2 9.7.5.0 と WebSphere Service Registry and Repository 8.0.0.1 を探し、仮想イメージを確認します。ライセンスが同意されない場合は、画像アイコンに十字が付いた赤い四角が付きます。
   a. ライセンスに同意するには、画像をクリックして詳細を表示します。現在の状況が表示されます。ご使用条件に対して「**同意する (accept)**」をクリックして、仮想イメージを使用する前に同意すべきライセンスをクリックします。完了すると、現在の状況が読み取り専用と表示され、ご使用条件が「同意済み (Accepted)」と表示されます。
3. `Catalog -> Script Packages` にナビゲートし、次のものを探します。
   - SOA Policy Gateway 2.0.0.0 - DataPower Domain
   - SOA Policy Gateway 2.0.0.0 - Promotion
   - SOA Policy Gateway 2.0.0.0 - Sample
   - SOA Policy Gateway 2.0.0.0 - Security

   これらのスクリプト・パッケージは、インストールが正常に完了するとすべて存在します。
4. `Patterns -> Virtual Systems` にナビゲートし、次のものを探します。
   - SOA Policy Gateway 2.0.0.0 - Advanced Runtime
   - SOA Policy Gateway 2.0.0.0 - Basic Runtime
   - SOA Policy Gateway 2.0.0.0 - Basic Runtime Sample
   - SOA Policy Gateway 2.0.0.0 - Governance Master

   これらのパターンは、インストールが正常に完了するとすべて存在します。

タスクの結果

これで、IBM SOA Policy Gateway Patternのインストールを確認しました。

次のタスク

正常にインストールされている場合は、53 ページの『第 5 章 IBM SOA Policy Gateway Pattern による作業』に進むことができます。正常にインストールされてい

ない場合は、 12 ページの『パターンのダウンロードおよびインストール』のトピックのステップ 7 以降を繰り返します。

ユーザー・アクセスの構成

ユーザーがアプライアンスのイメージやパターンにアクセスできるようにするには、最初にアプライアンスの管理者がユーザーのアクセスを許可する必要があります。最初にユーザーを作成し、ユーザーをグループに追加することも、最初にグループを作成し、その後ユーザーを作成してグループに追加することもできます。

このタスクについて

管理ユーザー (通常はアプライアンスの管理者) はパターンにアクセスして管理する他のユーザーを追加できます。

手順

ユーザー・アクセスを構成するには、以下の手順を実行します。

1. ユーザーおよびオプションでユーザー・グループを構成するために、次のオプションから 1 つ選択します。
   - インターフェースの「ユーザー (Users)」ウィンドウから、ユーザーを追加して構成します。
     a. メニューから「**システム (System)**」 > 「**ユーザー (Users)**」をクリックします。
     b. 「**追加**」アイコンをクリックします。
     c. ユーザーの実際の名前と短いユーザー名、E メール・アドレス、およびパスワードを指定して、「**OK**」をクリックします。
     d. 「ユーザー (Users)」パネルで追加したユーザーを選択し、アクセス権限を構成します。選択したユーザーのアクセス権限とアクションを構成します。
     e. 「**ユーザー・グループ (User groups)**」フィールドの 1 つ以上のユーザー・グループに、ユーザーを追加します。
   - ユーザー・グループを作成します。
     a. メニューから「**システム (System)**」 > 「**ユーザー・グループ (User Groups)**」をクリックします。
     b. 「**追加**」アイコンをクリックします。グループの名前と説明を入力します。
     c. 「ユーザー・グループ (User Groups)」パネルで、追加したグループを選択し、アクセス権限を構成します。
     d. 「**グループ・メンバー (Group members)**」フィールドにメンバーを追加し、グループに適用する権限を指定します。
2. オプション: 仮想イメージを既に追加している場合は、ユーザーまたはグループの仮想イメージへのアクセス権限を指定します。メニューから「**カタログ (Catalog)**」 > 「**仮想イメージ (Virtual images)**」をクリックして、「仮想イメー

ジ (Virtual Images)」ウィンドウを開きます。左側のパネルから、IBM SOA Policy Gateway Pattern 仮想イメージを選択して、右側のパネルにユーザーまたはグループを追加します。

次のタスク

仮想イメージをまだ追加していない場合は、追加してユーザーまたはグループのアクセス権限を指定します。

関連情報:

IBM PureApplication System: ユーザーとグループの管理

IBM Workload Deployer: ユーザーとグループの管理

第 4 章 パターン、パーツ、およびスクリプト・パッケージ

IBM SOA Policy Gateway Pattern パーツは、パターンの機能コンポーネントです。各パーツは 1 つの仮想マシンを表します。パターンとは、反復可能なデプロイメント用のトポロジーを定義したものであり、共有することができます。

パターンは、仮想システム内の各仮想マシンが提供する機能を示します。各機能はパターンのパーツとして識別されます。パターンは、関連付けられたパーツの特性を持つようになります。例えば、WSRR パーツがパターンに追加され、それがデプロイされると、その結果、WSRR インスタンスが稼働する仮想マシンが作成されます。

パーツ

パーツは、仮想マシン上で構成されるコンポーネントを示します。各パーツには一連のプロパティー (パラメーター) があり、これらはデプロイメント時に仮想システムの全体的な構成を定義するのに役立ちます。 IBM SOA Policy Gateway Pattern のイメージを IBM Workload Deployer にロードする際に、パーツが組み込まれます。

パターン

IBM SOA Policy Gateway Pattern パターンには、以下の 4 つのパターンが含まれます。

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

IBM Workload Deployer を使用して既存のパターンにアクセスしたりカスタム・パターンを作成したりする方法について詳しくは、 http://publib.boulder.ibm.com/infocenter/worlodep/v3r0m0/topic/com.ibm.worlodep.doc/welcome.htmlを参照してください。

パターン

仮想イメージが IBM Workload Deployer または IBM PureApplication System にロードされ、適切なアクセス権限がユーザーに割り当てられた場合、ユーザーは画像のパターンの処理を開始できます。

パターンは、クラウドにデプロイ可能な反復トポロジーを提供します。 デプロイされたパターンはクラウドで実行される仮想システムです。パターンには、事前定義されたものでも作成されたものでも、パーツが含まれます。いくつかのパーツは、仮想システムとしてクラウドにデプロイされる際にパターンが機能するために必要です。

SOA Policy Gateway Basic Runtime

SOA Policy Gateway Basic Runtime には、以下の必須パーツが含まれます。

- DB2 Enterprise
- WSRR スタンドアロン・サーバー

SOA Policy Gateway Basic Runtime Sample

SOA Policy Gateway Basic Runtime Sample には、以下の必須パーツが含まれます。

- DB2 Enterprise
- WSRR スタンドアロン・サーバー

SOA Policy Gateway Advanced Runtime

SOA Policy Gateway Advanced Runtime には、以下の必須パーツが含まれます。

- WSRR デプロイメント・マネージャー
- DB2 Enterprise HADR Primary
- DB2 Enterprise HADR Standby
- WSRR カスタム・ノード

SOA Policy Gateway Governance Master

SOA Policy Gateway Governance Master には、以下の必須パーツが含まれます。

- WSRR デプロイメント・マネージャー
- DB2 Enterprise HADR Primary
- DB2 Enterprise HADR Standby
- WSRR カスタム・ノード

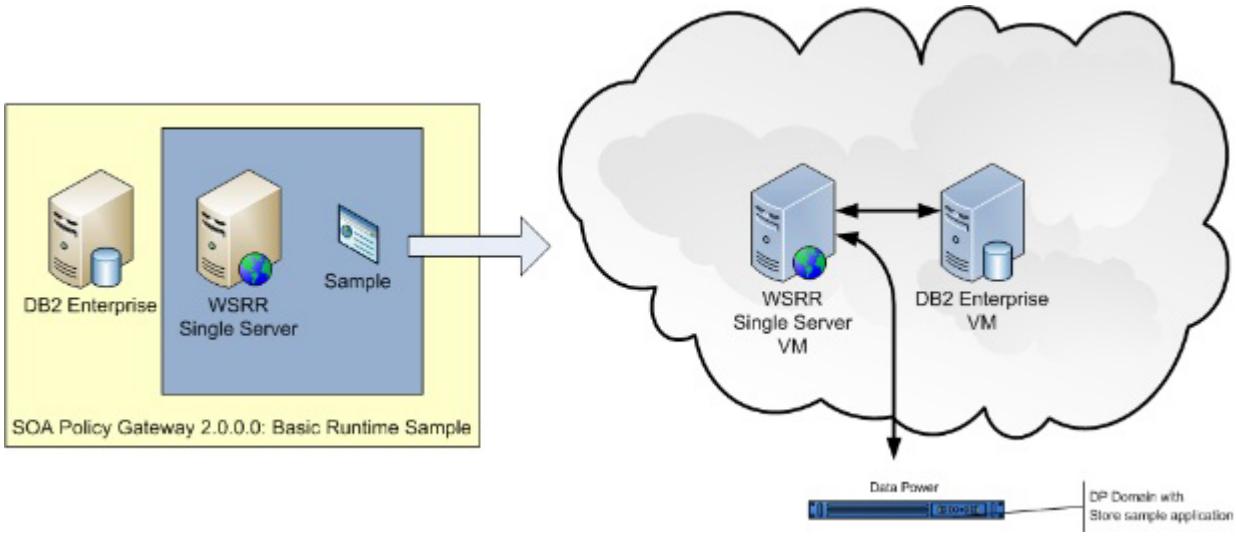
SOA Policy Gateway Basic Runtime Sample

SOA Policy Gateway Basic Runtime Sample は、SOA Policy Gateway Basic Runtime に、このリリースで現在サポートされるポリシーを示すサンプル・インターフェースおよびアプリケーションをプロビジョンします。

SOA Policy Gateway Basic Runtime Sample パターンには、以下のパーツが必要です。

- WSRR スタンドアロン・サーバー
- DB2 Enterprise

SOA Policy Gateway Basic Runtime Sample パターンは、デプロイメント環境にサンプル・アプリケーションをインストールします。これは、単純なサービスを実装し、サンプル WSDL および接続されたポリシーをサービスの WSRR にインストールし、実施されたポリシーをデモンストレーションするテスト・アプリケーションを提供する DataPower 内にサンプル・ドメインをインストールします。サンプル・アプリケーションについて詳しくは、73 ページの『サンプル・アプリケーション』を参照してください。これは DataPower 内にサンプル・ドメインをインストールし、WSRR 内にサンプルの WSDL とポリシーをインストールし、サービスに対する複数のポリシーを例示します。



実装されたポリシーには以下のものがあります。

表 1. Sample パターンのある Basic Runtime に含まれるポリシー

ポリシー・タイプ	説明
ロギング	要求コンテキスト ID に基づいて、要求を DataPower のログに記録します。
ルーティング	要求コンテキスト ID に基づいて、要求を指定のエンドポイントに経路指定します。
妥当性検査	要求をサービス実装 WSDL に照らして妥当性検査を行います。
拒否	アクション (拒否、キュー、その他) によるメッセージのカウントに基づいて、サービスへの要求を制御します。
セキュリティー AAA	XACML ベースのユーザー許可を使用してサービスへのアクセスを制御します。XACML は WSRR に保管されていません。
セキュリティーの編集	応答メッセージの一部を XACML に基づいて編集します。 XACML は WSRR に保管されていません。

スクリプトおよび拡張オプション

SOA Policy Gateway Basic Runtime パターンには、以下のスクリプトが必要です。

WSRR スタンドアロン・サーバー・パーツで:

- SOA Policy Gateway 2.0.0.0 - Sample

パーツとスクリプトのパラメーターを参照してください。

- 29 ページの『SOA Policy Gateway Basic Runtime Sample パターンの DB2 Enterprise パーツ構成パラメーター』
- 38 ページの『SOA Policy Gateway Basic Runtime Sample パターンの WSRR スタンドアロン・サーバー・パーツ構成パラメーター』
- 48 ページの『SOA Policy Gateway 2.0.0.0 - SOA Policy Gateway Basic Runtime Sample パターンのサンプル・スクリプト構成パラメーター』

関連概念:

27 ページの『DB2 Enterprise パーツ』
DB2 Enterprise パーツはいくつかの構成オプションを提供します。

36 ページの『WSRR スタンドアロン・サーバー・パーツ』
WSRR スタンドアロン・サーバー・パーツは幾つかの構成オプションを提供します。

46 ページの『スクリプト: SOA Policy Gateway 2.0.0.0 - Sample』
Sample スクリプトは、SOA Policy Gateway Basic Runtime Sample パターンと共に使用する、サンプル・アプリケーション・パラメーターを構成します。

73 ページの『サンプル・アプリケーション』
サンプル・アプリケーションは、構成可能な DataPower ドメインと、パターンの機能をデモンストレーションするために使用できる一連の WSRR 成果物です。

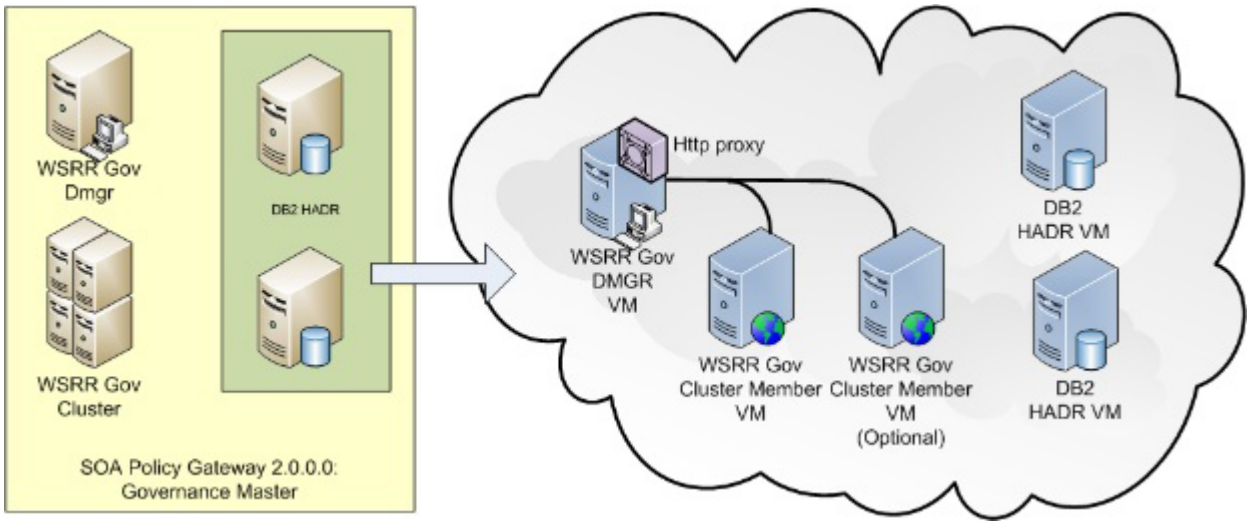
SOA Policy Gateway Governance Master

SOA Policy Gateway Governance Master パターンは、サービスとポリシーのオーサリングおよび管理のための、クラスター化されたガバナンス環境を提供します。この環境は、WSRR のデフォルトのガバナンス有効化プロファイルが構成されてプロビジョンされます。デフォルトのガバナンス有効化プロファイルは、ステージングと実動の 2 つのプロモーション・ターゲットをサポートします。

SOA Policy Gateway Governance Master パターンには、以下のパーツが必要です。

- DB2 HADR Primary
- DB2 HADR Standby
- WSRR デプロイメント・マネージャー
- WSRR カスタム・ノード

注: ランタイム・パターンをデプロイする前に、Governance Master パターンがデプロイされている必要があります。 Governance Master パターンの構成に使用されるパラメーターは、ランタイム・パターンがそれ自体を Governance Master で構成するために使用されます。 Governance Master へと構成できるのは、SOA Policy Gateway Basic Runtime パターンまたは SOA Policy Gateway Advanced Runtime だけです。



スクリプトおよび拡張オプション

SOA Policy Gateway Governance Master パターンには、以下のスクリプトが必要です。

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

パーツとスクリプトのパラメーターを参照してください。

- 32 ページの『SOA Policy Gateway Governance Master パターンの DB2 Enterprise HADR Primary パーツ構成パラメーター』
- 35 ページの『SOA Policy Gateway Governance Master パターンの DB2 Enterprise HADR Standby パーツ構成パラメーター』
- 39 ページの『SOA Policy Gateway Governance Master パターンの WSRR デプロイメント・マネージャー・パーツ構成パラメーター』
- 41 ページの『SOA Policy Gateway Governance Master パターンの WSRR カスタム・ノード・パーツ構成パラメーター』

Governance パターンを Governance Master として使用する

SOA Policy Gateway Governance Master パターンは、ステージングと実動の 2 つのプロモーション・ステージを含む、デフォルトの WSRR のガバナンス有効化プロファイルと共にデプロイされます。 WSRR 内のガバナンス有効化プロファイルについて詳しくは、IBM WebSphere Service Registry and Repository バージョン 8.0 インフォメーション・センター - ガバナンス有効化プロファイルを参照してください。SOA Policy Gateway Basic Runtime および SOA Policy Gateway Advanced Runtime パターンは、プロモーション・ターゲットとしてこの統合にデプロイすることができます。これを構成する方法について詳しくは、71 ページの『シナリオ: パターンにさらにランタイムを追加する』を参照してください。

関連概念:

30 ページの『DB2 Enterprise HADR Primary パーツ』
DB2 Enterprise HADR Primary パーツはいくつかの構成オプションを提供します。

34 ページの『DB2 Enterprise HADR Standby パーツ』
DB2 Enterprise HADR Standby パーツはいくつかの構成オプションを提供します。

38 ページの『WSRR デプロイメント・マネージャー・パーツ』
WSRR デプロイメント・マネージャー・パーツは、いくつかの構成オプションを提供します。

40 ページの『WSRR カスタム・ノード・パーツ』
WSRR カスタム・ノード・パーツは、いくつかの構成オプションを提供します。

関連情報:

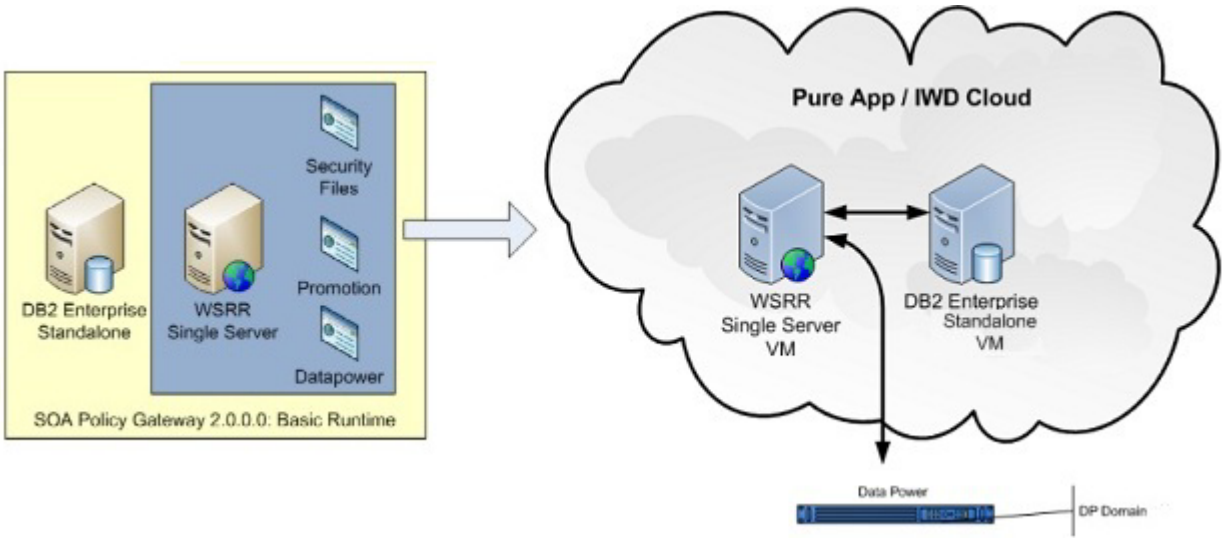
IBM WebSphere Service Registry and Repository バージョン 8.0 インフォメーション・センター - ガバナンス有効化プロファイル

SOA Policy Gateway Basic Runtime

SOA Policy Gateway Basic Runtime には、スタンドアロンとして使用することもデプロイ済み SOA Policy Gateway Governance Master パターンに統合して使用することもできる、ランタイムを提供するための簡単な手段が備わっています。 SOA Policy Gateway Basic Runtime パターンは、パターン内でプロビジョンされる WSRR ランタイム・サーバーと通信するように構成された、 DataPower ドメインのデプロイメントをサポートします。

SOA Policy Gateway Basic Runtime パターンには、以下のパーツが必要です。

- WSRR スタンドアロン・サーバー
- DB2 Enterprise



スクリプトおよび拡張オプション

SOA Policy Gateway Basic Runtime パターンには、以下のスクリプトが必要です。

WSRR スタンドアロン・サーバー・パーツで:

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

パーツとスクリプトのパラメーターを参照してください。

- 37 ページの『SOA Policy Gateway Basic Runtime パターンの WSRR スタンドアロン・サーバー・パーツ構成パラメーター』
- 28 ページの『SOA Policy Gateway Basic Runtime パターンの DB2 Enterprise パーツ構成パラメーター』
- 50 ページの『SOA Policy Gateway 2.0.0.0 - SOA Policy Gateway Basic Runtime パターンのセキュリティー・スクリプト構成パラメーター』
- 45 ページの『SOA Policy Gateway 2.0.0.0 - SOA Policy Gateway Basic Runtime パターンのプロモーション・スクリプト構成パラメーター』
- 43 ページの『SOA Policy Gateway 2.0.0.0 - SOA Policy Gateway Basic Runtime パターンの DataPower Domain スクリプト構成パラメーター』

SOA Policy Gateway Basic Runtime を Governance Runtime にプロモートする

Basic Runtime パターンが Governance Master パターンと共に構成されると、以下が行われます。

- セルをまたぐセキュリティーが構成される。
- Governance Master の `promotion.xml` ファイルが、Basic Runtime デプロイメントのデプロイメント・データによって更新される。

プロモーションを構成するには、以下のいずれかのステージ・オプションを選択する必要があります。

- 実動
- ステージング
- その他、または「Unset」

これらのオプションは、WSRR 内のガバナンス有効化プロファイルによって提供されるレベルに調整されます。ガバナンス・プロファイルが異なる場合、Governance Master ガバナンス・プロファイルが変更されると「その他 (other)」が選択されます。 WSRR 内のガバナンス有効化プロファイルについて詳しくは、IBM WebSphere Service Registry and Repository バージョン 8.0 インフォメーション・センター - ガバナンス有効化プロファイルを参照してください。

関連概念:

73 ページの『サンプル・アプリケーション』
サンプル・アプリケーションは、構成可能な DataPower ドメインと、パターンの機能をデモンストレーションするために使用できる一連の WSRR 成果物です。

27 ページの『DB2 Enterprise パーツ』
DB2 Enterprise パーツはいくつかの構成オプションを提供します。

36 ページの『WSRR スタンドアロン・サーバー・パーツ』
WSRR スタンドアロン・サーバー・パーツは幾つかの構成オプションを提供します。

49 ページの『スクリプト: SOA Policy Gateway 2.0.0.0 - Security』
Security スクリプトは、DataPower アプライアンスとの通信に必要な ZIP ファイルに含まれるセキュリティー情報を、 Linux セキュア・コピー・プログラム (SCP) をサポートする外部ファイル・サーバーから Dmgr または WSRR マシンにコピーします。

44 ページの『スクリプト: SOA Policy Gateway 2.0.0.0 - Promotion』
Promotion スクリプトにより、SOA Policy Gateway Basic Runtime または SOA Policy Gateway Advanced Runtime パターンを、 事前デプロイされた SOA Policy Gateway Governance Master パターンに統合できます。 これは Runtime および Governance パターンの間にセルをまたぐセキュリティーを確立し、同時にオプションで、WSRR プロモーションをガバナンス・マスター内に構成します。

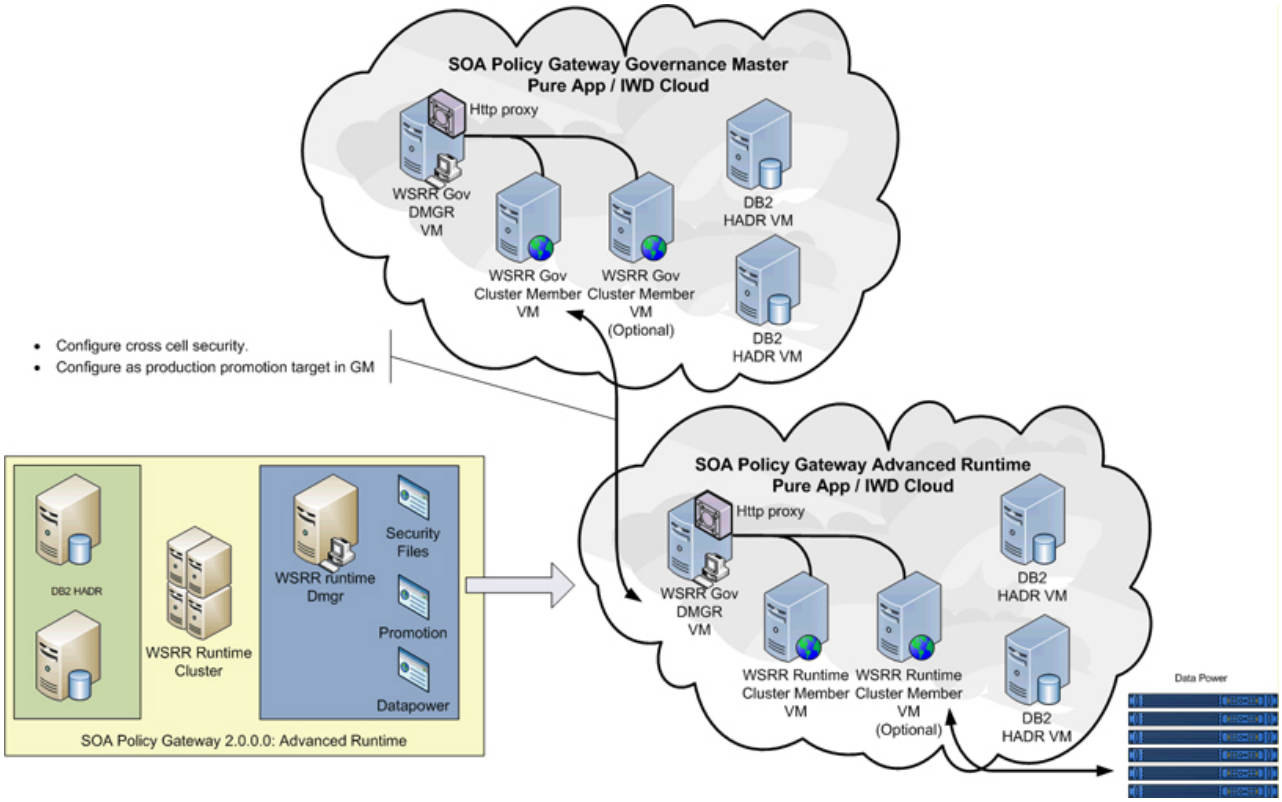
42 ページの『スクリプト: SOA Policy Gateway 2.0.0.0 - DataPower Domain』
DataPower Domain スクリプトは、デプロイメントの際に DataPower ドメインをプロビジョンします。 スクリプトは、単一の DataPower ドメインと WSRR ランタイムとの間の接続を構成します。 WSRR ランタイムに接続される DataPower ドメインごとに、 別個の DataPower Domain スクリプトが必要になります。

SOA Policy Gateway Advanced Runtime

SOA Policy Gateway Advanced Runtime には、さらに可用性の高いオプションが含まれており、SOA Policy Gateway Governance Master と共に使用する必要があります。

SOA Policy Gateway Advanced Runtime パターンには、以下のパーツが必要です。

- DB2 HADR Primary
- DB2 HADR Standby
- WSRR デプロイメント・マネージャー
- WSRR カスタム・ノード



スクリプトおよび拡張オプション

SOA Policy Gateway Governance Master パターンの WSRR デプロイメント・マネージャー・パーツには、以下のスクリプトが必要です。

- SOA Policy Gateway 2.0.0.0 - Security
- SOA Policy Gateway 2.0.0.0 - Promotion
- SOA Policy Gateway 2.0.0.0 - DataPower Domain (DataPower ドメインごとに 1 つ)

パーツとスクリプトのパラメーターを参照してください。

- 31 ページの『SOA Policy Gateway Advanced Runtime パターンの DB2 Enterprise HADR Primary パーツ構成パラメーター』
- 34 ページの『SOA Policy Gateway Advanced Runtime パターンの DB2 Enterprise HADR Standby パーツ構成パラメーター』
- 39 ページの『SOA Policy Gateway Advanced Runtime パターンの WSRR デプロイメント・マネージャー・パーツ構成パラメーター』
- 41 ページの『SOA Policy Gateway Advanced Runtime パターンの WSRR カスタム・ノード・パーツ構成パラメーター』
- 51 ページの『SOA Policy Gateway 2.0.0.0 - SOA Policy Gateway Advanced Runtime パターンのセキュリティー・スクリプト構成パラメーター』
- 46 ページの『SOA Policy Gateway 2.0.0.0 - SOA Policy Gateway Advanced Runtime パターンのプロモーション・スクリプト構成パラメーター』
- 44 ページの『SOA Policy Gateway 2.0.0.0 - SOA Policy Gateway Advanced Runtime パターンの DataPower Domain スクリプト構成パラメーター』

SOA Policy Gateway Advanced Runtime を Governance Runtime にプロモートする

Advanced Runtime パターンが Governance Master パターンと共に構成されると、以下が行われます。

- セルをまたぐセキュリティーが構成される。
- Governance Master の `promotion.xml` ファイルが、Advanced Runtime デプロイメントからのデータによって更新される。

プロモーションを構成するには、以下のいずれかのステージ・オプションを選択する必要があります。

- 実動
- ステージング
- その他、または「Unset」

これらのオプションは、WSRR 内のガバナンス有効化プロファイルによって提供されるレベルに調整されます。 Governance Master のガバナンス・プロファイルが変更されている場合は、プロモーション・レベルとして「その他」を使用してください。 WSRR 内のガバナンス有効化プロファイルについて詳しくは、IBM WebSphere Service Registry and Repository バージョン 8.0 インフォメーション・センター - ガバナンス有効化プロファイルを参照してください。

関連概念:

30 ページの『DB2 Enterprise HADR Primary パーツ』
DB2 Enterprise HADR Primary パーツはいくつかの構成オプションを提供します。

34 ページの『DB2 Enterprise HADR Standby パーツ』
DB2 Enterprise HADR Standby パーツはいくつかの構成オプションを提供します。

38 ページの『WSRR デプロイメント・マネージャー・パーツ』
WSRR デプロイメント・マネージャー・パーツは、いくつかの構成オプションを提供します。

40 ページの『WSRR カスタム・ノード・パーツ』
WSRR カスタム・ノード・パーツは、いくつかの構成オプションを提供します。

49 ページの『スクリプト: SOA Policy Gateway 2.0.0.0 - Security』
Security スクリプトは、DataPower アプライアンスとの通信に必要な ZIP ファイルに含まれるセキュリティー情報を、 Linux セキュア・コピー・プログラム (SCP) をサポートする外部ファイル・サーバーから Dmgr または WSRR マシンにコピーします。

44 ページの『スクリプト: SOA Policy Gateway 2.0.0.0 - Promotion』
Promotion スクリプトにより、SOA Policy Gateway Basic Runtime または SOA Policy Gateway Advanced Runtime パターンを、 事前デプロイされた SOA Policy Gateway Governance Master パターンに統合できます。 これは Runtime および Governance パターンの間にセルをまたぐセキュリティーを確立し、同時にオプションで、WSRR プロモーションをガバナンス・マスター内に構成します。

42 ページの『スクリプト: SOA Policy Gateway 2.0.0.0 - DataPower Domain』
DataPower Domain スクリプトは、デプロイメントの際に DataPower ドメインをプロビジョンします。 スクリプトは、単一の DataPower ドメインと WSRR ランタイムとの間の接続を構成します。 WSRR ランタイムに接続される DataPower ドメインごとに、 別個の DataPower Domain スクリプトが必要になります。

パーツ

以下のパーツが IBM SOA Policy Gateway Pattern を構成します。

DB2 Enterprise パーツ

DB2 Enterprise パーツはいくつかの構成オプションを提供します。

DB2 Enterprise 9.7.5 仮想システム・イメージの構成可能パラメーターについて、以下の表で記述します。

表 2. 構成可能なパラメーター

パラメーター名	説明
仮想 CPU 数	このパーツで表される仮想マシンに割り振られる仮想プロセッサーの数。
メモリー・サイズ (MB)	この仮想マシンに割り振られたメモリーの大きさ (メガバイト)。
パスワード (db2inst1)	オペレーティング・システムのユーザー ID db2inst1 のパスワード。 このユーザー ID は、DB2 インスタンスのインストール所有者およびデータベースとスキーマの所有者として使用されます。
パスワードの確認	db2inst1 パスワードを確認します。

表 2. 構成可能なパラメーター (続き)

パラメーター名	説明
パスワード (db2fenc1)	DB2 データベースで使用されるアドレス・スペースの外部でユーザー定義関数 (UDF) とストアード・プロシージャーを実行する際に使用するユーザー ID のパスワード。 fenced ユーザーとは、制限付きのオペレーティング・システム権限を使用して一部のストアード・プロシージャー (「fenced」ストアード・プロシージャー) を実行できるユーザーを指します。これにより、オペレーティング・システムが上書きを防ぐようになるため、fenced ストアード・プロシージャーによるインスタンス・ファイルの上書きを防ぐことができます。
パスワードの確認	db2fenc1 パスワードを確認します。
パスワード (dasusr1)	システム上で DB2 管理サーバーを実行する際に使用する DB2 管理サーバー・ユーザーのユーザー ID。 デフォルト・ユーザーは dasusr1 で、デフォルト・グループは dasadm1 です。 このユーザー ID は、DB2 GUI ツールで、ローカル・サーバーのデータベース・インスタンスやデータベースに対して管理タスクを実行する際にも使用されます。
パスワードの確認	dasusr1 パスワードを確認します。
パスワード (root)	ルート・ユーザー ID のパスワード。 これは、パターン内のこのパーツが表す仮想マシンのオペレーティング・システムのパスワードです。
パスワードの確認	root パスワードを確認します。
パスワード (virtuser)	オペレーティング・システムのユーザー ID virtuser のパスワード。 このユーザー ID は、仮想マシンの非ルート・ユーザー ID として使用されます。
パスワードの確認	virtuser パスワードを確認します。

その他のパラメーターは基本の仮想システムパターンから継承され、ロックされています。

SOA Policy Gateway Basic Runtime パターンの DB2 Enterprise パーツ構成パラメーター

デフォルト値を持たない必須パラメーターは、パターンをデプロイする前に構成する必要があります。

表 3. 構成可能なパラメーター

パラメーター名	必須	デフォルト値	説明
仮想 CPU 数	はい	1	このパーツで表される仮想マシンに割り振られる仮想プロセッサーの数。
メモリー・サイズ (MB)	はい	2048	この仮想マシンに割り振られたメモリーの大きさ (メガバイト)。
パスワード (db2inst1)	はい		オペレーティング・システムのユーザー ID db2inst1 のパスワード。 このユーザー ID は、DB2 インスタンスのインストール所有者およびデータベースとスキーマの所有者として使用されます。
パスワードの確認	はい		db2inst1 パスワードを確認します。

表 3. 構成可能なパラメーター (続き)

パラメーター名	必須	デフォルト値	説明
パスワード (db2fenc1)	はい		DB2 データベースで使用されるアドレス・スペースの外部でユーザー定義関数 (UDF) とストアード・プロシージャーを実行する際に使用するユーザー ID のパスワード。 fenced ユーザーとは、制限付きのオペレーティング・システム権限を使用して一部のストアード・プロシージャー (「fenced」ストアード・プロシージャー) を実行できるユーザーを指します。これにより、オペレーティング・システムが上書きを防ぐようになるため、fenced ストアード・プロシージャーによるインスタンス・ファイルの上書きを防ぐことができます。
パスワードの確認	はい		db2fenc1 パスワードを確認します。
パスワード (dasusr1)	はい		システム上で DB2 管理サーバーを実行する際に使用する DB2 管理サーバー・ユーザーのユーザー ID。 デフォルト・ユーザーは dasusr1 で、デフォルト・グループは dasadm1 です。 このユーザー ID は、DB2 GUI ツールで、ローカル・サーバーのデータベース・インスタンスやデータベースに対して管理タスクを実行する際にも使用されます。
パスワードの確認	はい		dasusr1 パスワードを確認します。
パスワード (root)	はい		ルート・ユーザー ID のパスワード。 これは、パターン内のこのパーツが表す仮想マシンのオペレーティング・システムのパスワードです。
パスワードの確認	はい		root パスワードを確認します。
パスワード (virtuser)	はい		オペレーティング・システムのユーザー ID virtuser のパスワード。 このユーザー ID は、仮想マシンの非ルート・ユーザー ID として使用されます。
パスワードの確認	はい		virtuser パスワードを確認します。

SOA Policy Gateway Basic Runtime Sample パターンの DB2 Enterprise パーツ構成パラメーター

SOA Policy Gateway Basic Runtime Sample で、デフォルト値はすべてのパラメーター用に事前構成されています。

表 4. 構成済みパラメーター

パラメーター名	必須	デフォルト値	説明
仮想 CPU 数	はい	1	このパーツで表される仮想マシンに割り振られる仮想プロセッサーの数。
メモリー・サイズ (MB)	はい	2048	この仮想マシンに割り振られたメモリーの大きさ (メガバイト)。

表 4. 構成済みパラメーター (続き)

パラメーター名	必須	デフォルト値	説明
パスワード (db2inst1)	はい	パスワード	オペレーティング・システムのユーザー ID db2inst1 のパスワード。 このユーザー ID は、DB2 インスタンスのインストール所有者およびデータベースとスキーマの所有者として使用されます。
パスワードの確認	はい	パスワード	db2inst1 パスワードを確認します。
パスワード (db2fenc1)	はい	パスワード	DB2 データベースで使用されるアドレス・スペースの外部でユーザー定義関数 (UDF) とストアード・プロシージャーを実行する際に使用するユーザー ID のパスワード。 fenced ユーザーとは、制限付きのオペレーティング・システム権限を使用して一部のストアード・プロシージャー (「fenced」ストアード・プロシージャー) を実行できるユーザーを指します。これにより、オペレーティング・システムが上書きを防ぐようになるため、fenced ストアード・プロシージャーによるインスタンス・ファイルの上書きを防ぐことができます。
パスワードの確認	はい	パスワード	db2fenc1 パスワードを確認します。
パスワード (dasusr1)	はい	パスワード	システム上で DB2 管理サーバーを実行する際に使用する DB2 管理サーバー・ユーザーのユーザー ID。 デフォルト・ユーザーは dasusr1 で、デフォルト・グループは dasadm1 です。 このユーザー ID は、DB2 GUI ツールで、ローカル・サーバーのデータベース・インスタンスやデータベースに対して管理タスクを実行する際にも使用されます。
パスワードの確認	はい	パスワード	dasusr1 パスワードを確認します。
パスワード (root)	はい	パスワード	ルート・ユーザー ID のパスワード。 これは、パターン内のこのパーツが表す仮想マシンのオペレーティング・システムのパスワードです。
パスワードの確認	はい	パスワード	root パスワードを確認します。
パスワード (virtuser)	はい	パスワード	オペレーティング・システムのユーザー ID virtuser のパスワード。 このユーザー ID は、仮想マシンの非ルート・ユーザー ID として使用されます。
パスワードの確認	はい	パスワード	virtuser パスワードを確認します。

DB2 Enterprise HADR Primary パーツ

DB2 Enterprise HADR Primary パーツはいくつかの構成オプションを提供します。

DB2 Enterprise HADR Primary パーツの構成可能パラメーターについて、以下の表で記述します。

表 5. 構成可能なパラメーター

パラメーター名	説明
仮想 CPU 数	このパーツで表される仮想マシンに割り振られる仮想プロセッサーの数。
メモリー・サイズ (MB)	この仮想マシンに割り振られたメモリーの大きさ (メガバイト)。
パスワード (db2inst1)	オペレーティング・システムのユーザー ID db2inst1 のパスワード。 このユーザー ID は、DB2 インスタンスのインストール所有者およびデータベースとスキーマの所有者として使用されます。
パスワードの確認	db2inst1 パスワードを確認します。
パスワード (db2fenc1)	DB2 データベースで使用されるアドレス・スペースの外部でユーザー定義関数 (UDF) とストアード・プロシージャーを実行する際に使用するユーザー ID のパスワード。 fenced ユーザーとは、制限付きのオペレーティング・システム権限を使用して一部のストアード・プロシージャー (「fenced」ストアード・プロシージャー) を実行できるユーザーを指します。これにより、オペレーティング・システムが上書きを防ぐようになるため、fenced ストアード・プロシージャーによるインスタンス・ファイルの上書きを防ぐことができます。
パスワードの確認	db2fenc1 パスワードを確認します。
パスワード (dasusr1)	システム上で DB2 管理サーバーを実行する際に使用する DB2 管理サーバー・ユーザーのユーザー ID のパスワード。デフォルト・ユーザーは dasusr1 で、デフォルト・グループは dasadm1 です。 このユーザー ID は、DB2 GUI ツールで、ローカル・サーバーのデータベース・インスタンスやデータベースに対して管理タスクを実行する際にも使用されます。
パスワードの確認	dasusr1 パスワードを確認します。
パスワード (root)	ルート・ユーザー ID のパスワード。 これは、パターン内のこのパーツが表す仮想マシンのオペレーティング・システムのパスワードです。
パスワードの確認	root パスワードを確認します。
パスワード (virtuser)	オペレーティング・システムのユーザー ID virtuser のパスワード。 このユーザー ID は、仮想マシンの非ルート・ユーザー ID として使用されます。
パスワードの確認	virtuser パスワードを確認します。

その他のパラメーターは基本の仮想システムパターンから継承され、ロックされています。

SOA Policy Gateway Advanced Runtime パターンの DB2 Enterprise HADR Primary パーツ構成パラメーター

デフォルト値を持たない必須パラメーターは、パターンをデプロイする前に構成する必要があります。

表 6. 構成可能なパラメーター

パラメーター名	必須	デフォルト値	説明
仮想 CPU 数	はい	1	このパーツで表される仮想マシンに割り振られる仮想プロセッサーの数。

表 6. 構成可能なパラメーター (続き)

パラメーター名	必須	デフォルト値	説明
メモリー・サイズ (MB)	はい	2048	この仮想マシンに割り振られたメモリーの大きさ (メガバイト)。
パスワード (db2inst1)	はい		オペレーティング・システムのユーザー ID db2inst1 のパスワード。 このユーザー ID は、DB2 インスタンスのインストール所有者およびデータベースとスキーマの所有者として使用されます。
パスワードの確認	はい		db2inst1 パスワードを確認します。
パスワード (db2fenc1)	はい		DB2 データベースで使用されるアドレス・スペースの外部でユーザー定義関数 (UDF) とストアード・プロシージャーを実行する際に使用するユーザー ID のパスワード。 fenced ユーザーとは、制限付きのオペレーティング・システム権限を使用して一部のストアード・プロシージャー (「fenced」ストアード・プロシージャー) を実行できるユーザーを指します。これにより、オペレーティング・システムが上書きを防ぐようになるため、fenced ストアード・プロシージャーによるインスタンス・ファイルの上書きを防ぐことができます。
パスワードの確認	はい		db2fenc1 パスワードを確認します。
パスワード (dasusr1)	はい		システム上で DB2 管理サーバーを実行する際に使用する DB2 管理サーバー・ユーザーのユーザー ID のパスワード。デフォルト・ユーザーは dasusr1 で、デフォルト・グループは dasadm1 です。 このユーザー ID は、DB2 GUI ツールで、ローカル・サーバーのデータベース・インスタンスやデータベースに対して管理タスクを実行する際にも使用されます。
パスワードの確認	はい		dasusr1 パスワードを確認します。
パスワード (root)	はい		ルート・ユーザー ID のパスワード。 これは、パターン内のこのパーツが表す仮想マシンのオペレーティング・システムのパスワードです。
パスワードの確認	はい		root パスワードを確認します。
パスワード (virtuser)	はい		オペレーティング・システムのユーザー ID virtuser のパスワード。 このユーザー ID は、仮想マシンの非ルート・ユーザー ID として使用されます。
パスワードの確認	はい		virtuser パスワードを確認します。

SOA Policy Gateway Governance Master パターンの DB2 Enterprise HADR Primary パーツ構成パラメーター

デフォルト値を持たない必須パラメーターは、パターンをデプロイする前に構成する必要があります。

表 7. 構成可能なパラメーター

パラメーター名	必須	デフォルト値	説明
仮想 CPU 数	はい	1	このパーツで表される仮想マシンに割り振られる仮想プロセッサーの数。
メモリー・サイズ (MB)	はい	2048	この仮想マシンに割り振られたメモリーの大きさ (メガバイト)。
パスワード (db2inst1)	はい		オペレーティング・システムのユーザー ID db2inst1 のパスワード。 このユーザー ID は、DB2 インスタンスのインストール所有者およびデータベースとスキーマの所有者として使用されます。
パスワードの確認	はい		db2inst1 パスワードを確認します。
パスワード (db2fenc1)	はい		DB2 データベースで使用されるアドレス・スペースの外部でユーザー定義関数 (UDF) とストアード・プロシージャーを実行する際に使用するユーザー ID のパスワード。 fenced ユーザーとは、制限付きのオペレーティング・システム権限を使用して一部のストアード・プロシージャー (「fenced」ストアード・プロシージャー) を実行できるユーザーを指します。これにより、オペレーティング・システムが上書きを防ぐようになるため、fenced ストアード・プロシージャーによるインスタンス・ファイルの上書きを防ぐことができます。
パスワードの確認	はい		db2fenc1 パスワードを確認します。
パスワード (dasusr1)	はい		システム上で DB2 管理サーバーを実行する際に使用する DB2 管理サーバー・ユーザーのユーザー ID のパスワード。デフォルト・ユーザーは dasusr1 で、デフォルト・グループは dasadm1 です。 このユーザー ID は、DB2 GUI ツールで、ローカル・サーバーのデータベース・インスタンスやデータベースに対して管理タスクを実行する際にも使用されます。
パスワードの確認	はい		dasusr1 パスワードを確認します。
パスワード (root)	はい		ルート・ユーザー ID のパスワード。 これは、パターン内のこのパーツが表す仮想マシンのオペレーティング・システムのパスワードです。
パスワードの確認	はい		root パスワードを確認します。
パスワード (virtuser)	はい		オペレーティング・システムのユーザー ID virtuser のパスワード。 このユーザー ID は、仮想マシンの非ルート・ユーザー ID として使用されます。
パスワードの確認	はい		virtuser パスワードを確認します。

DB2 Enterprise HADR Standby パーツ

DB2 Enterprise HADR Standby パーツはいくつかの構成オプションを提供します。

表 8. 構成可能なパラメーター

パラメーター名	説明
仮想 CPU 数	このパーツで表される仮想マシンに割り振られる仮想プロセッサーの数。
メモリー・サイズ (MB)	この仮想マシンに割り振られたメモリーの大きさ (メガバイト)。
パスワード (db2inst1)	オペレーティング・システムのユーザー ID db2inst1 のパスワード。 このユーザー ID は、DB2 インスタンスのインストール所有者およびデータベースとスキーマの所有者として使用されます。
パスワードの確認	db2inst1 パスワードを確認します。
パスワード (db2fenc1)	DB2 データベースで使用されるアドレス・スペースの外部でユーザー定義関数 (UDF) とストアード・プロシージャーを実行する際に使用するユーザー ID のパスワード。 fenced ユーザーとは、制限付きのオペレーティング・システム権限を使用して一部のストアード・プロシージャー (「fenced」ストアード・プロシージャー) を実行できるユーザーを指します。これにより、オペレーティング・システムが上書きを防ぐようになるため、fenced ストアード・プロシージャーによるインスタンス・ファイルの上書きを防ぐことができます。
パスワードの確認	db2fenc1 パスワードを確認します。
パスワード (dasusr1)	システム上で DB2 管理サーバーを実行する際に使用する DB2 管理サーバー・ユーザーのユーザー ID のパスワード。デフォルト・ユーザーは dasusr1 で、デフォルト・グループは dasadm1 です。 このユーザー ID は、DB2 GUI ツールで、ローカル・サーバーのデータベース・インスタンスやデータベースに対して管理タスクを実行する際にも使用されます。
パスワードの確認	dasusr1 パスワードを確認します。
パスワード (root)	ルート・ユーザー ID のパスワード。 これは、パターン内のこのパーツが表す仮想マシンのオペレーティング・システムのパスワードです。
パスワードの確認	root パスワードを確認します。
パスワード (virtuser)	オペレーティング・システムのユーザー ID virtuser のパスワード。 このユーザー ID は、仮想マシンの非ルート・ユーザー ID として使用されます。
パスワードの確認	virtuser パスワードを確認します。

その他のパラメーターは基本の仮想システムパターンから継承され、ロックされています。

SOA Policy Gateway Advanced Runtime パターンの DB2 Enterprise HADR Standby パーツ構成パラメーター

デフォルト値を持たない必須パラメーターは、パターンをデプロイする前に構成する必要があります。

表 9. 構成可能なパラメーター

パラメーター名	必須	デフォルト値	説明
仮想 CPU 数	はい	1	このパーツで表される仮想マシンに割り振られる仮想プロセッサーの数。
メモリー・サイズ (MB)	はい	2048	この仮想マシンに割り振られたメモリーの大きさ (メガバイト)。

表 9. 構成可能なパラメーター (続き)

パラメーター名	必須	デフォルト値	説明
パスワード (db2inst1)	はい		オペレーティング・システムのユーザー ID db2inst1 のパスワード。 このユーザー ID は、DB2 インスタンスのインストール所有者およびデータベースとスキーマの所有者として使用されます。
パスワードの確認	はい		db2inst1 パスワードを確認します。
パスワード (db2fenc1)	はい		DB2 データベースで使用されるアドレス・スペースの外部でユーザー定義関数 (UDF) とストアード・プロシージャーを実行する際に使用するユーザー ID のパスワード。 fenced ユーザーとは、制限付きのオペレーティング・システム権限を使用して一部のストアード・プロシージャー (「fenced」ストアード・プロシージャー) を実行できるユーザーを指します。これにより、オペレーティング・システムが上書きを防ぐようになるため、fenced ストアード・プロシージャーによるインスタンス・ファイルの上書きを防ぐことができます。
パスワードの確認	はい		db2fenc1 パスワードを確認します。
パスワード (dasusr1)	はい		システム上で DB2 管理サーバーを実行する際に使用する DB2 管理サーバー・ユーザーのユーザー ID のパスワード。デフォルト・ユーザーは dasusr1 で、デフォルト・グループは dasadm1 です。 このユーザー ID は、DB2 GUI ツールで、ローカル・サーバーのデータベース・インスタンスやデータベースに対して管理タスクを実行する際にも使用されます。
パスワードの確認	はい		dasusr1 パスワードを確認します。
パスワード (root)	はい		ルート・ユーザー ID のパスワード。 これは、パターン内のこのパーツが表す仮想マシンのオペレーティング・システムのパスワードです。
パスワードの確認	はい		root パスワードを確認します。
パスワード (virtuser)	はい		オペレーティング・システムのユーザー ID virtuser のパスワード。 このユーザー ID は、仮想マシンの非ルート・ユーザー ID として使用されます。
パスワードの確認	はい		virtuser パスワードを確認します。

SOA Policy Gateway Governance Master パターンの DB2 Enterprise HADR Standby パーツ構成パラメーター

デフォルト値を持たない必須パラメーターは、パターンをデプロイする前に構成する必要があります。

表 10. 構成可能なパラメーター

パラメーター名	必須	デフォルト値	説明
仮想 CPU 数	はい	1	このパーツで表される仮想マシンに割り振られる仮想プロセッサーの数。
メモリー・サイズ (MB)	はい	2048	この仮想マシンに割り振られたメモリーの大きさ (メガバイト)。
パスワード (db2inst1)	はい		オペレーティング・システムのユーザー ID db2inst1 のパスワード。 このユーザー ID は、DB2 インスタンスのインストール所有者およびデータベースとスキーマの所有者として使用されます。
パスワードの確認	はい		db2inst1 パスワードを確認します。
パスワード (db2fenc1)	はい		DB2 データベースで使用されるアドレス・スペースの外部でユーザー定義関数 (UDF) とストアード・プロシージャーを実行する際に使用するユーザー ID のパスワード。 fenced ユーザーとは、制限付きのオペレーティング・システム権限を使用して一部のストアード・プロシージャー (「fenced」ストアード・プロシージャー) を実行できるユーザーを指します。これにより、オペレーティング・システムが上書きを防ぐようになるため、fenced ストアード・プロシージャーによるインスタンス・ファイルの上書きを防ぐことができます。
パスワードの確認	はい		db2fenc1 パスワードを確認します。
パスワード (dasusr1)	はい		システム上で DB2 管理サーバーを実行する際に使用する DB2 管理サーバー・ユーザーのユーザー ID のパスワード。デフォルト・ユーザーは dasusr1 で、デフォルト・グループは dasadm1 です。 このユーザー ID は、DB2 GUI ツールで、ローカル・サーバーのデータベース・インスタンスやデータベースに対して管理タスクを実行する際にも使用されます。
パスワードの確認	はい		dasusr1 パスワードを確認します。
パスワード (root)	はい		ルート・ユーザー ID のパスワード。 これは、パターン内のこのパーツが表す仮想マシンのオペレーティング・システムのパスワードです。
パスワードの確認	はい		root パスワードを確認します。
パスワード (virtuser)	はい		オペレーティング・システムのユーザー ID virtuser のパスワード。 このユーザー ID は、仮想マシンの非ルート・ユーザー ID として使用されます。
パスワードの確認	はい		virtuser パスワードを確認します。

WSRR スタンドアロン・サーバー・パーツ

WSRR スタンドアロン・サーバー・パーツは幾つかの構成オプションを提供します。

WSRR スタンドアロン・サーバー・パーツの構成可能パラメーターについて、以下の表で記述します。

表 11. 構成済みパラメーター

パラメーター名	説明
仮想 CPU 数	このパーツで表される仮想マシンに割り振られる仮想プロセッサーの数。
メモリー・サイズ (MB)	この仮想マシンに割り振られたメモリーの大きさ (メガバイト)。
パスワード (root)	ルート・ユーザー ID のパスワード。 これは、パターン内のこのパーツが表す仮想マシンのオペレーティング・システムのパスワードです。
パスワードの確認	パスワード (root) のユーザー入力を確認します。
WebSphere 管理ユーザー名	WebSphere 環境の管理者ユーザー名。
WebSphere 管理パスワード	WebSphere 環境の管理者ユーザー・パスワード。
パスワードの確認	WebSphere 管理者パスワードのユーザー入力を確認します。
物理メモリーの予約	この仮想マシン専用に予約された物理メモリー。

その他のパラメーターは基本の仮想システムパターンから継承され、ロックされています。

SOA Policy Gateway Basic Runtime パターンの WSRR スタンドアロン・サーバー・パーツ構成パラメーター

デフォルト値を持たない必須パラメーターは、パターンをデプロイする前に構成する必要があります。

表 12. 構成可能なパラメーター

パラメーター名	必須	デフォルト値	説明
仮想 CPU 数	はい	1	このパーツで表される仮想マシンに割り振られる仮想プロセッサーの数。
メモリー・サイズ (MB)	はい	4096	この仮想マシンに割り振られたメモリーの大きさ (メガバイト)。
物理メモリーの予約	はい	False	この仮想マシン専用に予約された物理メモリー。
セル名	はい	SOAPolicyBasicCell	Basic Runtime パターンに含まれる仮想マシンの WebSphere セル名。
ノード名	はい	SOAPolicyBasicNode	Basic Runtime パターンに含まれる仮想マシンの WebSphere ノード名。
パスワード (root)	はい		ルート・ユーザー ID のパスワード。 これは、パターン内のこのパーツが表す仮想マシンのオペレーティング・システムのパスワードです。
パスワードの確認	はい		パスワード (root) のユーザー入力を確認します。
WebSphere 管理ユーザー名	はい	virtuser	WebSphere 環境の管理者ユーザー名。
WebSphere 管理パスワード	はい		WebSphere 環境の管理者ユーザー・パスワード。
パスワードの確認	はい		WebSphere 管理者パスワードのユーザー入力を確認します。

SOA Policy Gateway Basic Runtime Sample パターンの WSRR スタンドアロン・サーバー・パーツ構成パラメーター

SOA Policy Gateway Basic Runtime Sample で、デフォルト値はすべてのパラメーター用に事前構成されています。

表 13. 構成済みパラメーター

パラメーター名	必須	デフォルト値	説明
仮想 CPU 数	はい	1	このパーツで表される仮想マシンに割り振られる仮想プロセッサーの数。
メモリー・サイズ (MB)	はい	4096	この仮想マシンに割り振られたメモリーの大きさ (メガバイト)。
物理メモリーの予約	はい	False	この仮想マシン専用に予約された物理メモリー。
パスワード (root)	はい	パスワード	ルート・ユーザー ID のパスワード。 これは、パターン内のこのパーツが表す仮想マシンのオペレーティング・システムのパスワードです。
パスワードの確認	はい	パスワード	パスワード (root) のユーザー入力を確認します。
WebSphere 管理ユーザー名	はい	virtuser	WebSphere 環境の管理者ユーザー名。
WebSphere 管理パスワード	はい	パスワード	WebSphere 環境の管理者ユーザー・パスワード。
パスワードの確認	はい	パスワード	WebSphere 管理者パスワードのユーザー入力を確認します。

WSRR デプロイメント・マネージャー・パーツ

WSRR デプロイメント・マネージャー・パーツは、いくつかの構成オプションを提供します。

WSRR デプロイメント・マネージャー・パーツの構成可能パラメーターについて、以下の表で記述します。

表 14. 構成可能なパラメーター

パラメーター名	説明
仮想 CPU 数	このパーツで表される仮想マシンに割り振られる仮想プロセッサーの数。
メモリー・サイズ (MB)	この仮想マシンに割り振られたメモリーの大きさ (メガバイト)。
物理 CPU の予約	この仮想マシン専用に予約された物理 CPU 数。
物理メモリーの予約	この仮想マシン専用に予約された物理メモリー。
セル名	Advanced Runtime パターン用の WebSphere セル名。
ノード名	Advanced Runtime パターン内のデプロイメント・マネージャー仮想マシンにある、WebSphere ノードのノード名。
パスワード (root)	ルート・ユーザー ID のパスワード。 これは、パターン内のこのパーツが表す仮想マシンのオペレーティング・システムのパスワードです。
パスワードの確認	パスワード (root) のユーザー入力を確認します。
WebSphere 管理ユーザー名	WebSphere 環境の管理者ユーザー名。

表 14. 構成可能なパラメーター (続き)

パラメーター名	説明
WebSphere 管理パスワード	WebSphere 環境の管理者ユーザー・パスワード。
パスワードの確認	WebSphere 管理者パスワードのユーザー入力を確認します。

その他のパラメーターは基本の仮想システムパターンから継承され、ロックされています。

SOA Policy Gateway Advanced Runtime パターンの WSRR デプロイメント・マネージャー・パーツ構成パラメーター

デフォルト値を持たない必須パラメーターは、パターンをデプロイする前に構成する必要があります。

表 15. 構成可能なパラメーター

パラメーター名	必須	デフォルト値	説明
仮想 CPU 数	はい	1	このパーツで表される仮想マシンに割り振られる仮想プロセッサーの数。
メモリー・サイズ (MB)	はい	2048	この仮想マシンに割り振られたメモリーの大きさ (メガバイト)。
物理 CPU の予約	はい	False	この仮想マシン専用に予約された物理 CPU 数。
物理メモリーの予約	はい	False	この仮想マシン専用に予約された物理メモリー。
セル名	はい	SOAPolicyAdvancedCell	Advanced Runtime パターン用の WebSphere セル名。
ノード名	はい	SOAPolicyAdvancedNode	Advanced Runtime パターン内のデプロイメント・マネージャー仮想マシンにある、WebSphere ノードのノード名。
パスワード (root)	はい		ルート・ユーザー ID のパスワード。 これは、パターン内のこのパーツが表す仮想マシンのオペレーティング・システムのパスワードです。
パスワードの確認	はい		パスワード (root) のユーザー入力を確認します。
WebSphere 管理ユーザー名	はい	virtuser	WebSphere 環境の管理者ユーザー名。
WebSphere 管理パスワード	はい		WebSphere 環境の管理者ユーザー・パスワード。
パスワードの確認	はい		WebSphere 管理者パスワードのユーザー入力を確認します。

SOA Policy Gateway Governance Master パターンの WSRR デプロイメント・マネージャー・パーツ構成パラメーター

デフォルト値を持たない必須パラメーターは、パターンをデプロイする前に構成する必要があります。

表 16. 構成可能なパラメーター

パラメーター名	必須	デフォルト値	説明
仮想 CPU 数	はい	1	このパーツで表される仮想マシンに割り振られる仮想プロセッサーの数。
メモリー・サイズ (MB)	はい	2048	この仮想マシンに割り振られたメモリーの大きさ (メガバイト)。
物理 CPU の予約	はい	False	この仮想マシン専用に予約された物理 CPU 数。
物理メモリーの予約	はい	False	この仮想マシン専用に予約された物理メモリー。
セル名	はい	SOAPolicyGMCell	Advanced Runtime パターン用の WebSphere セル名。
ノード名	はい	SOAPolicyGMNode	Advanced Runtime パターン内のデプロイメント・マネージャー仮想マシンにある、WebSphere ノードのノード名。
パスワード (root)	はい		ルート・ユーザー ID のパスワード。 これは、パターン内のこのパーツが表す仮想マシンのオペレーティング・システムのパスワードです。
パスワードの確認	はい		パスワード (root) のユーザー入力を確認します。
WebSphere 管理ユーザー名	はい	virtuser	WebSphere 環境の管理者ユーザー名。
WebSphere 管理パスワード	はい		WebSphere 環境の管理者ユーザー・パスワード。
パスワードの確認	はい		WebSphere 管理者パスワードのユーザー入力を確認します。

WSRR カスタム・ノード・パーツ

WSRR カスタム・ノード・パーツは、いくつかの構成オプションを提供します。

WSRR カスタム・ノード・パーツの構成可能パラメーターについて、以下の表で記述します。

表 17. 構成可能なパラメーター

パラメーター名	説明
仮想 CPU 数	このパーツで表される仮想マシンに割り振られる仮想プロセッサーの数。
メモリー・サイズ (MB)	この仮想マシンに割り振られたメモリーの大きさ (メガバイト)。
物理 CPU の予約	この仮想マシン専用に予約された物理 CPU 数。
物理メモリーの予約	この仮想マシン専用に予約された物理メモリー。
セル名	カスタム・ノード・パーツ構成のセル名値は無視されます。デプロイメント・マネージャー・パーツの構成に指定されたセル名が使用されます。
ノード名	Advanced Runtime パターン内のカスタム・ノード仮想マシンにある、WebSphere ノードのノード名。
パスワード (root)	ルート・ユーザー ID のパスワード。 これは、パターン内のこのパーツが表す仮想マシンのオペレーティング・システムのパスワードです。
パスワードの確認	パスワード (root) のユーザー入力を確認します。

表 17. 構成可能なパラメーター (続き)

パラメーター名	説明
WebSphere 管理ユーザー名	WebSphere 環境の管理者ユーザー名。
WebSphere 管理パスワード	WebSphere 環境の管理者ユーザー・パスワード。
パスワードの確認	WebSphere 管理者パスワードのユーザー入力を確認します。

その他のパラメーターは基本の仮想システムパターンから継承され、ロックされています。

SOA Policy Gateway Advanced Runtime パターンの WSRR カスタム・ノード・パーツ構成パラメーター

デフォルト値を持たない必須パラメーターは、パターンをデプロイする前に構成する必要があります。

表 18. 構成可能なパラメーター

パラメーター名	必須	デフォルト値	説明
仮想 CPU 数	はい	2	このパーツで表される仮想マシンに割り振られる仮想プロセッサーの数。
メモリー・サイズ (MB)	はい	4096	この仮想マシンに割り振られたメモリーの大きさ (メガバイト)。
物理 CPU の予約	はい	False	この仮想マシン専用に予約された物理 CPU 数。
物理メモリーの予約	はい	False	この仮想マシン専用に予約された物理メモリー。
ノード名	はい	SOAPolicyAdvancedNode	Advanced Runtime パターン内のカスタム・ノード仮想マシンにある、WebSphere ノードのノード名。
パスワード (root)	はい		ルート・ユーザー ID のパスワード。 これは、パターン内のこのパーツが表す仮想マシンのオペレーティング・システムのパスワードです。
パスワードの確認	はい		パスワード (root) のユーザー入力を確認します。
WebSphere 管理ユーザー名	はい	virtuser	WebSphere 環境の管理者ユーザー名。
WebSphere 管理パスワード	はい		WebSphere 環境の管理者ユーザー・パスワード。
パスワードの確認	はい		WebSphere 管理者パスワードのユーザー入力を確認します。

SOA Policy Gateway Governance Master パターンの WSRR カスタム・ノード・パーツ構成パラメーター

デフォルト値を持たない必須パラメーターは、パターンをデプロイする前に構成する必要があります。

表 19. 構成可能なパラメーター

パラメーター名	必須	デフォルト値	説明
仮想 CPU 数	はい	2	このパーツで表される仮想マシンに割り振られる仮想プロセッサーの数。
メモリー・サイズ (MB)	はい	4096	この仮想マシンに割り振られたメモリーの大きさ (メガバイト)。
物理 CPU の予約	はい	False	この仮想マシン専用に予約された物理 CPU 数。
物理メモリーの予約	はい	False	この仮想マシン専用に予約された物理メモリー。
ノード名	はい	SOAPolicyGMNode	Advanced Runtime パターン内のカスタム・ノード仮想マシンにある、WebSphere ノードのノード名。
パスワード (root)	はい		ルート・ユーザー ID のパスワード。 これは、パターン内のこのパーツが表す仮想マシンのオペレーティング・システムのパスワードです。
パスワードの確認	はい		パスワード (root) のユーザー入力を確認します。
WebSphere 管理ユーザー名	はい	virtuser	WebSphere 環境の管理者ユーザー名。
WebSphere 管理パスワード	はい		WebSphere 環境の管理者ユーザー・パスワード。
パスワードの確認	はい		WebSphere 管理者パスワードのユーザー入力を確認します。

スクリプト・パッケージ

IBM SOA Policy Gateway Pattern には、4 つのスクリプト・パッケージが準備されています。

このパターンに含まれるスクリプト・パッケージは、以下のとおりです。

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

スクリプト: SOA Policy Gateway 2.0.0.0 - DataPower Domain

DataPower Domain スクリプトは、デプロイメントの際に DataPower ドメインをプロビジョンします。スクリプトは、単一の DataPower ドメインと WSRR ランタイムとの間の接続を構成します。 WSRR ランタイムに接続される DataPower ドメインごとに、別個の DataPower Domain スクリプトが必要になります。

パラメーター

表 20. 構成可能なパラメーター

パラメーター名	説明
DataPower_hostname	サンプル・アプリケーションのインストール先となる DataPower アプライアンスのホスト名。
DataPower_XML_mgmt_port	DataPower XML Management Interface に使用されるポート (通常は 5550)。
Datapower_admin_id	XML Management Interface を使用するための適切な権限がある管理者ユーザー ID。
DataPower_admin_password	DataPower_admin_id のパスワード。
パスワードの確認	DataPower_admin_password のユーザー入力を確認します。
New_DataPower_domain	DataPower アプライアンス上に作成する新しいドメイン・ネーム。既存のドメインと一致しないものである必要があります。そうしないと、スクリプト・パッケージは失敗するか、または終了します。値にスペースを含めることはできません。
securityFileCleanUp	DataPower にアップロードされた `DomainZipFile.zip` ファイルおよび WSRR 証明書が、スクリプト・パッケージが実行される WSRR インスタンスから削除されているかどうかを判別します。このファイルが削除されていない場合、証明書がインスタンス上に残されていると、機密漏れになります。

SOA Policy Gateway 2.0.0.0 - SOA Policy Gateway Basic Runtime パターンの DataPower Domain スクリプト構成パラメーター

デフォルト値を持たない必須パラメーターは、パターンをデプロイする前に構成する必要があります。

表 21. 構成可能なパラメーター

パラメーター名	必須	デフォルト値	説明
DataPower_hostname	はい		サンプル・アプリケーションのインストール先となる DataPower アプライアンスのホスト名。
DataPower_XML_mgmt_port	はい	5550	DataPower XML Management Interface に使用されるポート (通常は 5550)。
Datapower_admin_id	はい		XML Management Interface を使用するための適切な権限がある管理者ユーザー ID。
DataPower_admin_password	はい		DataPower_admin_id のパスワード。
パスワードの確認	はい		DataPower_admin_password のユーザー入力を確認します。
New_DataPower_domain	はい		DataPower アプライアンス上に作成する新しいドメイン・ネーム。既存のドメインと一致しないものである必要があります。そうしないと、スクリプト・パッケージは失敗するか、または終了します。値にスペースを含めることはできません。

表 21. 構成可能なパラメーター (続き)

パラメーター名	必須	デフォルト値	説明
Remove_security_files	はい	true	DataPower にアップロードされた DomainZipFile.zip ファイルおよび WSRR 証明書が、スクリプト・パッケージが実行される WSRR インスタンスから削除されているかどうかを判別します。このファイルが削除されていない場合、証明書がインスタンス上に残されていると、機密漏れになります。

SOA Policy Gateway 2.0.0.0 - SOA Policy Gateway Advanced Runtime パターンの DataPower Domain スクリプト構成パラメーター

デフォルト値を持たない必須パラメーターは、パターンをデプロイする前に構成する必要があります。

表 22. 構成可能なパラメーター

パラメーター名	必須	デフォルト値	説明
DataPower_hostname	はい		サンプル・アプリケーションのインストール先となる DataPower アプライアンスのホスト名。
DataPower_XML_mgmt_port	はい	5550	DataPower XML Management Interface に使用されるポート (通常は 5550)。
Datapower_admin_id	はい		XML Management Interface を使用するための適切な権限がある管理者ユーザー ID。
DataPower_admin_password	はい		DataPower_admin_id のパスワード。
パスワードの確認	はい		DataPower_admin_password のユーザー入力を確認します。
New_DataPower_domain	はい		DataPower アプライアンス上に作成する新しいドメイン・ネーム。既存のドメインと一致しないものである必要があります。そうしないと、スクリプト・パッケージは失敗するか、または終了します。値にスペースを含めることはできません。
Remove_security_files	はい	true	DataPower にアップロードされた DomainZipFile.zip ファイルおよび WSRR 証明書が、スクリプト・パッケージが実行される WSRR インスタンスから削除されているかどうかを判別します。このファイルが削除されていない場合、証明書がインスタンス上に残されていると、機密漏れになります。

スクリプト: SOA Policy Gateway 2.0.0.0 - Promotion

Promotion スクリプトにより、SOA Policy Gateway Basic Runtime または SOA Policy Gateway Advanced Runtime パターンを、事前デプロイされた SOA Policy Gateway Governance Master パターンに統合できます。これは Runtime および Governance パターンの間にセルをまたぐセキュリティーを確立し、同時にオプションで、WSRR プロモーションをガバナンス・マスター内に構成します。

パラメーター

表 23. 構成可能なパラメーター

パラメーター名	説明
WSRR_GOV_DMGR_hostname	WSRR クラスター用の Dmgr のホスト名。
WSRR_GOV_DMGR_cellname	WSRR クラスター用の WebSphere セル名。
WSRR_GOV_admin_user	WebSphere WSRR Governance Cell の管理 ID。
WSRR_GOV_admin_password	WebSphere WSRR Governance Cell の管理 ID のパスワード。
Verify password	WSRR_GOV_admin_password のユーザー入力を確認します。
Promotion_environment	「staging」、「production」、または「Unset」のいずれかでなければなりません。これらの値には大/小文字の区別があり、正確に一致する必要があります。
LTPA_key_password	LTPA 鍵は、ガバナンス・マスターに由来し、スクリプト・パッケージの際にエクスポートされて使用され、プロモーション環境ですべての CELLS にわたって使用されます。これはその LTPA 鍵をエクスポートするときに使用されるパスワードです。
パスワードの確認	LTPA_key_password のユーザー入力を確認します。

SOA Policy Gateway 2.0.0.0 - SOA Policy Gateway Basic Runtime パターンのプロモーション・スクリプト構成パラメーター

デフォルト値を持たない必須パラメーターは、パターンをデプロイする前に構成する必要があります。

表 24. 構成可能なパラメーター

パラメーター名	必須	デフォルト値	説明
WSRR_GOV_DMGR_hostname	はい		WSRR クラスター用の Dmgr のホスト名。
WSRR_GOV_DMGR_cellname	はい		WSRR クラスター用の WebSphere セル名。
WSRR_GOV_admin_user	はい		WebSphere WSRR Governance Cell の管理 ID。
WSRR_GOV_admin_password	はい		WebSphere WSRR Governance Cell の管理 ID のパスワード。
パスワードの確認	はい		WSRR_GOV_admin_password のユーザー入力を確認します。
Promotion_environment	はい		「staging」、「production」、または「Unset」のいずれかでなければなりません。これらの値には大/小文字の区別があり、正確に一致する必要があります。
LTPA_key_password	はい		LTPA 鍵は、ガバナンス・マスターに由来し、スクリプト・パッケージの際にエクスポートされて使用され、プロモーション環境ですべての CELLS にわたって使用されます。これはその LTPA 鍵をエクスポートするときに使用されるパスワードです。
パスワードの確認	はい		LTPA_key_password のユーザー入力を確認します。

SOA Policy Gateway 2.0.0.0 - SOA Policy Gateway Advanced Runtime パターンのプロモーション・スクリプト構成パラメーター

デフォルト値を持たない必須パラメーターは、パターンをデプロイする前に構成する必要があります。

表 25. 構成可能なパラメーター

パラメーター名	必須	デフォルト値	説明
WSRR_GOV_DMGR_hostname	はい		WSRR クラスター用の Dmgr のホスト名。
WSRR_GOV_DMGR_cellname	はい		WSRR クラスター用の WebSphere セル名。
WSRR_GOV_admin_user	はい		WebSphere WSRR Governance Cell の管理 ID。
WSRR_GOV_admin_password	はい		WebSphere WSRR Governance Cell の管理 ID のパスワード。
パスワードの確認	はい		WSRR_GOV_admin_password のユーザー入力を確認します。
Promotion_environment	はい		「staging」、「production」、または「Unset」のいずれかでなければなりません。これらの値には大/小文字の区別があり、正確に一致する必要があります。
LTPA_key_password	はい		LTPA 鍵は、ガバナンス・マスターに由来し、スクリプト・パッケージの際にエクスポートされて使用され、プロモーション環境ですべての CELLS にわたって使用されます。これはその LTPA 鍵をエクスポートするときに使用されるパスワードです。
パスワードの確認	はい		LTPA_key_password のユーザー入力を確認します。

スクリプト: SOA Policy Gateway 2.0.0.0 - Sample

Sample スクリプトは、SOA Policy Gateway Basic Runtime Sample パターンと共に使用する、サンプル・アプリケーション・パラメーターを構成します。

パラメーター

注: 値「Unset」が必要なパラメーターでは、大/小文字の区別があります。

表 26. 構成可能なパラメーター

パラメーター名	説明
SCP_host	`DomainZipFile.zip` を含む SCP サーバーのホスト名。
SCP_user	SCP サーバーへの接続に使用するユーザー名。
SCP_password	SCP サーバーへのログインに使用するパスワード。
パスワードの確認	SCP_password のユーザー入力を確認します。
SCP_zip_location	`DomainZipFile.zip` の URI ロケーション。たとえば、`/files/DomainZipFile.zip` など。
CLIENT_PUBLIC_KEY_file	DataPower Appliances XML Management Interface ポートへの接続に使用される PEM 証明書ファイルの名前。「Unset」値はサーバー認証だけに使用し、SSL では使用しないでください。

表 26. 構成可能なパラメーター (続き)

パラメーター名	説明
CLIENT_PUBLIC _KEY_password	DataPower Appliances XML Management Interface ポートへの接続に使用される公開証明書のパスワード。パスワードが使用されていない場合、値は「Unset」です。
パスワードの確認	CLIENT_PUBLIC_KEY_password のユーザー入力を確認します。
CLIENT_PRIVATE_KEY_file	DataPower Appliances XML Management Interface ポートへの接続に使用する、PEM 鍵ファイルの名前。これは相互認証に必要です。「Unset」値はサーバー認証だけに使用し、SSL では使用しないでください。
CLIENT_PRIVATE_KEY_password	DataPower Appliances XML Management Interface ポートへの接続に使用する、鍵ファイルのパスワード。これは相互認証に必要です。パスワードが使用されていない場合、値は「Unset」です。
パスワードの確認	CLIENT_PRIVATE_KEY_password のユーザー入力を確認します。
CLI_FILE_file	DomainZipFile.zip ファイルに含まれる CLI ファイルの名前。 この CLI は、ドメインのインストールおよび WSRR サーバー構成の最後に実行されます。
パスワードの確認	LTPA_KEY_password のユーザー入力を確認します。
DataPower_hostname	サンプル・アプリケーションのインストール先となる DataPower アプライアンスのホスト名。
DataPower_XML_mgmt_port	DataPower XML Management Interface に使用されるポート。
DataPower_admin_id	XML Management Interface を使用するための適切な権限がある管理者ユーザー ID。
DataPower_admin_password	DataPower_admin_id のパスワード。
パスワードの確認	DataPower_admin_password のユーザー入力を確認します。
SOAPolicySample_DataPower_domain	サンプル・ドメイン名。 これは DataPower アプライアンス上にある既存のドメインと一致しないものである必要があります。
SamplePolicySample_starting_port	アプリケーションには 5 つの空きポートが必要です。それらはこの値から順番に使用されます。例えば、値が 62000 の場合は、ポート 62000 から 62004 が使用されます。ポートが空いているかどうかの検査は、スクリプトからは行われません。
LDAP_hostname	サンプルでは LDAP サーバーが使用されます。これはそのサーバーのホスト名です。
LDAP_port	LDAP サーバーの非セキュア・ポート。通常は 389 です。
LDAP_password	LDAP_DN とバインドする際に使用されるパスワード。
パスワードの確認	LDAP_password のユーザー入力を確認します。
LDAP_DN	LDAP へのバインドに使用される識別名。例えば、cn=root,dc=ibm.com です。

SOA Policy Gateway 2.0.0.0 - SOA Policy Gateway Basic Runtime Sample パターンのサンプル・スクリプト構成パラメーター

デフォルト値を持たない必須パラメーターは、パターンをデプロイする前に構成する必要があります。

注: 値「Unset」が必要なパラメーターでは、大/小文字の区別があります。

表 27. 構成可能なパラメーター

パラメーター名	必須	デフォルト値	説明
SCP_host	はい		`DomainZipFile.zip` を含む SCP サーバーのホスト名。
SCP_user	はい		SCP サーバーへの接続に使用するユーザー名。
SCP_password	はい		SCP サーバーへのログインに使用するパスワード。
パスワードの確認	はい		SCP_password のユーザー入力を確認します。
SCP_zip_location	はい		`DomainZipFile.zip` の URI ロケーション。たとえば、`/files/DomainZipFile.zip` など。
CLIENT_PUBLIC_KEY_file	はい		DataPower Appliances XML Management Interface ポートへの接続に使用される PEM 証明書ファイルの名前。「Unset」値はサーバー認証だけに使用し、SSL では使用しないでください。
CLIENT_PUBLIC _KEY_password	はい		DataPower Appliances XML Management Interface ポートへの接続に使用される公開証明書のパスワード。パスワードが使用されていない場合、値は「Unset」です。
パスワードの確認	はい		CLIENT_PUBLIC_KEY_password のユーザー入力を確認します。
CLIENT_PRIVATE_KEY_file	はい		DataPower Appliances XML Management Interface ポートへの接続に使用する、PEM 鍵ファイルの名前。これは相互認証に必要です。「Unset」値はサーバー認証だけに使用し、SSL では使用しないでください。
CLIENT_PRIVATE_KEY_password	はい		DataPower Appliances XML Management Interface ポートへの接続に使用する、鍵ファイルのパスワード。これは相互認証に必要です。パスワードが使用されていない場合、値は「Unset」です。
パスワードの確認	はい		CLIENT_PRIVATE_KEY_password のユーザー入力を確認します。
DataPower_hostname	はい		サンプル・アプリケーションのインストール先となる DataPower アプライアンスのホスト名。
DataPower_XML_mgmt_port	はい	5550	DataPower XML Management Interface に使用されるポート。
DataPower_admin_id	はい		XML Management Interface を使用するための適切な権限がある管理者ユーザー ID。
DataPower_admin_password	はい		DataPower_admin_id のパスワード。

表 27. 構成可能なパラメーター (続き)

パラメーター名	必須	デフォルト値	説明
パスワードの確認	はい		DataPower_admin_password のユーザー入力を確認します。
SOAPolicySample_DataPower_domain	はい	SOAPolicySample	サンプル・ドメイン名。 これは DataPower アプライアンス上にある既存のドメインと一致しないものである必要があります。
SOAPolicySample_starting_port	はい	62001	アプリケーションには 5 つの空きポートが必要です。それらはこの値から順番に使用されます。例えば、値が 62000 の場合は、ポート 62000 から 62004 が使用されます。ポートが空いているかどうかの検査は、スクリプトからは行われません。
LDAP_hostname	はい		サンプルでは LDAP サーバーが使用されます。これはそのサーバーのホスト名です。
LDAP_port	はい	389	LDAP サーバーの非セキュア・ポート。通常は 389 です。
LDAP_password	はい		LDAP_DN とバインドする際に使用されるパスワード。
パスワードの確認	はい		LDAP_password のユーザー入力を確認します。
LDAP_DN	はい		LDAP へのバインドに使用される識別名。例えば、cn=root,dc=ibm.com です。

スクリプト: SOA Policy Gateway 2.0.0.0 - Security

Security スクリプトは、DataPower アプライアンスとの通信に必要な ZIP ファイルに含まれるセキュリティー情報を、 Linux セキュア・コピー・プログラム (SCP) をサポートする外部ファイル・サーバーから Dmgr または WSRR マシンにコピーします。

コピーされるセキュリティー・ファイルには、以下のものが含まれます。

- DPC アクセス証明書
- DPC アクセス公開証明書
- DPC 秘密鍵
- DP CLI スクリプト
- フォルダー証明書チェーン

DataPower のコマンド・ライン・インターフェース (CLI) スクリプトにより、パターン・デプロイメント・フェーズの際にデプロイされたドメインを構成できます。

注: 機密セキュリティー証明書は、デプロイメントの後に外部ファイル・サーバーから削除する必要があります。

パラメーター

表 28. 構成可能なパラメーター

パラメーター名	説明
SCP_host	`DomainZipFile.zip` ファイルを含む SCP サーバーのホスト名。
SCP_user	SCP サーバーへの接続に使用するユーザー名。

表 28. 構成可能なパラメーター (続き)

パラメーター名	説明
SCP_password	SCP サーバーへのログインに使用するパスワード。
パスワードの確認	SCP_password のユーザー入力を確認します。
SCP_zip_location	DomainZipFile.zip ファイルの URI ロケーション。たとえば、/files/DomainZipFile.zip など。
CLIENT_PUBLIC_KEY_file	DataPower Appliances XML Management Interface ポートへの接続に使用する、PEM 証明書ファイルの名前。
CLIENT_PUBLIC_KEY_password	DataPower Appliances XML Management Interface ポートへの接続に使用する、クライアント証明書のパスワード。これは、相互認証に使用可能な場合は必須です。パスワードが使用されていない場合、値を「Unset」にすることができます。
CLIENT_PRIVATE_KEY_file	DataPower Appliances XML Management Interface ポートへの接続に使用する、PEM 鍵ファイルの名前。これは相互認証に必要です。
CLIENT_PRIVATE_KEY_password	DataPower Appliances XML Management Interface ポートへの接続に使用する、鍵ファイルのパスワード。これは相互認証に必要です。パスワードが使用されていない場合、値を「Unset」にすることができます。
CLI_file	DomainZipFile.zip に含まれる CLI ファイルの名前。この CLI は、ドメインのインストールおよび WSRR サーバー構成の最後に実行されます。

SOA Policy Gateway 2.0.0.0 - SOA Policy Gateway Basic Runtime パターンのセキュリティー・スクリプト構成パラメーター

デフォルト値を持たない必須パラメーターは、パターンをデプロイする前に構成する必要があります。

表 29. 構成可能なパラメーター

パラメーター名	必須	デフォルト値	説明
SCP_host	はい		DomainZipFile.zip ファイルを含む SCP サーバーのホスト名。
SCP_user	はい		SCP サーバーへの接続に使用するユーザー名。
SCP_password	はい		SCP サーバーへのログインに使用するパスワード。
パスワードの確認	はい		SCP_password のユーザー入力を確認します。
SCP_zip_location	はい		DomainZipFile.zip ファイルの URI ロケーション。たとえば、/files/DomainZipFile.zip など。
CLIENT_PUBLIC_KEY_file	はい		DataPower Appliances XML Management Interface ポートへの接続に使用する、PEM 証明書ファイルの名前。
CLIENT_PUBLIC_KEY_password	はい		DataPower Appliances XML Management Interface ポートへの接続に使用する、クライアント証明書のパスワード。これは、相互認証に使用可能な場合は必須です。パスワードが使用されていない場合、値を「Unset」にすることができます。
CLIENT_PRIVATE_KEY_file	はい		DataPower Appliances XML Management Interface ポートへの接続に使用する、PEM 鍵ファイルの名前。これは相互認証に必要です。

表 29. 構成可能なパラメーター (続き)

パラメーター名	必須	デフォルト値	説明
CLIENT_PRIVATE_KEY_password	はい		DataPower Appliances XML Management Interface ポートへの接続に使用する、鍵ファイルのパスワード。これは相互認証に必要です。パスワードが使用されていない場合、値を「Unset」にすることができます。
CLI_file	はい	Unset	DomainZipFile.zip に含まれる CLI ファイルの名前。この CLI は、ドメインのインストールおよび WSRR サーバー構成の最後に実行されます。

SOA Policy Gateway 2.0.0.0 - SOA Policy Gateway Advanced Runtime パターンのセキュリティー・スクリプト構成パラメーター

デフォルト値を持たない必須パラメーターは、パターンをデプロイする前に構成する必要があります。

表 30. 構成可能なパラメーター

パラメーター名	必須	デフォルト値	説明
SCP_zip_location	はい		DomainZipFile.zip ファイルの URI ロケーション。たとえば、/files/DomainZipFile.zip など。
SCP_host	はい		DomainZipFile.zip ファイルを含む SCP サーバーのホスト名。
SCP_user	はい		SCP サーバーへの接続に使用するユーザー名。
SCP_password	はい		SCP サーバーへのログインに使用するパスワード。
パスワードの確認	はい		SCP_password のユーザー入力を確認します。
CLIENT_PUBLIC_KEY_file	はい		DataPower Appliances XML Management Interface ポートへの接続に使用する、PEM 証明書ファイルの名前。
CLIENT_PUBLIC_KEY_password	はい		DataPower Appliances XML Management Interface ポートへの接続に使用する、クライアント証明書のパスワード。これは、相互認証に使用可能な場合は必須です。パスワードが使用されていない場合、値を「Unset」にすることができます。
CLIENT_PRIVATE_KEY_file	はい		DataPower Appliances XML Management Interface ポートへの接続に使用する、PEM 鍵ファイルの名前。これは相互認証に必要です。
CLIENT_PRIVATE_KEY_password	はい		DataPower Appliances XML Management Interface ポートへの接続に使用する、鍵ファイルのパスワード。これは相互認証に必要です。パスワードが使用されていない場合、値を「Unset」にすることができます。
CLI_file	はい	Unset	DomainZipFile.zip に含まれる CLI ファイルの名前。この CLI は、ドメインのインストールおよび WSRR サーバー構成の最後に実行されます。

第 5 章 IBM SOA Policy Gateway Pattern による作業

IBM SOA Policy Gateway Pattern では、製品を成すトポロジーを繰り返しデプロイ可能にするためのパターン定義を提供しています。各パターンは、IBM SOA Policy Gateway Pattern 内の特定の機能を提供しており、各パターンをサポートする複数のイメージを収めています。パターンは、ビジネス・ニーズに基づいてデプロイメント前に構成する必要があります。

デプロイメント・プロセスの一環として、パートのパラメーターを構成します。詳しくは、64 ページの『パターンのデプロイ』を参照してください。

関連タスク:

11 ページの『第 3 章 IBM SOA Policy Gateway Pattern 入門』
このパターンでは、WSRR における管理されたポリシーとサービス定義を利用しつつ、WebSphere DataPower を使用してメッセージを制御します。このセクションのトピックを読めば、このシナリオで網羅される範囲、ビジネスでこのシナリオに従うのが良い理由、関係するユーザー・ロール、および本製品で提供される機能の概要を理解できます。

パターン構成およびパターン前提条件の計画

IBM SOA Policy Gateway Pattern は、サービス定義やポリシーを制御し、これらのポリシーを実施するための環境を迅速かつ高い信頼性でプロビジョンする方法を提供します。ガバナンス要件と、必要なリソースを判別します。

環境をデプロイするには、リモート管理用の DataPower アプライアンスを準備し、そのアプライアンスと安全に通信するために必要な資産を収集します。環境は、SOA Policy Gateway Basic Runtime Sample をデプロイすることによってテストできます。テストすることで、環境がデプロイメント用に適切に構成されていることを確認し、ポリシーの実施をデモンストレーションすることができます。環境の妥当性検査後に、WSRR のベスト・プラクティスを使用して、必要な IBM SOA Policy Gateway Pattern ガバナンスおよびランタイム構成が決定されます。パターンのデプロイメントは、Governance Master から始まり、次に必要な構成とマッチングする Runtime パターンが続きます。

IBM SOA Policy Gateway Pattern の準備およびデプロイ

次のようにして、DataPower を準備し、セキュリティー・ファイルを収集します。

1. リモート管理用に DataPower アプライアンスを準備します。詳しくは、55 ページの『IBM SOA Policy Gateway Pattern のための DataPower の構成』を参照してください。
2. DataPower アプライアンスが保護されている場合、 DataPower のセキュリティー・セクションを読み、そのアプライアンスとの通信に必要な DataPower セキュリティー・ファイルを収集します。
3. クラウド環境内の DataPower システムがアプライアンスと通信できること、およびアプライアンスがデプロイ済みシステムと通信できることを確認します。

実動デプロイメントを作成する前に、SOA Policy Gateway Basic Runtime Sample を使用してパターンの機能をデモンストレーションできます。 Basic Runtime Sample を使用する必要がある場合は、以下のステップを実行してください。

1. クラウド内のデプロイ済みシステムからアクセス可能な Linux 上に SCP サーバーを準備します。 SCP は、セキュア・コピー・コマンドです。 SCP サーバーは、セキュリティー構成ごとにパターンを変更する必要がなくなるように、パターンの外部のセキュリティー・ファイルをホストする方法を提供します。
2. DataPower に実装されたサンプル・アプリケーションで使用されるセキュリティー ID をホストするための LDAP サーバーを準備します。詳しくは、 63 ページの『サンプルのための LDAP の構成』を参照してください。
3. インフラストラクチャーを妥当性検査するための SOA Policy Gateway Basic Runtime Sample パターンをデプロイします。詳しくは、 65 ページの『SOA Policy Gateway Basic Runtime Sample パターンのデプロイ』を参照してください。
4. サンプルの使用を完了した後は、LDAP サーバーは不要になります。

次のようして、実動デプロイメントを準備します。

1. デプロイメントに必要なスケールを決定します。Governance Master とランタイム・デプロイメント用のクラスター・サイズを決定します。

   注: デプロイしたクラスターを、別のクラスター・メンバーで拡張することはできません。
2. Governance Master のセル名と管理ユーザー ID およびパスワードを定義します。
3. SCP サーバー上で DataPower セキュリティー `DomainZipFile.zip` ファイルをホストします。詳しくは、 56 ページの『セキュリティー `DomainZipFile.zip` の作成』を参照してください。

次のようにして実稼働環境に Governance Master をデプロイします。

1. SOA Policy Gateway Governance Master パターンをデプロイします。デプロイメントが完了するまで待ってから、実稼働環境のランタイム・パターンをデプロイします。詳しくは、 66 ページの『SOA Policy Gateway Governance Master パターンのデプロイ』を参照してください。

次のようにして実稼働環境ランタイム・パターンをデプロイします。

1. クラスター化環境とスタンドアロン環境のどちらが必要であるかを決定します。
2. 複数の DataPower ドメインが必要である場合は、 Basic Runtime パターンまたは Advanced Runtime パターンのクローンを作成して、必要な各ドメインのクローンに DataPower スクリプト・パッケージを追加します。

   注: この構成の完了後は、その他の DataPower ドメインは追加できなくなります。
   詳しくは、 73 ページの『複数の DataPower ドメインを伴うデプロイ』を参照してください。
3. Governance Master パターン情報を使用して、ランタイム・パターンを構成します。詳しくは、 67 ページの『SOA Policy Gateway Governance Master デプロイメント情報』を参照してください。

4. ランタイムをステージング、実動、またはその他のいずれにするかを決定します。
5. Basic Runtime パターンまたは Advanced Runtime パターンをデプロイします。詳しくは、 69 ページの『SOA Policy Gateway Advanced Runtime パターンのデプロイ』または 68 ページの『SOA Policy Gateway Basic Runtime パターンのデプロイ』を参照してください。
6. 完全にデプロイされるまで待ってから、別のランタイムをデプロイしてください。

.

ランタイムのデプロイメントが完了すると、以下のようになります。

1. SCP ファイル・サーバーは不要になります。
2. WSRR および WebSphere セキュリティーをデフォルト・セキュリティー構成から更新できるようになります。詳しくは、 56 ページの『セキュリティー管理』を参照してください。
3. DataPower ドメインでゲートウェイ構成の準備が整いました。

IBM SOA Policy Gateway Pattern のための DataPower の構成

SOAPolicy スクリプトを実行する前に、以下の DataPower 構成ステップを実行してください。

手順

1. サポートされている DataPower アプライアンスに、管理者としてログインします。
2. 「XML 管理インターフェース (XML Management Interface)」を検索します。
3. 状態が有効になっていることを確認します。
4. 以下のものがアクティブで、正しく保護されていることを確認します。
   - SOAP 管理 URI
   - SOAP 構成管理
   - SOAP 構成管理 (v2004)
   - AMP エンドポイント
   - SLM エンドポイント
   - WS-Management エンドポイント
   - WSDM エンドポイント
   - UDDI サブスクリプション
   - WSRR サブスクリプション

IBM SOA Policy Gateway Pattern パターンのセキュリティー

顧客は、WSRR と DataPower の間で、さまざまなレベルのセキュリティー (特に、SSL のエリア) を必要とします。 SOA Policy Gateway Basic Runtime、SOA Policy Gateway Basic Runtime Sample、および SOA Policy Gateway Advanced Runtime の各パターンを使用している場合、IBM SOA Policy Gateway Pattern は構成スクリプトと DataPower の間で 3 つのレベルの SSL 通信をサポートします。

SSL が必須ではない場合

SSL の使用が必須ではない場合、curl クライアントの公開鍵と秘密鍵は指定されず、「Unset」のままになります。

注: SSL が使用されない場合、DataPower に送信されるすべてのデータは、ユーザーおよびパスワード情報も含めていずれも暗号化されません。これは、セキュリティーのぜい弱性を表します。 DataPower に対する SOMA 呼び出しで使用されるパスワードでは暗号化がサポートされていないため、暗号化されないまま DataPower アプライアンスにトランスポートされます。したがって、最小限のセキュリティーを確保するためにサーバー・サイド認証が使用されます。

DataPower アプリケーションと Basic/Advanced パターン内のスクリプトとの間の相互認証

DataPower アプリケーションと、Basic パターンおよび Advanced パターンに含まれるスクリプトとの間で相互認証を行う必要がある場合:

- curl クライアントの公開鍵および秘密鍵の指定が必須です。

セキュリティー管理

パターンで使用される WSRR イメージと WebSphere Application Server イメージには、デフォルト・セキュリティーのみが設定されています。真にセキュアな環境を生成するには、これらを標準の WebSphere セキュリティー技法で保護する必要があります。

以下のリンクから、WebSphere Network Deployment バージョン 8.0 のインフォメーション・センターを参照してください。

- WebSphere Application Server, Network Deployment (分散プラットフォームおよび Windows) バージョン 8.0: IBM WebSphere Application Server, Network Deployment (分散プラットフォームおよび Windows) バージョン 8.0 インフォメーション・センター
- アプリケーション・セキュリティー: IBM WebSphere Application Server, Network Deployment (分散プラットフォームおよび Windows) バージョン 8.0 インフォメーション・センター - アプリケーションとその環境の保護
- セキュリティーのエンドツーエンド・パス: IBM WebSphere Application Server, Network Deployment (分散プラットフォームおよび Windows) バージョン 8.0 インフォメーション・センター - アプリケーションとその環境の保護

セキュリティー DomainZipFile.zip の作成

セキュリティー `DomainZipFile.zip` を、SOA Policy Gateway Basic Runtime パターン、SOA Policy Gateway Advanced Runtime パターン、および SOA Policy Gateway Basic Runtime Sample のために作成します。

手順

次のルールを使用して `DomainZipFile.zip` を作成します。

1. `DomainZipFile.zip` の構造は次のようでなければなりません。

注: ディレクトリー構造のみが要求されており、個々のファイルには任意の名前を付けることができます。ただし、証明書と鍵ファイルは、すべて PEM 形式である必要があります。

注: DataPower のホスト名をパスに使用すると、DataPower アプライアンスごとに別の証明書を使用できます。

表 31. 基本パターンと拡張パターンに必要なファイル

ファイル名とルート・ディレクトリーに相対的なロケーション	注
CurlClientPublicKeyFile.crt	相互認証が使用されている場合にのみ必要です。 PEM 形式のみ。
CurlClientPrivateKeyFile.key	相互認証が使用されている場合にのみ必要です。
/*dataPowerHostName*/certificate1.crt	WSRR にアップロードされる DataPower 証明書。証明書チェーン全体が PEM 形式でなければなりません。WSRR にアップロードされる DataPower 証明書。以下の内容のみが含まれていなければなりません。 ------BEGINCERTIFICATE---- to -----END CERTIFICATE----- ファイル拡張子は、.crt または .pem でなければなりません。
/*dataPowerHostName*/certificate2.crt	ファイル拡張子は、.crt または .pem でなければなりません
/*dataPowerHostName*/certificate3.crt	ファイル拡張子は、.crt または .pem でなければなりません

2. SOA Policy Gateway Advanced Runtime パターンの場合のみ、実行される cli ファイルを追加します (オプション)。

表 32. 拡張パターンに必要な追加ファイル

ファイル名とルート・ディレクトリーに相対的なロケーション	注
/cli.cli	DataPower ドメイン構成の最後に実行される単一の CLI ファイル

3. DomainZipFile.zip は SCP サーバー・ロケーションに配置します。 ファイルが機密情報を含んでいるため、構成の終了後に削除することをお勧めします。パターン構成スクリプトは、DomainZipFile.zip から取得したファイル、および SCP 環境から SCP を使用して作成された DomainZipFile.zip のコピーを削除します。
4. 次の SCP サーバーの情報のメモを取ります。
   - SCP のホスト名
   - DomainZipFile.zip への SCP のパス
   - SCP のユーザーとパスワード

DomainZipFile ファイルの使用

パターンにおける各種レベルのセキュリティーごとに、DomainZipFile ファイルのユース・ケースを示します。

DomainZipFile.zip ファイルは Basic Runtime、Basic Runtime Sample、および Advanced Runtime パターンで使用できます。

SSL は、パターン・スクリプト・パッケージを DataPower アプライアンスに接続する上で必須ではありません。SSL を使用しない場合は、パターンによって作成された DataPower ドメインをカスタマイズするために cli スクリプトを必要としない限り、DomainZipFile.zip ファイルを作成する必要はありません。この場合、最低でもサーバー認証を使用しないなら、データは暗号化されません。こうすると、クライアントのスクリプティング中にユーザーとパスワードの情報が DataPower に HTTP 接続上で渡されるため、セキュリティー・リスクとなります。それらは、DomainZipFile.zip ファイル内の証明書によって保護されます。

クライアント証明書の妥当性検査を行うように DataPower ホストを構成していない場合は、スクリプト・クライアントと DataPower アプライアンスとの間で相互認証を使用する必要はありません。最低限、サーバー認証の使用が推奨されています。

このトピックのケース・シナリオでは、各種レベルのセキュリティーが扱われます。

本製品は、以下のケース・シナリオをサポートしています。

ケース 1: SSL は不要

ケース 2: SSL は不要だが、ドメインのカスタマイズのために cli スクリプトが必要

ケース 3: スクリプト・クライアントによる DataPower 証明書のサーバー認証が必要

ケース 4: DataPower アプライアンスによる相互認証が必要

ケース 1: SSL は不要

略述したセキュリティー上の理由により、このオプションは開発シナリオのみで使用することをお勧めします。SSL を使用しない場合は、以下を行います。

1. SCP_host のパラメーターを 『Unset』 に設定します。Basic Runtime または Advanced Runtime パターンを使用している場合、SCP_host は SOA Policy Gateway 2.0.0.0 - Security パッケージ・スクリプトにあります。Basic Runtime Sample パターンを使用している場合、SCP_host は SOA Policy Gateway 2.0.0.0 スクリプトにあります。これにより、パターン内のスクリプトは、SCP を使用して DomainZipFile.zip ファイルを取得しないように設定されます。
2. ステップ 1 と同じスクリプト・パッケージで、以下のパラメーターを 『Unset』 に設定します。
   - CLIENT_PUBLIC_KEY_file
   - CLIENT_PUBLIC_KEY_password
   - パスワードの確認
   - CLIENT_PRIVATE_KEY_file
   - CLIENT_PRIVATE_KEY_password
   - パスワードの確認

ケース 2: SSL は不要だが、ドメインのカスタマイズのために cli スクリプトが必要

略述したセキュリティー上の理由により、このオプションは開発シナリオのみで使用することをお勧めします。SSL を使用しないものの、cli スクリプトが必要な場合は、以下を行います。

1. SCP_host のパラメーターを 『Unset』 に設定します。Basic または Advanced Runtime パターンを使用している場合、SCP_host は SOA Policy Gateway 2.0.0.0 - Security パッケージ・スクリプトにあります。Basic Runtime Sample パターンを使用している場合、SCP_host は SOA Policy Gateway 2.0.0.0 スクリプトにあります。これにより、パターン内のスクリプトは、SCP を使用して DomainZipFile.zip ファイルを取得しないように設定されます。
2. ステップ 1 と同じスクリプト・パッケージで、以下のパラメーターを Unset に設定します。
   - CLIENT_PUBLIC_KEY_file
   - CLIENT_PUBLIC_KEY_password
   - パスワードの確認
   - CLIENT_PRIVATE_KEY_file
   - CLIENT_PRIVATE_KEY_password
   - パスワードの確認

   注: SCP_host が 『Unset』 の場合、Basic Runtime および Advanced Runtime パターンで実行する cli スクリプトがない限り、DomainZipFile.zip ファイルは不要です。
3. 使用する cli スクリプト・ファイルを、DomainZipFile.zip ファイルのルートに置きます。 DomainZipFile.zip ファイルの構造の例を以下に示します。

   ```
   /cli.cli
   ```

   このファイルは、DataPower Domain スクリプト・パッケージの最後で実行されます。cli.cli は、ファイル名の例です。ファイル名にスペースを含めることはできません。

ケース 3: スクリプト・クライアントによる DataPower 証明書のサーバー認証が必要

XML Management Interface を保護する DataPower 証明書チェーンの全証明書を含める必要があります。これらを見つけるには、以下のステップを実行します。

1. XML Management Interface の SSL プロキシー・プロファイルを調べて、暗号プロファイルを見つけます。暗号プロファイルには、XML Management Interface の保護に使用する証明書が含まれる、識別資格情報が入ります。
2. 以下の証明書を DomainZipFile.zip ファイルに追加します。

   形式は次のとおりです。
   - dataPowerHostName/certificateChainMember1.crt
   - dataPowerHostName/certificateChainMember2.pem
   - dataPowerHostName/certificateChainMember(n).crt

マルチドメイン・シナリオを使用する場合は、同ファイルに、2 つの異なる dataPowerHostName ディレクトリーを含め、DataPower 証明書チェーンごとに以下のようなファイルを追加することができます。

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

注: DataPower 証明書チェーン・ファイルは、タイプが .crt または .pem で、証明書そのものだけが入っていなければなりません。ここで使用されている .crt または .pem ファイルの名前は例です。ファイル名にスペースを含めることはできません。

3. オプション: サーバー認証のみを、Basic Runtime および Advanced Runtime パターンによって使用される SOA Policy Gateway 2.0.0.0 - Security パッケージ・スクリプトで、または Basic Runtime Sample パターンの SOA Policy Gateway 2.0.0.0 - Sample スクリプトで必要とする場合は、それらのスクリプトに含まれる以下のパラメーターの値として 『Unset』 を使用してください。
   - CLIENT_PUBLIC_KEY_file
   - CLIENT_PUBLIC_KEY_password
   - パスワードの確認
   - CLIENT_PRIVATE_KEY_file
   - CLIENT_PRIVATE_KEY_password
   - パスワードの確認
4. オプション: cli スクリプトが必要な場合は、以下を行います。

   使用する cli スクリプト・ファイルを、DomainZipFile.zip ファイルのルートに置きます。 DomainZipFile.zip ファイルの構造の例を以下に示します。

   ```
   /cli.cli
   ```

   このファイルは、DataPower Domain スクリプト・パッケージの最後で実行されます。cli.cli は、ファイル名の例です。ファイル名にスペースを含めることはできません。

ケース 4: DataPower アプライアンスによる相互認証が必要

このケースでは、クライアントと DataPower サーバーが、互いの証明書の妥当性検査を行う必要があります。これが必要になるのは、XML Management Interface の SSL プロキシー・プロファイルで DataPower ホストが、クライアントの証明書を妥当性検査するように構成されている場合のみです。

1. 以下の証明書を DomainZipFile.zip ファイルに追加します。

   形式は次のとおりです。

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

注: DataPower 証明書チェーン・ファイルは、タイプが `.crt` または `.pem` で、証明書そのものだけが入っていなければなりません。ここで使用されている `.crt` または `.pem` ファイルの名前は例です。ファイル名にスペースを含めることはできません。

クライアント証明書ファイルおよびクライアント鍵ファイルでは、証明書ファイルまたは鍵ファイルのデータを、ファイル内の次のように示された行の前に配置することができます。`-----BEGIN CERTIFICATE-----`。

2. オプション: サーバー認証を、Basic Runtime および Advanced Runtime パターンによって使用される SOA Policy Gateway 2.0.0.0 - Security パッケージ・スクリプトで、または Basic Runtime Sample パターンの SOA Policy Gateway 2.0.0.0 - Sample スクリプトで必要とする場合は、それらのスクリプトに含まれる以下のパラメーターの値として 『Unset』 を使用してください。
   - CLIENT_PUBLIC_KEY_file
   - CLIENT_PRIVATE_KEY_file
   - CLIENT_PRIVATE_KEY_password
   - パスワードの確認
3. 公開鍵ファイルのパスワードがない場合は、以下の値として 『Unset』 を指定できます。
   - CLIENT_PUBLIC_KEY_password
   - パスワードの確認
4. スクリプト・パッケージによって使用される curl コマンドは、ファイル・タイプが `.pem` であることを前提としているため、**--key-type** と **--cert-type** はデフォルトで PEM に設定されます。証明書ファイルおよび鍵ファイルでは、この内容を、特定の証明書ファイルまたは鍵ファイル内の `-----BEGIN CERTIFICATE-----` の前に配置できます。
5. オプション: cli スクリプトが必要な場合 (Basic Runtime または Advanced Runtime パターンを使用) は、以下を行います。

   使用する cli スクリプト・ファイルを、`DomainZipFile.zip` ファイルのルートに置きます。 `DomainZipFile.zip` ファイルの構造の例を以下に示します。

   ```
   /cli.cli
   ```

   このファイルは、DataPower Domain スクリプト・パッケージの最後で実行されます。`cli.cli` は、ファイル名の例です。ファイル名にスペースを含めることはできません。

ケースを選択することにより、DomainZipFile.zip ファイルを使用または不使用で、適切なレベルのセキュリティーが構成されました。

WSRR にアップロードする DataPower 証明書

DomainZipFile.zip ファイルの dataPowerHostName ディレクトリーに、証明書のディレクトリーを提供できます。これは WSRR Dmgr サーバーまたは WSRR Standalone サーバーにアップロードできます。

独自の手段で行う DomainZipFile.zip ファイルのダウンロード

セキュリティー・スクリプト・パッケージで SCP サーバーを使用せずに、独自の DomainZipFile.zip を備えることができます。

手順

他の手段でこのファイルをご使用の環境に配置するには、以下を実行する必要があります。

1. **SCP_host** パラメーターを Unset に設定する必要があります。
2. SOA Gateway パターン・スクリプトの実行前に、カスタム・スクリプト・パッケージを作成して、DomainZipFile.zip を /tmp ディレクトリーに作成する必要があります。
3. Advanced パターンの場合、DomainZipFile.zip ファイルを /tmp/security/RetrieveDomainFiles ディレクトリーに作成します。
4. サンプル付きの Basic パターンの場合、DomainZipFile.zip ファイルを /installSample/Retrieve_Domain_Files ディレクトリーに作成します。

   注: DomainZipFile.zip ファイルがない場合、証明書または鍵を使用することがパラメーターで指定されているなら、スクリプトが失敗する可能性があります。

証明書の CN 値

DomainZipFile.zip ファイルの一部として提供される証明書においては、その証明書内の CN 値を考慮する必要があります。

SSL を使用するように選択するとホスト名検証は常にアクティブになるので、スクリプト・パッケージで証明書が使用される場合は以下を考慮に入れる必要があります。

- クライアント証明書 (公開および秘密/鍵) では、スクリプトを実行する WSRR Server や WSRR Dmgr のホストを正確に知る方法はありません。そのため、CN 値は IBM Workload Deployer 環境内で可能性のあるすべてのクライアント・ホスト上で実行できるように汎用的でなければなりません。例えば、*clientname*.yourcompany.com のようにします。
- DataPower マシンの証明書は、DomainZipFile.zip ファイル内の個別のディレクトリーです。例:

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

- 証明書 (DataPower ホストのチェーンにある最後のホスト) の CN 値は、そのホスト名として有効なものでなければなりません。例えば、dp1.yourcompany.com や *dp*.yourcompany.com とします。

サンプルのための LDAP の構成

サンプルでは、いくつかの特定の項目が設定された Lightweight Directory Access Protocol (LDAP) が必要です。

このタスクについて

LDAP を構成する際に、エレメントとプロパティーを定義する必要があります。

注: これらのパスワードを変更しないでください。

手動構成ステップの代わりに、このタスクに示された構成の詳細を含む 2 つの LDIF ファイルが入っている、以下の `.zip` ファイルの内容を解凍し、それらのファイルを使用して LDAP サーバーを更新することができます。soaSamples.zip。

手順

次のエレメントを持つ LDAP を作成します。

1. サフィックスを定義します。

```
dc=ibm.com
```

2. 次のプロパティーを使用して、ドメイン `dc=ibm.com` を定義します。

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

3. コンテナーを定義します。
   a. コンテナー・グループを定義します。

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

   b. コンテナー・ユーザーを定義します。

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

4. 次のユーザーを定義します。
   a. 以下のプロパティーを持つユーザー ConsumerA

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

   b. 以下のプロパティーを持つユーザー ConsumerB

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

   c. 以下のプロパティーを持つユーザー ConsumerX

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

5. 次のグループを定義します。
   a. 以下のプロパティーを持つグループ MANAGER を定義します。

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

   b. 以下のプロパティーを持つグループ Clerk を定義します。

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

   c. 以下のプロパティーを持つグループ Customer を定義します。

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

6. サンプルを実行する前に、LDAP に関する次の情報を収集してください。
   - 識別名 (DN) (`cn=root` など)。
   - パスワード (`passw0rd` など)。
   - 非セキュアなポート (389 など)。
   - LDAP ホスト名 (`ldap.customer.com` など)。

パターンのデプロイ

IBM Workload Deployer 3.1.0.2 または IBM SOA Policy Gateway Pattern によってパターンをクラウドにデプロイすると、稼働する IBM PureApplication System 環境を実現できます。 IBM SOA Policy Gateway Pattern イメージに用意された定義済みのパターンをデプロイするか、または自分で作成したパターンをデプロイすることができます。

始める前に

パターンをデプロイするにはまず、必要なパートがすべて構成された、定義済みのパターン、または完成した新しいパターンを用意する必要があります。

このタスクについて

パターンをデプロイすると、クラウドで稼働する仮想システム、すなわち新規にプロビジョンされた IBM SOA Policy Gateway Pattern ランタイム環境が作成されます。

手順

プライベート・クラウドで稼働させるために IBM SOA Policy Gateway Pattern をデプロイするには、以下のステップを実行します。

1. 「仮想システム・パターン」ウィンドウ内のパターンのリストから、デプロイするパターンを選択します。
2. 「**デプロイ**」アイコンをクリックします。
3. パターンをデプロイするために必要なフィールドに入力します。 ウィンドウ内で、仮想システムの名前と、その他の必要な情報を入力してください。各アイテムの横のチェック・マークは、それ以上の構成は必要ないことを示します。 構成するパートのパラメーターは、パターンをデプロイする前に変更できます。これを行うには、パート名をクリックして、パート用のエディターを開きます。必要とされる順序で仮想マシンが作成され、続いて始動します。

タスクの結果

デプロイメント・プロセスにより、定義されたパートの仮想マシンが作成されて始動し、必要なコンソールへのリンクが設定されます。デプロイメントの時間は、デプロイするパターンの複雑度に応じて異なります。デプロイされたパターンは、仮想システム、すなわち新規にプロビジョンされた IBM SOA Policy Gateway Pattern ランタイム環境です。

次のタスク

「仮想システム・インスタンス」ウィンドウから、インスタンスの状況を表示して、デプロイメントの完了を確認し、管理を開始することができます。

関連情報:

IBM Workload Deployer: 仮想システム・パターンの管理

IBM PureApplication System: 仮想システム・パターンの管理

SOA Policy Gateway Basic Runtime Sample パターンのデプロイ

SOA Policy Gateway Basic Runtime Sample パターンをデプロイすると、稼働する、そのパターンの仮想システム・インスタンスが作成されます。

始める前に

パターンをデプロイする前に、以下の前提条件を満たす必要があります。

- サンプルのために DataPower を構成します。 55 ページの『IBM SOA Policy Gateway Pattern のための DataPower の構成』を参照してください。
- サンプルのためにセキュリティーを構成します。 55 ページの『IBM SOA Policy Gateway Pattern パターンのセキュリティー』を参照してください。
- セキュリティー・ファイルをホストするために SCP サーバーをセットアップします。
- サンプルのために LDAP を構成します。 63 ページの『サンプルのための LDAP の構成』を参照してください。

このタスクについて

パターンをデプロイすると、クラウドで稼働する仮想システム・インスタンスが作成されます。

手順

SOA Policy Gateway Basic Runtime Sample パターンをデプロイするには、以下のステップを実行します。

1. 「**パターン**」 > 「**仮想システム**」をクリックします。
2. 仮想システム・パターンのリストから、「**SOA Policy Gateway 2.0.0.0 - Basic Runtime Sample**」を選択します。
3. 「デプロイ」アイコンをクリックします。
4. パターンをデプロイするために必要なフィールドに入力します。 各アイテムの横のチェック・マークは、それ以上の構成は必要ないことを示します。
   a. 「**仮想システム名**」ボックスで、インスタンス用の固有の名前を入力します。
   b. 仮想パターンを構成します。 「**仮想パートの構成**」をクリックしてから、パート名をクリックして、パートとスクリプトのためのエディターを開きます。

      注: このパターンにおけるパスワードはすべて (DataPower_admin_id パラメーターは除く)、デフォルトで `password` となります。

      - 29 ページの『SOA Policy Gateway Basic Runtime Sample パターンの DB2 Enterprise パーツ構成パラメーター』.
      - 38 ページの『SOA Policy Gateway Basic Runtime Sample パターンの WSRR スタンドアロン・サーバー・パーツ構成パラメーター』
      - 48 ページの『SOA Policy Gateway 2.0.0.0 - SOA Policy Gateway Basic Runtime Sample パターンのサンプル・スクリプト構成パラメーター』
5. 「**OK**」をクリックしてパターンをデプロイします。

次のタスク

デプロイメントを検証するには、71 ページの『デプロイメントの検証』を参照してください。

SOA Policy Gateway Governance Master パターンのデプロイ

SOA Policy Gateway Governance Master パターンをデプロイすると、稼働する、そのパターンの仮想システム・インスタンスが作成されます。

このタスクについて

パターンをデプロイすると、クラウドで稼働する仮想システム・インスタンスが作成されます。

手順

SOA Policy Gateway Governance Master パターンをデプロイするには、以下のステップを実行します。

1. 「**パターン**」 > 「**仮想システム**」をクリックします。
2. 仮想システム・パターンのリストから、「**SOA Policy Gateway 2.0.0.0 - Governance Master**」を選択します。
3. 「デプロイ」アイコンをクリックします。
4. パターンをデプロイするために必要なフィールドに入力します。 各アイテムの横のチェック・マークは、それ以上の構成は必要ないことを示します。
   a. 「**仮想システム名**」ボックスで、インスタンス用の固有の名前を入力します。
   b. 仮想パターンを構成します。 「**仮想パートの構成**」をクリックしてから、パート名をクリックして、パート用のエディターを開きます。
      - 32 ページの『SOA Policy Gateway Governance Master パターンの DB2 Enterprise HADR Primary パーツ構成パラメーター』
      - 39 ページの『SOA Policy Gateway Governance Master パターンの WSRR デプロイメント・マネージャー・パーツ構成パラメーター』
      - 41 ページの『SOA Policy Gateway Governance Master パターンの WSRR カスタム・ノード・パーツ構成パラメーター』
      - 35 ページの『SOA Policy Gateway Governance Master パターンの DB2 Enterprise HADR Standby パーツ構成パラメーター』
5. 「**OK**」をクリックしてパターンをデプロイします。

次のタスク

デプロイメントを検証するには、71 ページの『デプロイメントの検証』を参照してください。

SOA Policy Gateway Governance Master デプロイメント情報

Governance Master は、SOA Policy Gateway Basic Runtime または SOA Policy Gateway Advanced Runtime パターンのデプロイより前にデプロイする必要があります。

このタスクについて

Governance Master インスタンスのデプロイメント情報は、ランタイム・パターンのデプロイメント値への入力として必要です。

手順

必要な値を Governance Master インスタンスで見つけるには、以下を行います。

1. 「**インスタンス**」 > 「**仮想システム**」とナビゲートします。
2. デプロイメント Governance Master インスタンスを選択します。
3. 「**仮想マシン**」を展開します。
4. ***WSRRDMGR*** という名前の仮想マシンを展開します。
5. 以下の点に注意してください。

- 「**ハードウェアおよびネットワーク**」セクションで、ホスト名と IP アドレスを確認します。ホスト名は「**ネットワーク・インターフェース 0**」の値です。
- 「**WebSphere 構成**」セクションで、セル名を確認します。

注: Governance Master インスタンスのデプロイメント時に使用された、ホスト名または IP、セル名、および WebSphere 管理ユーザー名とパスワードは、SOA Policy Gateway Basic Runtime または SOA Policy Gateway Advanced Runtime パターンにおける以下のパラメーターに必要な入力です。

- WSRR_GOV_DMGR_hostname
- WSRR_GOV_DMGR_cellname
- WSRR_GOV_admin_user
- WSRR_GOV_admin_password

SOA Policy Gateway Basic Runtime パターンのデプロイ

SOA Policy Gateway Basic Runtime パターンをデプロイすると、稼働する、そのパターンの仮想システム・インスタンスが作成されます。

始める前に

Basic Runtime パターンをデプロイする前に、以下を実行してください。

- IBM SOA Policy Gateway Pattern のために DataPower を構成します。55 ページの『IBM SOA Policy Gateway Pattern のための DataPower の構成』を参照してください。
- IBM SOA Policy Gateway Pattern のためにセキュリティーを構成します。55 ページの『IBM SOA Policy Gateway Pattern パターンのセキュリティー』を参照してください。
- セキュリティー・ファイルをホストするために SCP サーバーをセットアップします。
- Governance Master デプロイメント情報を取得します。67 ページの『SOA Policy Gateway Governance Master デプロイメント情報』を参照してください。

このタスクについて

パターンをデプロイすると、クラウドで稼働する仮想システム・インスタンスが作成されます。

注: ガバナンス有効化プロファイル (GEP) を使用している場合は、SOA Policy Gateway Basic Runtime パターンまたは SOA Policy Gateway Advanced Runtime パターンでステージング環境と実動環境を同時にデプロイできません。これは、プロモーション・プロパティーの構成プロセス中に競合が発生してしまうためです。最初にステージング環境をデプロイした後に、実動環境をデプロイしてください。

手順

SOA Policy Gateway Basic Runtime パターンをデプロイするには、以下のステップを実行します。

1. 「**パターン**」 > 「**仮想システム**」をクリックします。

2. 仮想システム・パターンのリストから、「**SOA Policy Gateway Basic Runtime 2.0.0.0**」を選択します。
3. 「デプロイ」アイコンをクリックします。
4. パターンをデプロイするために必要なフィールドに入力します。 各アイテムの横のチェック・マークは、それ以上の構成は必要ないことを示します。
   a. 「**仮想システム名**」ボックスで、インスタンス用の固有の名前を入力します。
   b. 仮想パターンを構成します。 「**仮想パートの構成**」をクリックしてから、パート名をクリックして、パートとスクリプトのためのエディターを開きます。
      - 28 ページの『SOA Policy Gateway Basic Runtime パターンの DB2 Enterprise パーツ構成パラメーター』
      - 37 ページの『SOA Policy Gateway Basic Runtime パターンの WSRR スタンドアロン・サーバー・パーツ構成パラメーター』
      - 50 ページの『SOA Policy Gateway 2.0.0.0 - SOA Policy Gateway Basic Runtime パターンのセキュリティー・スクリプト構成パラメーター』
      - 45 ページの『SOA Policy Gateway 2.0.0.0 - SOA Policy Gateway Basic Runtime パターンのプロモーション・スクリプト構成パラメーター』
      - 43 ページの『SOA Policy Gateway 2.0.0.0 - SOA Policy Gateway Basic Runtime パターンの DataPower Domain スクリプト構成パラメーター』
5. 「**OK**」をクリックしてパターンをデプロイします。

次のタスク

デプロイメントを検証するには、71 ページの『デプロイメントの検証』を参照してください。

SOA Policy Gateway Advanced Runtime パターンのデプロイ

SOA Policy Gateway Advanced Runtime パターンをデプロイすると、稼働する、そのパターンの仮想システム・インスタンスが作成されます。

始める前に

Advanced Runtime パターンをデプロイする前に、以下を実行してください。

- IBM SOA Policy Gateway Pattern のために DataPower を構成します。 55 ページの『IBM SOA Policy Gateway Pattern のための DataPower の構成』を参照してください。
- IBM SOA Policy Gateway Pattern のためにセキュリティーを構成します。 55 ページの『IBM SOA Policy Gateway Pattern パターンのセキュリティー』を参照してください。
- セキュリティー・ファイルをホストするために SCP サーバーをセットアップします。
- Governance Master デプロイメント情報を取得します。 67 ページの『SOA Policy Gateway Governance Master デプロイメント情報』を参照してください。

このタスクについて

パターンをデプロイすると、クラウドで稼働する仮想システム・インスタンスが作成されます。

注: ガバナンス有効化プロファイル (GEP) を使用している場合は、SOA Policy Gateway Basic Runtime パターンまたは SOA Policy Gateway Advanced Runtime パターンでステージング環境と実動環境を同時にデプロイできません。これは、プロモーション・プロパティーの構成プロセス中に競合が発生してしまうためです。最初にステージング環境をデプロイした後に、実動環境をデプロイしてください。

手順

SOA Policy Gateway Advanced Runtime パターンをデプロイするには、以下のステップを実行します。

1. 「**パターン**」 > 「**仮想システム**」をクリックします。
2. 仮想システム・パターンのリストから、「**SOA Policy Gateway 2.0.0.0 - Advanced Runtime**」を選択します。
3. 「デプロイ」アイコンをクリックします。
4. パターンをデプロイするために必要なフィールドに入力します。 各アイテムの横のチェック・マークは、それ以上の構成は必要ないことを示します。
   a. 「**仮想システム名**」ボックスで、インスタンス用の固有の名前を入力します。
   b. オプション: 環境を選択し、デプロイメントをスケジュールします。
   c. 仮想パターンを構成します。 「**仮想パートの構成**」をクリックしてから、パート名をクリックして、パートとスクリプトのためのエディターを開きます。
      - 31 ページの『SOA Policy Gateway Advanced Runtime パターンの DB2 Enterprise HADR Primary パーツ構成パラメーター』
      - 39 ページの『SOA Policy Gateway Advanced Runtime パターンの WSRR デプロイメント・マネージャー・パーツ構成パラメーター』
      - 51 ページの『SOA Policy Gateway 2.0.0.0 - SOA Policy Gateway Advanced Runtime パターンのセキュリティー・スクリプト構成パラメーター』
      - 46 ページの『SOA Policy Gateway 2.0.0.0 - SOA Policy Gateway Advanced Runtime パターンのプロモーション・スクリプト構成パラメーター』
      - 44 ページの『SOA Policy Gateway 2.0.0.0 - SOA Policy Gateway Advanced Runtime パターンの DataPower Domain スクリプト構成パラメーター』
      - 41 ページの『SOA Policy Gateway Advanced Runtime パターンの WSRR カスタム・ノード・パーツ構成パラメーター』
      - 34 ページの『SOA Policy Gateway Advanced Runtime パターンの DB2 Enterprise HADR Standby パーツ構成パラメーター』
5. 「**OK**」をクリックしてデプロイします。

次のタスク

デプロイメントを検証するには、『デプロイメントの検証』を参照してください。

デプロイメントの検証

パターンをデプロイしたら、正常にデプロイメントされたかどうかを検証します。

手順

1. 仮想システムのデプロイメント履歴で、障害がないかどうかデプロイメント・ログを調べます。詳しくは、 117 ページの『デプロイメントの問題のトラブルシューティング』を参照してください。
2. オプション: SOA Policy Gateway Basic Runtime Sample をデプロイした場合は、チュートリアルにしたがって、用意されたサンプル・アプリケーションを使用してサンプル・メッセージをいくつか送信することで、デプロイ済みのインスタンスをテストします。 76 ページの『サンプル・テスト・ケースの実行』を参照してください。

シナリオ: パターンにさらにランタイムを追加する

ガバナンス有効化プロファイルには、開発、テスト、ステージング、および実動という 4 つの個別の環境を含む、事前定義された環境分類システムが備わっています。

このタスクについて

ステージング環境および実動環境は、サービス・バージョンなどのケイパビリティー・バージョンのライフサイクルを定義する SOA ライフサイクルでも体系化されています。つまり、ステージング環境および実動環境に固有の状態および遷移があるので、プロモーション構成ファイルにターゲット・システムを定義することにより、これらのランタイムへの制御されたプロモーションが可能になります。これは、ケイパビリティー・バージョンを汎用向けに公開する前にテストできるようステージング環境が実動環境の前にくるような環境を、組織が同じように定義する場合に適切です。ただし、多くの組織では追加の環境が必要となるので、それらの相違に対応するためにプロファイルの修正が必要です。このセクションでは、新しいランタイム環境を WSRR ガバナンス有効化プロファイルに追加する 1 つの方法を説明します。

デプロイメント環境の計画について詳しくは、 53 ページの『パターン構成およびパターン前提条件の計画』を参照してください。

手順

1. 事前定義された SOA Policy Gateway Governance Master をデプロイします。詳しくは、 66 ページの『SOA Policy Gateway Governance Master パターンのデプロイ』を参照してください。
2. オプション: WSRR ガバナンス有効化プロファイルを変更します。詳しくは、IBM WebSphere Service Registry and Repository バージョン 8.0 インフォメーション・センター - チュートリアル: ランタイム環境のカスタマイズを参照してください。

3. Governance Master に関する詳細を使用して、SOA Policy Gateway Basic Runtime または SOA Policy Gateway Advanced Runtime パターンを構成します。詳しくは、67 ページの『SOA Policy Gateway Governance Master デプロイメント情報』を参照してください。

   注: プロモーション環境値を 『Unset』 に設定する必要があります。
4. 事前定義された SOA Policy Gateway Basic Runtime または SOA Policy Gateway Advanced Runtime をデプロイします。詳しくは、68 ページの『SOA Policy Gateway Basic Runtime パターンのデプロイ』および 69 ページの『SOA Policy Gateway Advanced Runtime パターンのデプロイ』を参照してください。

IBM SOA Policy Gateway Pattern の複製とカスタマイズ

IBM SOA Policy Gateway Pattern は編集できません。IBM SOA Policy Gateway Pattern 仮想システム・パターンに用意されたトポロジーでは必要な機能が得られない場合は、パターンを複製してから、編集して新しいパターンを作成することができます。

このタスクについて

以下の方法でパターンをカスタマイズできます。

- さらに DataPower ドメインを追加する。詳しくは、73 ページの『複数の DataPower ドメインを伴うデプロイ』を参照してください。
- デフォルトのクラスター・サイズを大きくする。詳しくは、IBM Workload Deployer バージョン 3.1 インフォメーション・センターを参照してください。

  注: クラスター・サイズを拡張する際は、WSRR デプロイメント・マネージャーのメモリー・サイズも引き上げてください。
- サーバーで圧縮セキュリティー・ファイルを取得する方法を選択可能。詳しくは、56 ページの『セキュリティー管理』を参照してください。
- 独自のデフォルト値の定義とロックが可能 (DataPower 管理者 ID など)。パラメーターのロックについて詳しくは、IBM Workload Deployer バージョン 3.1 インフォメーション・センターを参照してください。
- 独自の手段で `DomainZipFile.zip` ファイルをダウンロード可能。詳しくは、62 ページの『独自の手段で行う `DomainZipFile.zip` ファイルのダウンロード』を参照してください。

手順

パターンを複製して編集し、新しいパターンを作成するには、以下のステップを実行します。

1. 「パターン」ウィンドウの左パネルで、複製するパターンを選択します。
2. 複製アイコンをクリックし、新しいパターンの名前を指定します。説明など、付加的な情報を設定することもできます。
3. 新しいパターンを選択し、編集アイコンをクリックして構成を変更します。パートの追加および削除とその構成を行ったり、いくつかのパートの数を増加または減少させたり、いくつかのパートをデプロイする順序を変更したりできます。

次のタスク

作成したパターンのタイプのために、必要なパートがすべて適切に構成されていることを確認してください。構成が完了したら、このパターンをデプロイできます。

関連情報:

IBM Workload Deployer: 仮想システム・パターンの管理

IBM PureApplication System: 仮想システム・パターンの管理

複数の DataPower ドメインを伴うデプロイ

SOA Policy Gateway Basic Runtime および SOA Policy Gateway Advanced Runtime パターンは、複製して、複数の DataPower ドメインが含まれるようにカスタマイズできます。

手順

1. SOA Policy Gateway Basic Runtime または SOA Policy Gateway Advanced Runtime パターンを複製します。 詳しくは、 72 ページの『IBM SOA Policy Gateway Pattern の複製とカスタマイズ』を参照してください。
2. パターンを編集するには、「**編集**」をクリックします。
3. 「**スクリプト**」セクションを展開します。
4. さらに追加するドメインごとに、「**SOA Policy Gateway 2.0.0.0 DataPower Domain**」スクリプト・パッケージを、Advanced Runtime パターンの WSRR デプロイメント・マネージャー・パート、または Basic Runtime パターンの WSRR スタンドアロン・パートにドラッグ・アンド・ドロップします。
5. 「**編集の完了**」をクリックします。
6. 追加するドメインごとに以下の情報を入力し、パターンをデプロイします。
   - DataPower_hostname
   - DataPower_XML_mgmt_port
   - DataPower_admin_id
   - DataPower_admin_password
   - パスワードの確認
   - New_DataPower_domain
   - securityFileCleanUp

     注: 複数のドメインを使用する際、最後のドメインにおける securityFileCleanUp の値は **`true`** に設定し、他のすべてのドメインにおける値は **`false`** に設定する必要があります。

   パターンのデプロイについて詳しくは、 68 ページの『SOA Policy Gateway Basic Runtime パターンのデプロイ』または 69 ページの『SOA Policy Gateway Advanced Runtime パターンのデプロイ』を参照してください。

サンプル・アプリケーション

サンプル・アプリケーションは、構成可能な DataPower ドメインと、パターンの機能をデモンストレーションするために使用できる一連の WSRR 成果物です。

サンプル・アプリケーションの基本シナリオは、store (Warehouse) のインベントリー・アプリケーションです。次の 3 つの操作を持つ Store Web サービスがあります。

- purchase
- findInventory
- returnProduct

基本サービス・レベル定義 (SLD) には、次の 2 つのメディエーション・ポリシーがあります。

- 「Store.wsdl に対する妥当性検査 (Validation against Store.wsdl)」。これは、DataPower 妥当性検査がオフになっていることを想定します。
- 「90 秒以内に 5 つのメッセージが出された場合にリジェクト (Reject if there are more than 5 messages in 90 seconds)」。これは、簡単なデモの下限しきい値です。

このサービスのコンシューマーは、現在「Gold」と「匿名」の 2 つのサービス・レベル・アグリーメント (SLA) を持ちます。 HTTP ヘッダーの顧客コンテキストが「Gold」の場合、それらの顧客は即時に別のエンドポイントに経路指定されます。このコンテキストが「匿名」である (つまり現時点で「Gold」ではない) 場合、項目に対して異なる価格値が付けられている Store Mock Service エンドポイントに移動します。

このシナリオでは、ユーザー・グループのメンバーシップに基づいて、findInventory 操作の許可が実行されます。 75 ページの図 5 は、ボックスごとに異なる DataPower ゲートウェイを表して、アプリケーションのフローを示しています。

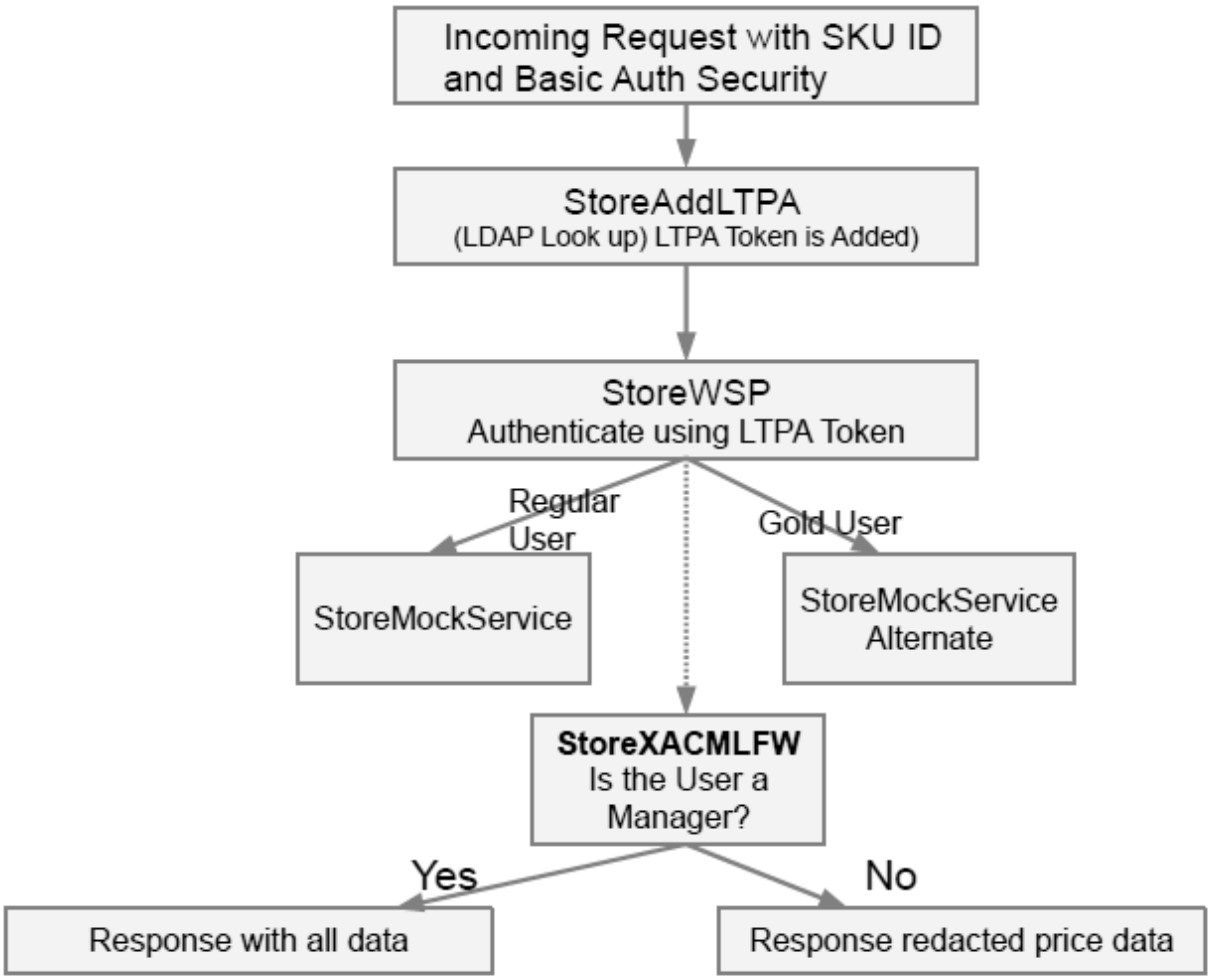


図 5. サンプル・アプリケーション・フロー・ダイアグラム

関連タスク:

72 ページの『IBM SOA Policy Gateway Pattern の複製とカスタマイズ』
IBM SOA Policy Gateway Pattern は編集できません。IBM SOA Policy Gateway Pattern 仮想システム・パターンに用意されたトポロジーでは必要な機能が得られない場合は、パターンを複製してから、編集して新しいパターンを作成することができます。

サンプルの WSRR 成果物の概要

WSRR 成果物は、ウェアハウジング操作を説明します。

Warehouse には、基本的なビジネス機能があります。この Warehouse は、さらに大きな Bob's Warehouse Organization に属しています。サービスのバージョン Store V1.0 は、Store サービスを表します。 Store サービス・レベル定義 (SLD) には、2 つのサービス・レベル・アグリーメント (SLA) があります。 1 つは、ユーザーを別の優先サービスに経路指定する「Gold」ユーザー用 SLA であり、もう 1 つはその他のすべてのユーザーを対象として、要求が行われた DataPower で単純に通知をログに記録する匿名ユーザー用 SLA です。 Store SLD には、他にも 2 つのサン

プル・ポリシーが付加されています。最初のポリシーは、90 秒以内に 5 つのメッセージが出された後で、メッセージを拒否します。 2 つ目のポリシーは、Store.wsdl スキーマに対して妥当性検査を実行します。

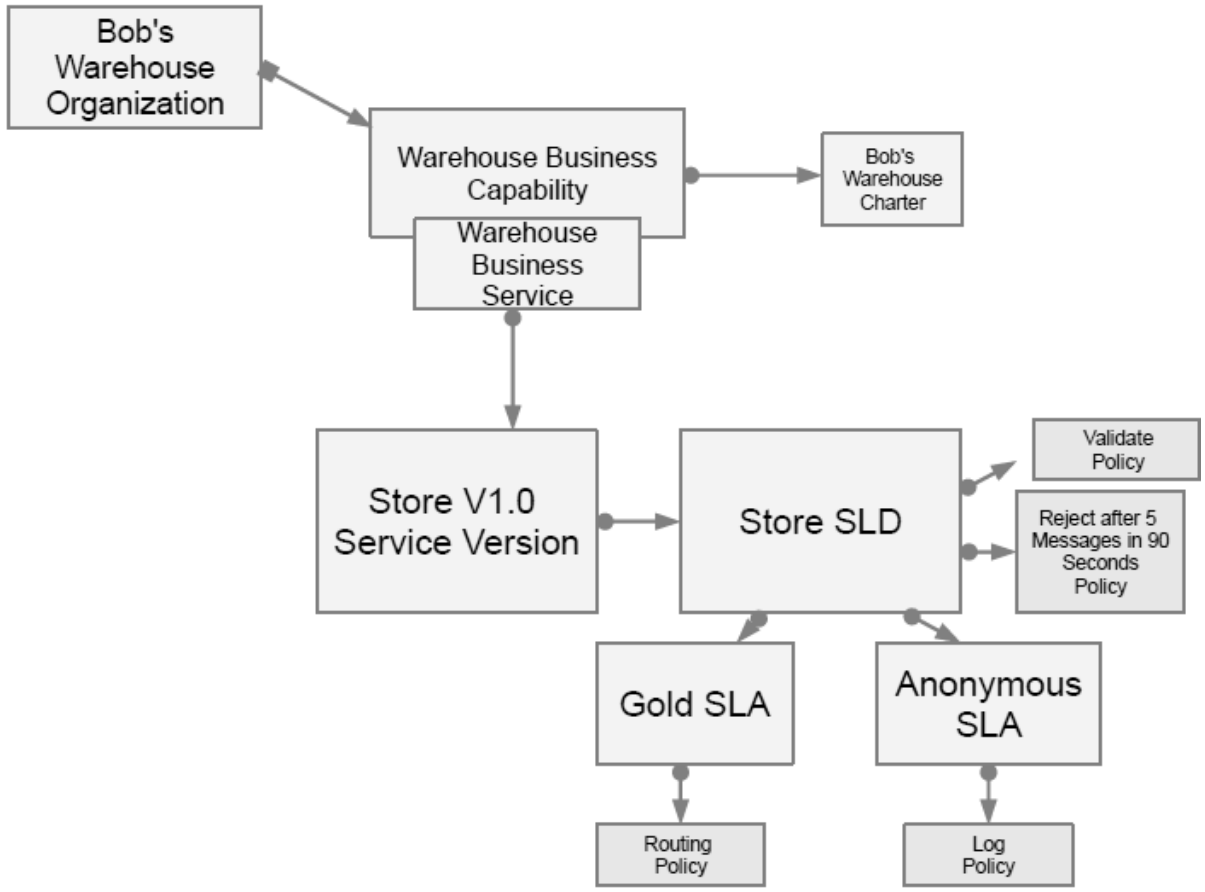


図 6. サンプル・ドメイン

サンプル・テスト・ケースの実行

サンプルの Web アプリケーションまたはコマンド・ラインを使用して、デプロイ済みの SOA Policy Gateway Basic Runtime Sample でサンプル・アプリケーションをテストすることができます。サンプル・アプリケーションで実行可能なコマンド・ライン・テストは 6 種類あります。

Basic Sample Runtime をデプロイするには、65 ページの『SOA Policy Gateway Basic Runtime Sample パターンのデプロイ』を参照してください。

注: 以下の XML サンプルで使用される `SamplePolicySample_starting_port` の値は、SOA Policy Gateway Basic Runtime Sample のログで確認できます。

サンプルの Web アプリケーションのテスト・ケースの実行

Web アプリケーションのテスト・ケースを実行する手順は、以下のとおりです。

1. デプロイ済み WSRR 環境のホスト名を、デプロイ済みの仮想システム・インスタンスを開いて確認します。 そのためには、「**仮想マシン (Virtual machines)**」セクションを展開し、WSRR スタンドアロン・サーバーの仮想マシンを選択して、仮想マシンの詳細を確認します。 「**ハードウェアおよびネットワーク**」セクションで、ホスト名は「**ネットワーク・インターフェース 0**」の値です。
2. Web ブラウザーで URL「`http://<wssrHostName>:9080/SoaPolicyTester`」を開きます。
3. DataPower に実装されるサンプル・アプリケーションのテスト画面が表示されます。
4. オプションは以下のとおりです。
   - **標準の送信 (Send Standard)** - Store サービスに findInventory 要求を送信します。 コンテキスト ID は「Silver」ユーザーです。 正常な結果は「`Part: SKU10 Price: 461.73`」です。
   - **経路指定された送信 (Send Routed)** - Store サービスに findInventory 要求を送信します。 コンテキスト ID は「Gold」ユーザーであり、要求はサービスの Gold 実装に経路指定されます。 正常な結果は「`Part: GOLDSKU10 Price: 461.73`」です。
   - **無効な送信 (Send Invalid)** - 無効なペイロードを指定した要求を送信します。妥当性検査ポリシーには、要求の妥当性検査のために DataPower が必要であり、正常な結果は DataPower からの応答メッセージ「`Internal Error (from client)`」です。
   - **ユーザー ID = ConsumerA (User ID = ConsumerA)** - ConsumerA のユーザー ID による呼び出しには、マネージャーのみが価格を確認できるようにするため、XACML ポリシーが実施されます。応答メッセージの「価格 (Price)」の値は、編集されます。 正常な結果には、「`Price: 0.0`」が含まれます。
   - **多数の標準要求 (Many Standard Requests)** - 90 秒以内に要求が 6 回以上実行されると、拒否ポリシーが実施されます。 実施されているポリシーをデモンストレーションする正常な応答は、「`Rejected: "Rejected (from client)"`」です。
5. WSRR コンソールを開いて、サービスおよびポリシーを検討します。 詳しくは、 を参照してください。

コマンド・ラインを使用してサンプル・アプリケーションのテスト・ケースを実行する手順は、以下のとおりです。

コマンド・ラインを使用した、編集シナリオによる XACML Permit/Deny のデモンストレーション

以下の要求 XML を DataPower StoreAddLTPA サービスに送信できます。

```
<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>
```

上に示した要求 XML の例が `silver.xml` という名前のファイル内にあると想定して、次の curl コマンドを実行します。

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

この例で、ConsumerX はマネージャーなので、完全な価格情報が応答として表示されます。

```
<?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>
```

コマンド・ラインを使用した編集シナリオの実行

ConsumerA はマネージャーではないので、別の応答が表示されます。 curl コマンドを実行します。

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

応答では価格が編集されて 0.0 になっていることに注目してください。

```
<?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>
```

コマンド・ラインを使用したルーティング・ポリシーのテスト

SLA ContextId がルーティング・ポリシーの起動に使用されます。 このケースでは、ゴールド・カスタマーの SLA が、SLA 内の 『Gold』 の値となります。 contextIdentifier が Gold の、サンプル要求の内容を以下に示します。

```
<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>
```

上に示した要求 XML の例が gold.xml という名前のファイル内にあると想定して、 次の curl コマンドを実行します。

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

応答は次のようになります。

```
<?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>
```

戻り応答の SKU 値は GOLDSKU で、ゴールド・エンドポイントの使用を示していることに注目してください。

コマンド・ラインを使用したスキーマの妥当性検査のテスト

妥当性検査ポリシーは、要求のスキーマを、 Store.wsl およびそれに関連付けられた Company.xsd に照らして検査します。

次の XML、badvalid.xml は、本体に含まれるエレメントが <sku> という名前であるべきところが <skubad> という名前なので、無効となる要求を示しています。

```
<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>
```

次の curl 要求を実行する場合:

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

次のエラーが発生します。

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

コマンド・ラインを使用したメディエーション・ポリシーでの拒否のテスト

サンプルに含まれるメディエーション・ポリシーの 1 つは、 メッセージ・カウントが 90 秒間に 5 回実行された後に、拒否の検査を行います。 次のコマンドを 6 回実行してください。

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

サンプル要求は次のとおりです。

```
<?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>
```

このケースでは ConsumerX がマネージャーなので、最初の 5 回の実行で、以下のように完全な価格情報が表示されます。

```
<?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>
```

6 回目の実行では、以下のエラーが表示されます。

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

注: 90 秒以内の間隔で別のテストを実行すると、すぐにこのエラーが表示される可能性があります。

コマンド・ラインを使用したメディエーション・ポリシーでの通知のテスト

contextId が「Gold」ではない場合は、 マップされた SLA はないので、匿名の SLA が使用されます。 匿名 SLA のメディエーション・ポリシーは、ログに記録するか、または通知するです。このためには、デバッグ・モードがサンプル・ドメインに対して有効になっている必要があります。 次のコマンドを実行します。

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

このケースでは ConsumerX がマネージャーなので、 以下のように完全な価格情報が表示されます。

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

以下のメッセージが、ドメインのデフォルト・ログに出力されます。

```
Notify action triggered ('operation_38_2_sla1-1-filter_1-notify') from source policy
    ('LogEveryTime_287d0790-83d9-11e1-a255-9187e20cddb0_05aec6ec-3674-4165-85de-a0f7be48a938'
```

注: このメッセージを表示するには、ロギングがデバッグに設定されている必要があります。そうでない場合は、DataPower Web コンソールの「トラブルシューティング (Troubleshooting)」アイコンをクリックしてください。 「ロギング」セクションで、「ログ・レベル (Log level)」の値を「デバッグ (debug)」に変更して、「**ログ・レベルの設定 (Set Log Level)**」をクリックします。

ログを見つけるには、 「**ファイル**」を選択してから「**ファイル管理 (File Administration)**」 > 「**ファイル処理 (File Management)**」を選択します。 ログは `logtemp` フォルダーにあり、`default-log` という名前です。ログのラッピングのために、テストを実行する前にまずログ・ファイルを Web ブラウザー・ウィンドウ

に入れてから、 テストを実行した後にブラウザーのタブをテストしてリフレッシュしてください。

関連タスク:

65 ページの『SOA Policy Gateway Basic Runtime Sample パターンのデプロイ』
SOA Policy Gateway Basic Runtime Sample パターンをデプロイすると、稼働する、そのパターンの仮想システム・インスタンスが作成されます。

サンプル・アプリケーションの拡張

サンプル・アプリケーションは、バインディング・スタイル・シートと XSL スタイル・シートを修正することにより、変更できます。

Bindings スタイル・シートに対する変更

変数 xacml-subjects がスタイル・シート `apil-xacml-binding-new.xsl` に追加されています。これには、要求のサブジェクト・セクションの作成が含まれています。この変数は、後に `sendToPDP.xsl` からアクセスされます。

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

sendToPDP.xsl

このスタイル・シートは、url-open を使用して StoreXACMLFW を呼び出します。呼び出しは別の XML ファイアウォールに対するボックスで行われるので、SSL プロキシー・プロファイルは使用されません。「ポリシー決定ポイント (PDP) (Policy Decision Point (PDP))」を別の DataPower ボックスに移動する必要があった場合、SSL プロキシー・プロファイルを作成して url-open 呼び出しと共に使用することも可能でした。

```
<xsl:param name="resource" />
<!--
<xsl:variable name="incoming_resource">
<xsl:value-of select="$resource" />
</xsl:variable>
<xsl:message dp:priority="debug">
********** ABOUT TO CALL PDP for RESOURCE equal *************
<xsl:value-of select="$incoming_resource" />
</xsl:message>
-->
- <!--
building the XACML request for masking
-->
<xsl:variable name="customized-request">
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
<soapenv:Header />
<soapenv:Body>
<xacml-context:Request xmlns:wsa="http://www.w3.org/2005/08/addressing"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xacml-context="urn:oasis:names:tc:xacml:2.0:context:schema:os"
xmlns:ws="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
wss-wssecurity-secext-1.0.xsd">
- <!--
copy in the subjects saved from AAA request processing
-->
<xsl:copy-of select="dp:variable('var://context/snip/xacml/xacmlSubjects')/*" />
<xacml-context:Resource>
<xacml-context:ResourceContent>
<xsl:copy-of select="./soap:Envelope/soap:Body" />
</xacml-context:ResourceContent>
<xacml-context:Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#string">
```

```
<xacml-context:AttributeValue>PriceInfo</xacml-context:AttributeValue>
</xacml-context:Attribute>
</xacml-context:Resource>
<xacml-context:Action>
<xacml-context:Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
DataType="http://www.w3.org/2001/XMLSchema#string">
<xacml-context:AttributeValue>View</xacml-context:AttributeValue>
</xacml-context:Attribute>
</xacml-context:Action>
<xacml-context:Environment>
<xacml-context:Attribute AttributeId="ContextId" DataType="http://www.w3.org/2001/XMLSchema#string"
Issuer="http://security.tivoli.ibm.com/policy/distribution">
<xacml-context:AttributeValue>StorePriceData</xacml-context:AttributeValue>
</xacml-context:Attribute>
</xacml-context:Environment>
</xacml-context:Request>
</soapenv:Body>
</soapenv:Envelope>
</xsl:variable>
- <!--
Use set-variable so that it is visible in Probe, which is convenient
-->
<dp:set-variable name="'var://context/snip/xacml/BacksideXacmlRequest'" value="$customized-request" />
- <!--
Report the XACML-REQUEST to the debug log
-->
<xsl:message dp:priority="debug">
<XACML-REQUEST>
<xsl:copy-of select="$customized-request" />
</XACML-REQUEST>
</xsl:message>
<xsl:variable name="headers">
<header name="SOAPAction">xacml:authorization</header>
</xsl:variable>
- <!--
Call the XACML PDP for decision
-->
<xsl:variable name="rtss-response">
<xsl:variable name="StoreGWURL">
<xsl:value-of select="concat('http://','127.0.0.1',':',$StoreGWPort,'/rtss/authz/services/AuthzService')" />
</xsl:variable>
<dp:url-open target="{$StoreGWURL}" http-headers="$headers" response="responsecode">
<xsl:copy-of select="$customized-request" />
</dp:url-open>
</xsl:variable>
- <!--
Use set-variable so that it is visible in Probe, which is convenient
-->
<dp:set-variable name="'var://context/snip/xacml/BacksideXacmlResponse'" value="$rtss-response" />
- <!--
Report the XACML-RESPONSE to the debug log
-->
<xsl:message dp:priority="debug">
<XACML-RESPONSE>
<xsl:value-of select="$rtss-response" />
</XACML-RESPONSE>
</xsl:message>
</xsl:template>
</xsl:stylesheet>
```

sendToPDP.xsl ファイルを検討する場合、以下の項目に注目する必要があります。

1. スタイル・シートは XACMLFW のポートを soavars.xsl から取得します。
2. 変数 rtssResponse は Runtime Security Services が使用する書式、そしてそれにより、DataPower on-box PDP が処理できる書式と正確に一致する必要があります。
3. スタイル・シートは以下の方法で SOAP 要求を作成します。
   - サブジェクト情報は、以前の apil-binding.xsl スタイル・シートから構成され、選択要求の以下のコピーから取得されます。

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

4. このアクションは、単にアクションを表示するためのものです。
   `<xacml-context:AttributeValue>View</xacml-context:AttributeValue>`
5. 環境は、IBM Tivoli® Security Policy Manager / Runtime Security Services 用語では、アプリケーション・オブジェクトと呼ばれる StorePriceData です。

編集用のポリシー・スタイル・シートを見てみましょう。

StorePrivateDataXACML.xml

```
<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>
```

以下の点に注意してください。

- 役割はマネージャーでなければなりません。

```
<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>
```

- リソースは PriceInfo でなければなりません。

```
<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>
```

- アクションは「表示」でなければなりません。

```
<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>
```

サンプル XSL スタイル・シートの変更

アプリケーションで使用される .xsl スクリプトを変更できるポイントがいくつかあります。

手順

サンプル XSL スタイル・シートを変更するために、次のことが可能です。

1. AZ の資格情報のマッピングを変更します。

   rgxacml.xsl スタイル・シートを開き、次の XSL ステートメントを実行します。

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

   次の変数が soavars.xsl スタイル・シートで定義されています。

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

   サンプルには、LDAP サーバーへの暗号化されていないパスワードが含まれています。暗号化されたパスワードを暗号化解除するように、提供されたスタイル・シートをカスタマイズできます。

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

   baseDN は、dc=ibm.com とハードコーディングされています。別のサフィックスや baseDN を使用して LDAP を構成した場合は、この行を変更してサンプルをカスタマイズします。

2. Redaction スタイル・シートを変更します。

   noPriceInfo.xsl スタイル・シートには、次のコードが含まれ、価格の値をゼロにリセットします。編集ロジックに他のフィールドを追加したり、フィールドの値を決定するための計算を含む、より複雑な変換を追加したりできます。

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

   スタイル・シートは、後で他のすべてのエレメントに対して、ID 変換を行います。

サンプルの追加の学習

サンプルについてさらに学習するには、DataPower に XACML「ポリシー決定ポイント (PDP) (Policy Decision Point (PDP))」を構成し、ポリシー文書を編集します。

DataPower の XACML PDP の変更

XACML によるアクセス制御をさらに説明するため、DataPower のセキュリティー・ポリシー決定ポイント (PDP) に使用される XACML の変更について解説します。

手順

PDP を変更または追加するには、次のようにします。

1. DataPower 制御パネルから、`XACML PDP` を検索します。
2. 既存の PDP をクリックするか、「**追加 (Add)**」をクリックします。
3. `local:///storePrivateDataXACML.xml` など、URL を入力します。
4. ポリシーのサポートに必要な依存ファイルまたはディレクトリー・ファイルを追加します。

   注: XACML ポリシー・ファイルをファイル・システムで直接編集した場合は、PDP 定義に戻り、URL など変更したものを再入力するか、またはドメインを再始動して変更を有効にする必要があります。

ポリシー文書の編集

Business Space ユーザー・インターフェースを使用して、ポリシー文書を編集します。

始める前に

SOA ガバナンス・スペースを構成します。詳しくは、 100 ページの『初回使用時の Business Space の構成』を参照してください。

手順

1. 必要な条件とアクションを持つメディエーション・ポリシーを作成します。例えば、5 分間のメッセージ数が 5 より多いという条件や、拒否のアクションです。 メディエーション・ポリシーの作成について詳しくは、 114 ページの『新しいポリシーのオーサリング』を参照してください。
2. 「**終了 (Finish)**」をクリックします。 「参照 (Browse)」ビューが表示されます。
3. メディエーション・ポリシーを制御します。 ポリシー文書の制御について詳しくは、 116 ページの『ポリシーのライフサイクルの管理』を参照してください。
   a. サービス・レジストリー・ナビゲーターでポリシー文書をクリックするか、検索ウィジェットで検索します。アクションがポリシー文書エディターに表示されます。
   b. 「**仕様の提案 (Propose Specification)**」をクリックします。
   c. 「**仕様の承認 (Approve Specification)**」をクリックします。

   ポリシーが承認されました。ポリシーを再定義、置き換え、または廃止して、ライフサイクルの管理や既存の定義の編集を行うことができます。

関連タスク:

114 ページの『新しいポリシーのオーサリング』
Business Space ユーザー・インターフェースでメディエーション・ポリシーをオーサリングする場合、ポリシーの条件とアクションを指定します。

116 ページの『ポリシーのライフサイクルの管理』
Business Space ユーザー・インターフェースを使用して、ポリシーのガバナンス状態を遷移できます。

関連情報:

IBM WebSphere Service Registry and Repository バージョン 8.0 インフォメーション・センター - Business Space ユーザー・インターフェースの使用

DataPower サンプル・ドメイン

パターンには、パターンの使用を開始するためのサンプルの DataPower ドメインが備わっています。 DataPower 開発者は、既存のゲートウェイを独自のアプリケーションのテンプレートとして使用できます。サンプルの環境には、5 つのゲートウェイが含まれています。 Store サービス用に 1 つの 1 次ゲートウェイ、そして呼び出す Store Gateway 用のバックエンドの例を提供する 4 つのサポート用ゲートウェイ、編集シナリオ用の XACML サポート、および追加のセキュリティー機能を提供するフロントエンドがあります。

Store Web サービス・プロキシー

Store Web サービス・プロキシー (WSP) は、アプリケーション・ドメインの 1 次ゲートウェイです。これは、LTPA トークンが接続された要求を受信します。

要求されると、要求の処理ルールによって以下のアクションが実行されます。

1. Validation ポリシーの要求に応じて、要求を妥当性検査します。詳しくは、 75 ページの『サンプルの WSRR 成果物の概要』を参照してください。
2. サービス・レベル・アグリーメント (SLA) が「Gold」である場合、要求を別のエンドポイントに経路指定します。
3. その要求に対して、認証、許可の実行、およびアカウンティング (AAA) を行います。これには、以下のようなアクションが含まれます。
   a. LTPA トークンを持つユーザーを認証します。
   b. 顧客が属するグループなどの情報を提供する LDAP サーバーに対して、資格情報をマップします。これらのグループには、「マネージャー (Manager)」、「店員 (Clerk)」、および「顧客 (Customer)」などがあります。
   c. 提供された入力を、「XACML ポリシー決定ポイント (PDP) (XACML policy decision point (PDP))」が理解できる要求オブジェクトに変換します。
   d. DataPower ボックスで XACML PDP を使用した許可を、IBM Tivoli Security Policy Manager で作成可能な XACML ポリシー文書を使用して実行します。ポリシーの基準は、ユーザーが「マネージャー (Manager)」、「顧客 (Customer)」、または「店員 (Clerk)」でなければならないということです。findInventory 操作の戻りは「マネージャー (Manager)」または「店員 (Clerk)」のいずれかでなければならず、purchase 操作は「顧客 (Customer)」によって実行されなければなりません。
4. XSL スクリプトを使用して ConsumerID の値を設定します。

5. 要求から HTTP セキュリティー・ヘッダー全体を削除します。
6. Store サービスのバックエンドを呼び出します。

要求が処理されると、応答処理ルールは以下のアクションを実行します。

1. StoreXACMLFW ゲートウェイ (このシナリオでは PDP として動作します) を呼び出します。
2. 応答に基づき、ユーザーが「マネージャー (Manager)」役割を保持しているかどうかに応じて価格情報フィールドが編集されます (ゼロが埋め込まれます)。

サンプルの XML ファイアウォール

サンプルでは、以下の XML ファイアウォールが定義されています。

StoreAddLTPA XML ファイアウォール

StoreAdd LTPA XML ファイアウォールの機能は、ユーザーが基本認証 (例えば LTPA やそれと類似のものではない) のみを使用して呼び出せるもの以外のポートをフロントエンドに提供することです。要求の処理ルールは以下のとおりです。

1. 基本認証による識別。
2. 非常に簡単な LDAP ルックアップによる認証。
3. LTPA トークンを後処理の一部として追加。
4. LTPA 情報が添付された状態で、要求を StoreWSP セキュリティー・ポリシーに転送。

StoreMockService XML ファイアウォール

StoreMockService は、XML ファイアウォールを実装として使用するサンプル・サービスです。 findInventory、購入、および戻り操作は、すべてサポートされます。応答値は静的です。このサンプル・サービスは、WebSphere Application Server をパターンに含めることができない場合に作成されます。ポリシーの 3 つの要求ルールは、マッチング・アクションを使用して要求操作を判別し、一致した項目に基づいて、静的 SOAP 応答により応答します。静的 SOAP 応答は、完全なサービスの実装ではなく、要求操作に基づいて提供されます。

StoreMockServiceAlternate XML ファイアウォール

StoreMockServiceAlternate は、XML ファイアウォールを実装として使用するサンプル・サービスです。 findInventory、購入、および戻り操作は、すべてサポートされます。このサービスは、適用されているルーティング・ポリシーを例示するために使用されます。

StoreXACMLFW ファイアウォール

このシナリオでは、XACML ベースの許可/拒否メカニズムの結果に基づいて編集を実行します。 DataPower では、応答フローで個々の AAA アクションを呼び出す方法はありません。 XACML の「ポリシー決定ポイント (PDP) (Policy Decision Point (PDP))」を収める別個のゲートウェイが作成されます。この PDP は、StoreXACMLFW の要求ルールで、AAA アクションにカプセル化されています。

StoreXACMLFW は、DataPower の XML ファイアウォール・ゲートウェイです。この実装は、機能性を提供する簡単な方法であるため使用されます。 StoreXML フ

ファイアウォールは、Tivoli Runtime Security Services サーバーと同じ WSDL インターフェースを使用します。 StoreWSP ゲートウェイは、要求オブジェクトを作成し、それを SSL を使用して保護して StoreXMLFW ゲートウェイに送信します。

StoreXML ファイアウォールの要求ルールは、以下を行います。

1. 認証用に SSL 情報を使用して AAA を実行します。
2. On Box XACML PDP を使用して、許可を実行します。 PDP が使用するポリシーは、最初は IBM Tivoli Security Policy Manager で作成されますが、標準エディターを使用して再作成でき、そのスキーマは XACML 仕様で定義されます。
3. この許可プロセスでは、要求の変換は必要ありません。
4. XACML 要求が有効な場合、要求処理ルールは許可応答をフェッチして、クライアントに返します。それ以外の場合、例外処理ルールで処理される例外がスローされ、クライアントに拒否応答を返します。

注: この許可/拒否/不確定は、サンプル・レベルでの応答に限定されます。追加のエラー情報が、顧客固有のフローに組み込まれることがあります。

XACML セキュリティー・ポリシー

このトピックでは、XACML 文書の作成方法について説明します。

サンプルで使用される XACML 文書は、IBM Tivoli Security Policy Manager ポリシー・エディターで作成されますが、このような文書を任意のテキスト・エディターや XML エディターを使用して手動で作成することができます。既存の XACML ポリシーを構成または変更するには、OASIS 仕様 (https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml) を参照してください。

サンプルで使用される XACML セキュリティー・ポリシーは、`storeSWPXACML.xml` および `storePrivateDataXACML.xml` に収められています。これらのポリシーを使用して、「ポリシー決定ポイント (PDP) (policy decision point (PDP))」に着信した要求を評価することができます。要求は、次の 4 つの主要なエレメントで構成されます。

1. 「サブジェクト (Subjects)」セクション - 要求呼び出し元の識別名の詳細と、呼び出し元の属しているグループが含まれます。
2. 「リソース (resource)」セクション - 呼び出し元がアクセス権限を取得する文書が含まれます。サンプルでは、2 つのタイプのリソースが使用されます。1 つ目は Web サービスにおける操作であり、2 つ目は応答のデータ (この場合は priceInfo リソース) に対する許可です。
3. 「環境 (Environment)」セクション - 要求の環境に関する情報が含まれます。
4. 「アクション (action)」- 許可された素材でユーザーが何を行うか。編集シナリオでは、アクションは単純に priceInfo データを表示することです。

StoreWSP セキュリティー・ポリシー

`storeSWPXACML.xml` ファイル内のセキュリティー・ポリシーは、グループを Web サービス・オペレーションにマップします。

以下はセキュリティー・ポリシーの例です。

```
<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>
```

注: 「サブジェクト (subject)」セクションで、x500 名または「マネージャー (Manager)」のサブジェクト役割で一致が起こります。ポリシー .xml ファイルの全体を調べると、「顧客 (Customer)」および「店員 (Clerk)」でも同様のマッピングが行われていることがわかります。 findInventory 操作でこれら 3 つのグループのすべてを使用することが許可されている一方で、returnProduce 操作および purchase 操作は特定のグループにしか許可されていないことが判明します。

Redaction ゲートウェイ

storeCallPDP.xsl スタイル・シートの詳細。

storeCallPDP.xsl スタイル・シートを調べると、以下のことに気付きます。

1. storeSendToPDP.xsl スタイル・シートが組み込まれています。これは、storeXAMLFW を呼び出すロジックを持つスタイル・シートです。
2. storeSendToPDP 内のテンプレート call_PDP inside の呼び出し
3. 呼び出しの応答からの決定の抽出 (例えば、「Permit」)。
4. var:/context/response/displayfilter 値が allData.xsl または noPriceInfo.xsl のいずれかのスタイル・シートに設定されています。
5. Reaction の XACML である storePrivateDataXACML.xml で、構造が StoreWSP シナリオで使用される構造とほぼ同じであることを検査します。違いは、マネージャーの役割にアクセス権限がある点だけです。

storeCallPDP.xsl

```
<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:dp="http://www.datapower.com/extensions"
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">****** SETTING THE PRIVATE FILTER ********</xsl:message>
        <dp:set-variable name="'var://context/response/displayFilter'" value="'local:///allData.xsl'" />
      </xsl:when>
      <xsl:otherwise>
        I<dp:set-variable name="'var://context/response/displayFilter'" value="'local:///noPriceInfo.xsl'" />
      </xsl:otherwise>
    </xsl:choose>
  </xsl:template>
</xsl:stylesheet>
```

SOA Policy Gateway Basic Runtime Sample で作成される WSRR 成果物

SOA Policy Gateway Basic Runtime Sample パターンで作成される WSRR 成果物と、サンプルがそれらの成果物を使用する方法。

表 33. SOA Policy Gateway Basic Runtime Sample パターン用に作成される WSRR 成果物

オブジェクト	説明
組織	Bob's Warehouse。
ビジネス・ケイパビリティー	Bob's Warehouse 組織の所有する Warehouse。
サービスのバージョン	Store 1.0 は Store Web サービス、Store サービス・レベル定義 (SLD)、および Warehouse ビジネス・ケイパビリティーを使用します。
WSDL	Store.wsdl
XSD	Company.xsd

表 33. SOA Policy Gateway Basic Runtime Sample パターン用に作成される WSRR 成果物 (続き)

オブジェクト	説明
ポリシー	• Validate.xml • RouteForGold.xml • LogEveryTime.xml • RejectAfter5MsgIn90Seconds.xml
ポリシー接続	• Anonymous Users_GenericObject_Anonymous Users_LogEveryTime.xml - LogEveryTime ポリシーを匿名ユーザー用サービス・レベル・アグリーメント (SLA) に接続します。 • Gold SLA_GenericObject_Gold SLA_RouteForGold.xml - RouteForGold ポリシーを Gold SLA に接続します。 • Store_GenericObject_Store_urn :RejectAfter5MsgIn90Seconds.xml - RejectAfter5MsgIn90Seconds ポリシーを Store SLD に接続します。 • Store_GenericObject_Store_urn:Validate.xml - Validate ポリシーを Store SLD に接続します。
SLD	Store SLD - Store 1.0 サービス・バージョンによって使用されます。
SLA	Gold SLA - ContextId が「Gold」の場合に Gold エンドポイントに経路指定されます。
匿名 SLA	匿名ユーザー - LogEveryTime ポリシー通知を使用し、ContextId が「Gold」ではない場合に実行されます。

サンプル・アプリケーションによる WSRR 成果物の使用

StoreWSP は、WSRR サブスクリプションを使用して WSDL およびポリシー成果物を検索します。要求が StoreWSP を介して処理された場合には、必ず以下のアクションが実行されます。

1. Store 1.0 サービス・バージョンは、Store SLD に接続されます。この Store SLD には、Validate および RejectAfter5MsgIn90Seconds の 2 つの直接ポリシーが接続されています。ポリシーが実行される順序は不定です。
   a. 過去 90 秒以内に 5 回の要求が行われている場合、要求はリジェクトされます。
   b. 要求は Store.wsdl とそれに関連する Company.xsd に照らして妥当性検査されます。
2. Store 1.0 サービスは Store SLD を使用します。この Store SLD には、Gold ユーザーに対して使用される Gold SLA と、その他すべてのユーザーに対して使用される匿名ユーザー用 SLA の 2 つの SLA があります。 ContextId 属性が「Gold」の場合、要求は StoreMockServiceAlternate XML ファイアウォールに経路指定されます。それ以外の「Silver」などの値の場合は、匿名ユーザー用 SLA に引き継がれ、LogEveryTime ポリシーが実行されます。これにより、通知はサンプル・ドメインの `default.log` に配置されます。この通知は、ドメインでデバッグ・モードが有効になっている場合にのみ確認できます。その後、メッセージは StoreMockService XML ファイアウォールに経路指定されます。

SOA Policy Gateway Basic Runtime Sample で作成される DataPower 成果物

SOA Policy Gateway Basic Runtime Sample パターンで作成される DataPower 成果物。

表 34. SOA Policy Gateway Basic Runtime Sample パターン用に作成された DataPower の成果物

タイプ	名前	目的
WebService プロキシー	StoreWSP	基本サービス。
XML ファイアウォール	StoreAddLTPA StoreMockService StoreAlternateMockService StoreXACMLFW	LTPA トークンを認証し、追加します。 非 Gold 顧客のサービス・プロバイダー Gold 顧客のサービス・プロバイダー PriceInfo に対するアクセス権限を検査します。
WSRR サーバー	WSRRSVR	WSRR への接続。
WSRR サブスクリプション	StoreSub	WSRR 名前空間やオブジェクトなどの検索情報を提供します。
AAA ポリシー	StoreAddLTPA	LDAP の基本認証 ID。 Looks-up 認証。 要求に LTPA トークンを追加します。
AAA ポリシー	StoreWSDLAAA	LTPA ID および認証。 許可のグループ・マッピング。 XACML 許可。
AAA ポリシー	StoreXACMLFWAZ	PriceInfo に対する XACML 許可。
SSL プロキシー・プロファイル	WSRRPP	WSRR サーバーの SSL プロキシー・プロファイル。
暗号プロファイル	WSRRCP	WSRR サーバーの暗号プロファイル。
妥当性検査の資格情報	WSRRVC	妥当性検査の資格情報には、暗号証明書 WSRRCERT が含まれます。その他すべての設定はデフォルトです。
暗号証明書	WSRRCERT	WSRRCERT は署名者証明書を使用します。この証明書は、単一サーバー用のデフォルトの証明書である NodeDefaultKeyStore から抽出されたものか、 IBM HTTP Server が存在した ND 環境の場合は CMSKeyStore デフォルト証明書です。

StoreWSP Web サービス・プロキシーの処理ルール

サンプルの中央ゲートウェイは StoreWSP です。このゲートウェイのポリシーには、要求ルールと応答ルールが含まれています。

要求ルール

StoreWSP_default_request-rule の主なポリシー・アクションは、AAA と呼ばれます。 AAA アクションでは、LTPA トークンが妥当性検査され、ユーザー・グループが検索され、許可が実行されて、ユーザーが「マネージャー (Manager)」、「店員 (Clerk)」、または「顧客 (Customer)」のどの LDAP グループに属しているかを調べます。これは、AAA AZ ステップにより、DataPower アプライアンスで StoreWSDLPDP「ポリシー決定ポイント (PDP) (Policy Decision Point (PDP))」が呼び出されると実行されます。この PDP では、storeWSPXACML.xml XACML ポリシーが使用されます。

応答ルール

応答ルール StoreWSP_default_response-rule では、変換によって StoreXACMLFW XML ファイアウォール・サービスが呼び出されます。

この変換では、ユーザーが「マネージャー (Manager)」グループのメンバーであるかどうかに基づいて、ユーザーが価格情報へのアクセスを許可されるかどうかを判別します。許可される場合、*var:///context/response/displayFilter* 変数が `local:///allData.xsl` に設定されます。このユーザーが「マネージャー (Manager)」LDAP グループのメンバーではない場合、*var:///context/response/displayFilter* 変数は `local:///noPriceInfo.xsl` に設定されます。

この変換では、次に、応答に対してスタイル・シート・アクションが実行されます。

StoreXAMLFW 処理ルール

カスタム・スタイル・シートの storeSendToPDP.xsl は、ローカル XML FW StoreXACMLFW に対して呼び出しを行います。このファイアウォールでは、2 つの処理ルールが使用されます。 StoreXACMLFW_request には、allData.xsl 変換を使用する単一の AAA ポリシー・アクションが含まれています。この AAA アクション StoreXACMLFWAZ は、XACML PDP StorePDP アクションを呼び出します。storePrivateDataXACML.xml XACML ポリシーを使用して、ユーザーが価格情報に対して許可されるかどうかの判別が行われます。

サンプル XSL スタイル・シート

サンプル・アプリケーションには、末尾が `.xsl` の以下のスタイル・シートが含まれ、インストール済みドメインのローカル・ディレクトリーに入っています。

表 35. サンプル・アプリケーションのスタイル・シート

スタイル・シート	目的
`allData.xsl`	ソースからターゲットに対してすべてのデータをコピーする ID スタイル・シート。これは、「編集 (Redaction)」機能にも、XACML XML ゲートウェイに対する呼び出しにも使用されます。

表 35. サンプル・アプリケーションのスタイル・シート (続き)

スタイル・シート	目的
apil-xacml-binding-new.xsl	資格情報マッピング情報を使用して、SOAP 要求を作成します。この SOAP 要求は、DataPower アプライアンスの「ポリシー決定ポイント (PDP) (Policy Decision Point (PDP))」で処理することができます。このスタイル・シートは、DataPower アプライアンスの store ディレクトリー内に準備されている tspm-xacml-binding-sample.xsl スタイル・シートを変更したものです。この採用されたスクリプトから提供される主な機能は、XACML 要求のサブジェクト情報を編集スタイル・シートで使用可能にする、外部アクセス可能な変数を追加することです。
noPriceInfo.xsl	このスタイル・シートは、価格エレメントを値 0.0 に設定します。
rgxacml.xsl	このスタイル・シートは、DataPower アプライアンスの store ディレクトリー内にある tspm-retrieve-groups.xsl スタイル・シートをカスタマイズしたものです。このスタイル・シートの主な目的は、着信したユーザーを検索してそのグループ情報を取り出せるようにするために、LDAP DN、ホスト名、パスワード、ポートなどを提供することです。
soavars.xsl	このスタイル・シートは、rgxacml.xsl スタイル・シートが使用する変数に LDAP 情報を定義する、例示用に限定されたスタイル・シートです。例においては、パスワードが暗号化されておらず、実動のプラクティスではありません。
storeCallPDP.xsl	このスタイル・シートには、XACML ゲートウェイを呼び出し、Permit/Deny の決定を処理し、allData.xsl または noPriceInfo.xsl のいずれかを実行するフィルター変数を設定するためのコードがあります。
storeSendToPDP.xsl	このスタイル・シートは、XACML ゲートウェイに送信される SOAP 要求を構成します。 apil-xacml-binding-new.xsl スタイル・シートで取得したサブジェクト情報と、リソース情報、アクション情報、および環境情報が含まれます。

XSL スタイル・シートを使用する DataPower オブジェクト

DataPower オブジェクトは、サンプル・アプリケーションで提供されるいくつかの XSL スタイル・シートを使用します。

表 36. XSL スタイル・シートを使用する DataPower オブジェクト

スタイル・シート	目的
allData.xsl	storeCallPDP.xsl スタイル・シートで内部的に使用されます。このスタイル・シートは、AAA ポリシー StoreXACMLFWAZ でカスタム変換として使用されます。
apil-xacml-binding-new.xsl	StoreWSDLAAA AAA ポリシーの AZ ステップでカスタム・スタイル・シートとして使用されます。
noPriceInfo.xsl	storeCallPDP.xsl スタイル・シートで内部的に使用されます。
soavars.xsl	rgxacml.xsl スタイル・シートで内部的に使用されます。
storeCallPDP.xsl	Store_default-response ルールで変換として呼び出されます。
storeSendToPDP.xsl	storeCallPDP.xsl スタイル・シートで内部的に使用されます。

第 6 章 デプロイしたインスタンスを扱う作業

IBM SOA Policy Gateway Pattern イメージをデプロイしたら、独自のサービス定義を登録し、独自のポリシーをそれらの定義に付加することができます。また、デプロイしたシステムを表示および管理できます。デプロイしたインスタンスのリストを表示するには、「**インスタンス**」 > 「**仮想システム**」をクリックします。

インスタンスの詳細の表示

デプロイしたインスタンスの詳細を表示するには、「仮想システム・インスタンス」ウィンドウ内のインスタンスのリストでインスタンスを選択します。仮想システム・インスタンスの詳細は、右側に表示されます。この詳細には、そのデプロイメントのクラウド・インフラストラクチャーでプロビジョンされた仮想マシンのリスト、IP アドレス、仮想マシンの状況、およびロールの状況が含まれます。ロールとは、仮想マシン上で仮想アプリケーション・ミドルウェアによって実行される機能の単位です。また、仮想マシンのロールの正常性状況に関する情報を表示することもできます。例えば、仮想マシン上で CPU がクリティカルな状況である場合は、緑色の状況矢印の上に赤いチェック・マークが表示されます。

インスタンスのプロビジョニングおよびデプロイメントの状況を確認するには、詳細ビューの「**現在の状況**」の値を参照してください。

プロビジョニングの際の仮想マシンおよびスクリプトの状況を表示するには、詳細ビューの「**ヒストリー**」セクションを展開します。

仮想マシンおよびスクリプト・ログの詳細を表示するには、詳細ビューの「**仮想マシン**」セクションを展開します。システムのホストおよび IP アドレスは、「**ハードウェアおよびネットワーク**」セクションの「**ネットワーク・インターフェース 0**」の値です。稼働中の仮想マシンを展開して、スクリプト・ログを「**スクリプト・パッケージ**」セクションで表示し、使用中の仮想マシンにアクセスするためのリンクを「**コンソール**」セクションで表示します。

デプロイしたインスタンスの管理

仮想システム・パターンをデプロイした後、作成された仮想システム・インスタンスを表示および管理して、IBM SOA Policy Gateway Pattern 環境を把握することができます。

始める前に

仮想システム・インスタンスを表示するには、まず仮想システム・パターンをデプロイしておく必要があります。

このタスクについて

パターンをデプロイすると、仮想システム・インスタンス、すなわち新規にプロビジョンされた IBM SOA Policy Gateway Pattern ランタイム環境が作成されます。デプロイメントの完了時には、仮想システム・インスタンスが稼働しています。

手順

IBM SOA Policy Gateway Pattern 仮想システム・インスタンスを管理するには、以下のステップを実行します。

1. 「**インスタンス**」 > 「**仮想システム**」をクリックして、「仮想システム・インスタンス」ウィンドウにアクセスします。
2. 「仮想システム・インスタンス」ウィンドウ内のインスタンスのリストから、デプロイされたインスタンスを選択します。
3. インスタンスが稼働している場合は、仮想システム・ビュー内のコンソール・リンクから、仮想システムのコンポーネントにログインすることができます。使用可能なコンポーネントは、作成したパターンに応じて異なります。例えば、以下の操作が考えられます。
   - デプロイメント・マネージャーの管理コンソールを起動してログインし、作成されたクラスターを調べます。
   - プロセス・センターを起動し、プロセス・デザイナーをダウンロードしてプロセス・アプリケーションを作成します。
   - IBM Integration Designer をセットアップし、プロセス・オーサリングのためにプロセス・センターに接続します。

WSRR への接続 - Business Space

Business Space ユーザー・インターフェースを使用して、ポリシーを管理します。

このタスクについて

WSRR システムのホスト・アドレスを使用して、Business Space ユーザー・インターフェースにアクセスします。

手順

1. 「**インスタンス**」 > 「**仮想システム**」をクリックして、「仮想システム・インスタンス」ウィンドウにアクセスします。
2. 「仮想システム・インスタンス」ウィンドウ内のインスタンスのリストから、デプロイされたインスタンスを選択します。 インスタンスの詳細が表示されます。
3. Business Space ユーザー・インターフェースを使用して、WSRR システムにアクセスします。
   - 「**コンソール**」セクションで「**WSRR Business Space**」をクリックして、WSRR システムで実行されている Business Space に接続します。
   - あるいは、外部 Web ブラウザーで以下を実行します。
     a. WSRR のホスト名とポート番号を確認します。「**仮想マシン**」セクションを展開し、WSRR スタンドアロン・サーバーの仮想マシンを選択して、仮想マシンの詳細を表示します。「**ハードウェアおよびネットワーク**」セクションで、ホスト名は「**ネットワーク・インターフェース 0**」の値です。
     b. Business Space の URL を入力します。
        – セキュリティーが有効な WSRR スタンドアロン・サーバーの場合: `https://<hostname>:9443/BusinessSpace`
        – クラスターの場合: `http://<hostname>/BusinessSpace`

ここで、*<hostname>* と *port* は、WSRR サーバーのホスト名とポート値です。

タスクの結果

Business Space が表示されます。これを使用してポリシーを追加、編集、または削除できます。

次のタスク

WSRR システムで Business Space を初めて使用する場合は、100 ページの『初回使用時の Business Space の構成』を参照し、手順にしたがって操作スペースを作成してください。

関連情報:

IBM WebSphere Service Registry and Repository バージョン 8.0 インフォメーション・センター

WSRR への接続 - サービス・レジストリー・コンソール

サービス・レジストリー・コンソールを使用して、サービス・バージョンを分類します。

このタスクについて

WSRR システムのホスト・アドレスを使用して、「サービス・レジストリー・コンソール」ユーザー・インターフェースにアクセスします。

手順

1. 「**インスタンス**」 > 「**仮想システム**」をクリックして、「仮想システム・インスタンス」ウィンドウにアクセスします。
2. 「仮想システム・インスタンス」ウィンドウ内のインスタンスのリストから、デプロイされたインスタンスを選択します。 インスタンスの詳細が表示されます。
3. WSRR システムにアクセスします。
   - 「**コンソール**」セクションで「**WSRR_Web_UI**」をクリックして、WSRR システムで実行されている Business Space に接続します。
   - あるいは、外部 Web ブラウザーで以下を実行します。
     a. WSRR のホスト名とポート番号を確認します。「**仮想マシン**」セクションを展開し、WSRR スタンドアロン・サーバーの仮想マシンを選択して、仮想マシンの詳細を表示します。「**ハードウェアおよびネットワーク**」セクションで、ホスト名は「**ネットワーク・インターフェース 0**」の値です。
     b. 次のサービス・レジストリー・コンソールの URL を入力します。
     http://*hostname*/ServiceRegistry

     ここで、*hostname* は WSRR サーバーのホスト名です。

関連情報:

IBM WebSphere Service Registry and Repository バージョン 8.0 インフォメーション・センター

初回使用時の Business Space の構成

Business Space ユーザー・インターフェースを使用してポリシーを作成できるようにするには、事前に SOA ガバナンス・スペースを作成する必要があります。

始める前に

Business Space へのアクセスについて詳しくは、 98 ページの『WSRR への接続 - Business Space』を参照してください。

このタスクについて

Business Space ウィジェットを使用するには、スペースを作成する必要があります。スペースは、特定のロールのために定義されます。ポリシー・オーサリングは、SOA ガバナンス・スペースで作業するのが最適です。SOA ガバナンス・スペースをまだ作成していない場合は、これを作成する必要があります。「SOA ガバナンスのサービス・レジストリー」テンプレートに基づいてスペースを作成するには、以下のステップを実行します。

手順

1. ページ上部の「**スペースの管理 (Manage Spaces)**」をクリックします。「スペース・マネージャー (Space Manager)」ダイアログが表示されます。
2. 「**スペースの作成 (Create Space)**」をクリックします。「スペースの作成 (Create Space)」ダイアログが表示されます。
3. スペース名フィールドに名前を入力します。例えば、`SOA Governance` とします。オプションで、説明を入力します。
4. 「**テンプレートを使用して新規スペースを作成します**」リストから「**SOA ガバナンスのサービス・レジストリー**」を選択し、「**保存**」をクリックします。
5. 「**スペース・マネージャー (Space Manager)**」リストに新規スペースが表示されます。新しいスペースをクリックして開きます。

タスクの結果

SOA ガバナンス・スペースが作成されます。SOA ガバナンス・スペースを開くには、以下を実行します。

1. ページ上部の「**スペースに進む**」をクリックします。「スペースに移動 (Go To Spaces)」ダイアログが表示されます。
2. SOA ガバナンス・ユーザーのスペースをクリックします。具体的な名前は、スペースの作成時に指定された内容に基づきます。

次のタスク

「サービス・レジストリー・アクション」ウィジェットに、さらにアクションを追加することができます。

1. Business Space で「**ページの編集**」をクリックします。

2. 「サービス・レジストリー・アクション」ウィジェットで「**設定の編集**」をクリックします。
3. 以下のアクションを選択して表示します。
   - サービス・レベル定義の作成
   - サービス・バージョンの作成
   - サービス・レベル・アグリーメントの作成
   - ビジネス・ケイパビリティーの作成
4. 「サービス・レジストリー・アクション」ウィジェットで「**保存して閉じる**」をクリックします。
5. 「**編集の終了**」をクリックします。

パターンのデプロイメント後の構成

パターンをデプロイした後で、セキュリティーおよびその他の設定を構成する必要があります。

サンプル・アプリケーションの LDAP の設定変更

SOA Policy Gateway Basic Runtime Sample を使用しており、 LDAP サーバーのセキュリティー設定 (例: パスワードやユーザー名) を変更する必要がある場合は、これらの値を 2 箇所で変更する必要があります。

変更を加える箇所は、次のとおりです。

- AAA ポリシー StoreAddLTPA の「AAA ポリシー認証 (AAA Policy Authentication)」セクション - このポリシーを見つけるには、DataPower 管理 Web ユーザー・インターフェースの検索ウィンドウを使用して、「AAA」を検索します。正しい AAA ポリシーを選択して、「認証 (Authentication)」タブの値を変更します。
- soavars.xsl ファイル - DataPower Web 管理ユーザー・インターフェースの「ファイル管理 (File Management)」セクションを使用します。 DataPower アプライアンスの SOA Policy Gateway Basic Runtime Sample パターンによって作成されたドメインを開いて、ローカル・ディレクトリーで soavars.xsl ファイルを参照します。必要に応じて LDAPHost、LDAPPort、LDAPCN、LDAPPassword の各変数を変更します。

  注: これらの変更内容を有効にするには、ドメインの再始動が必要になる場合があります。

DataPower 証明書の DN 値の認証

提供される IBM SOA Policy Gateway Pattern で SSL が使用される場合、 DN ホストの検査はデフォルトの WebSphere Application Server セキュリティーよりも厳密になります。

WebSphere Application Server では、DN ホストの検査はデフォルトでは無効です。しかし、IBM SOA Policy Gateway Pattern で使用されるスクリプト・パッケージでは、 DN ホスト検査がオンになり、無効にすることはできません。デフォルトの WebSphere Application Server と DataPower との間で機能する非常に特殊な証明書

は、IBM SOA Policy Gateway Pattern で使用される「SOA Policy Gateway 2.0.0.0 - Security」スクリプト・パッケージや「SOA Policy Gateway 2.0.0.0 - Sample」スクリプト・パッケージでは機能しない可能性があります。例えば、`myserver.yourcompany.com` の DN は WebSphere Application Server のデフォルトでは受け入れられますが、スクリプト・パッケージでは受け入れられません。デプロイメントで使用される DataPower 証明書の追加または削除については、『WSRR トラストストアからの DataPower 証明書の削除または追加』を参照してください。

LTPA 鍵の変更

この手順では、LTPA 鍵の変更方法について説明します。 LTPA 鍵は、基本のすべてのセルで共有されます。 SOA Policy Gateway Basic Runtime Sample パターンでは使用されません。 LTPA 鍵は、ガバナンス・マスターからエクスポートされて、ステージング、実動、設定解除などのランタイム環境にインポートされます。

手順

1. ガバナンス・マスターの WSRR Dmgr から新しい LTPA キーをエクスポートします。
2. LTPA 鍵を、Dmgr またはスタンドアロンのランタイム WSRR インスタンスにインポートします。
3. ランタイム・インスタンスが拡張 ND 環境の場合は、次のステップを順序どおりに実行します。
   a. すべてのノードを同期します。
   b. WSRR クラスターを停止します。
   c. ノード・エージェントを停止します。
   d. Dmgr を停止します。
4. 環境が拡張の場合は、逆の順序で再始動する必要があります。
   a. Dmgr を開始します。
   b. ノード・エージェントを開始します。
   c. WSRR クラスターを開始します。
5. WSRR がスタンドアロン・サーバーの場合、LTPA 鍵の変更を有効にするには、停止してから再始動する必要があります。

WSRR トラストストアからの DataPower 証明書の削除または追加

このタスクでは、DataPower 証明書の追加または削除の方法について説明します。このタスクを実行すると、ポリシーの更新時に、WSRR と DataPower の間の同期更新機能の今後の設定が簡単になるというメリットがあります。

このタスクについて

DataPower 証明書は、パターンの一部として curl ツールによって使用されます。DataPower 呼び出しは、ノードまたはセルのデフォルトのトラストストアにアップロードされます。これにより、ポリシーの更新時に、WSRR と DataPower の間の同期更新機能の今後の使用が簡単に設定できるようになります。この機能が必要ない場合、この手順は DataPower 証明書の削除方法の説明になります。また、この手順

は、証明書を変更する必要があるときに、新しい DataPower 証明書を追加する方法の説明にもなります。

手順

1. Dmgr またはスタンドアロンの WSRR (`http://hostname:9060/admin`) にログインします。ユーザーおよびパスワードを入力します。
2. 「**セキュリティー、SSL 証明書、および鍵管理 (Security, SSL certficates and key management)**」にナビゲートします。
3. 「**鍵ストアと証明書 (Key Stores and Certificates)**」をクリックします。
4. 基本パターンを選択した場合は「**NodeDefaultTrustStore**」をクリックし、拡張パターンを選択した場合は「**CellDefaultTruststore**」をクリックします。
5. 「**署名者証明書 (Signer Certificates)**」をクリックします。
6. 削除する証明書のチェック・ボックスをオンにします。
7. 「**削除 (Delete)**」 をクリックします。
8. 「**保存 (Save)**」をクリックします。
9. オプション: 新しい DataPower 証明書を追加する必要がある場合は、「**追加 (Add)** 」をクリックして、新しい証明書を追加します。

ポリシー適用ポイントの構成

DataPower アプライアンスは、IBM SOA Policy Gateway Pattern のポリシー適用ポイント (PEP) です。アプリケーション・ドメインがデプロイされるとき、そのドメインのコンテンツを作成することができます。

手順

Web サービス・プロキシー (WSP) を作成します。

1. DataPower 制御パネルで「**Web サービス・プロキシー (Web Service Proxy)**」をクリックします。
2. 「**追加 (Add)**」をクリックして、プロキシーの名前を入力します。
3. 「**WSRR サブスクリプション (WSRR Subscription)**」タブを開きます。「WSRR サーバー (WSRR Server)」リストで、「**WSRRSVR**」をクリックします。
4. フロント・サイド・ハンドラー、名前空間、オブジェクト名など、必要な他の情報を指定して、Web サービス・プロキシーの構成を作成します。

WSP のポリシーを作成します。

5. WSP エディターの「**ポリシー (Policy)**」タブを開きます。
6. 適切なレベルで「**処理ルール (Processing Rules)**」をクリックします。新しいルールを作成することも、提供されているデフォルトのルールを編集することもできます。追加する重要なポリシー・アクションは、「**AAA アクション (AAA Action)**」です。これは、パターンの鍵となる識別、認証、および許可を処理します。

   AAA アクションに対して指定する必要がある重要な項目には、入力と出力、および AAA ポリシーが含まれます。 AAA ポリシー・アクションの作成プロセス中にポリシーを作成することも、AAA エディターを使用して前もって作成しておくこともできます。

- 識別は、ユーザーが識別されるステップです。サンプルでは、識別に使用される形式は 2 つありました。 StoreAddLTPA XML ファイアウォールでは、識別は基本認証を使用して実行されました。 StoreWSP ファイアウォールでは、識別は LTPA トークンによって提供されました。
- 認証は、ユーザーがシステムで既知のユーザーであることが証明されるステップです。選択するオプションは多数あります。サンプルでは、2 つの例を示しました。1 つ目では LDAP を使用してユーザーが検索され、2 つ目では有効な LTPA トークンを受け入れました。
- 許可は、ユーザーがリソース (この場合は Web サービス・オペレーション) に対して許可されるステップです。 XACML On Box PDP 許可を使用するには、以下の重要なエレメントが指定される必要があります。
  - メソッド: 「**XACML の許可を使用する (Use XACML Authorization)**」。
  - XACML のバージョン (2.0 など)。
  - PDP タイプ (拒否ベースの PDP など)。
  - On Box PDP の使用: 「**オン (On)**」
  - PDP の名前。XACML が指定されています。
  - PDP を構成します。詳しくは、 86 ページの『DataPower の XACML PDP の変更』を参照してください。
  - AAA と XACML をバインドするためのカスタムの XSL スタイル・シート: 開始点として `apil-xacml-bindingnew.xsl` を使用します。

Redaction を使用するようゲートウェイを構成するには、次のようにします。

7. XACML の `.xml` ファイルを、編集用に適用する特定のセキュリティー・ポリシーに一致するよう変更します。
8. 編集サンプルに従う AAA アクションを使用して、XML ファイアウォールを作成します。
9. 上の AAA アクションによって使用される PDP を、編集の適用に使用しているスタイル・シートを指すよう変更します。
10. XACML サービスの SOAP ペイロードを作成する `storeCallPDP.xsl` スタイル・シートをコピーして変更します。特に、アクションとリソースが、作成した XACML ポリシー文書の要件に一致するようにします。
11. 変更したスタイル・シートが、新しい XACML XML ファイアウォールの適切なポートを呼び出していることを確認します。

次のタスク

SOA Policy Gateway Advanced Runtime および SOA Policy Gateway Basic Runtime パターンでは、ドメインを作成して WSRR サーバー構成をセットアップすることに加えて、カスタム CLI スクリプトを実行してドメインを拡張することが可能です。 CLI スクリプトは、`DomainZipFile.zip` 構造のルートに存在する必要があります。例えば、`/cli.cli` となります。 CLI は、どの標準 CLI コマンドでも実行できますが、CLI が参照するすべての成果物は、存在しているか、パターンによって作成された DataPower ドメインからアクセス可能である必要があります。 SOA Policy Gateway Advanced Runtime または SOA Policy Gateway Basic Runtime パターンのインスタンスをデプロイするとき、セキュリティー・パッケージ・パラメー

ター内の CLI ファイル名を入力するプロンプトが出されます。

SOA Policy Gateway Basic Runtime パターンによる作業

SOA Policy Gateway Basic Runtime パターンは、次の 3 つの主要機能で構成されています。DataPower と WSRR のパターン・スクリプトの間のセキュリティーに必要なファイルの取得、DataPower でのドメインの構成、最後にプロモーションの構成です。

完了時には、以下の処置が実施されています。

1. 新しいドメインが、指定した DataPower アプライアンスに存在します。
2. WSRR サーバー定義がドメインに存在します。
3. カスタム CLI スクリプトが、DataPower ドメインに対して実行されています。
4. WSRR サーバーが構成されています。
5. カスタマーによって提供された DataPower 署名者証明書が、WSRR セルの NodeDefaultTruststore にアップロードされています。
6. SOA Policy Gateway Basic Runtime パターンの WSRR セルと、SOA Policy Gateway Governance Master セルとの間のプロモーションが構成されています。
7. 署名者証明書が交換されています。Governance Dmgr の署名者証明書が、Basic セルの NodeDefaultTrustStore に配置され、Basic セル Dmgr の署名者証明書が、Governance セルの CellDefaultTrustStore に配置されています。
8. LTPA 鍵が交換されています。Governance セルの LTPA 鍵が、Basic セルにインポートされています。
9. Governance Master の WSRR クラスターの各ホストが、Basic セルのトラステッド・レルムに追加されています。Basic セルの WSRR クラスターの各ホストが、Governance Master のトラステッド・レルムに追加されています。
10. 所定の入力でステージング環境または実動環境としてセルが指定された場合は、プロモーション・プロパティー・ファイルが構成されています。

完全にセキュアな実動環境を完成させるには他のステップを実行する必要がありますが、ここで実行した構成により、以下を行うことが可能になります。

1. サービスとポリシーを作成し、WSRR で SOA ポリシー・ライフサイクルを介してそれらのガバナンスを実施します (ステージング環境と実動環境が設定された場合)。これは、デフォルトの GEP を使用して行います。
2. サブスクリプションを作成するために、事前に作成された WSRR サーバー定義を使用できる、Web サービス・プロキシーを作成します。

SOA Policy Gateway Advanced Runtime パターンによる作業

SOA Policy Gateway Advanced Runtime パターンは、次の 3 つの主要機能で構成されています。DataPower と WSRR のパターン・スクリプトの間のセキュリティーに必要なファイルの取得、DataPower でのドメインの構成、最後にプロモーションの構成です。

完了時には、以下の処置が実施されています。

1. 新しいドメインが、指定した DataPower アプライアンスに存在します。

2. WSRR サーバー定義がドメインに存在します。
3. カスタム CLI スクリプトが、DataPower ドメインに対して実行されています。
4. n 個のノードがある WSRR クラスター環境が、作成および構成されています。
5. カスタマーによって提供された DataPower 署名者証明書が、WSRR セルの CellDefaultTruststore にアップロードされています。
6. SOA Policy Gateway Advanced Runtime パターンの WSRR セルと、SOA Policy Gateway Governance Master セルとの間のプロモーションが構成されています。
   a. 署名者証明書が交換されています。Governance Dmgr の署名者証明書が、Advanced セルの CellDefaultTrustStore に配置され、Advanced セル Dmgr の署名者証明書が、Governance セルの CellDefaultTrustStore に配置されています。
   b. LTPA 鍵が交換されています。Governance セルの LTPA 鍵が、Advanced セルにインポートされています。
   c. Governance Master の WSRR クラスターの各ホストが、Advanced セルのトラステッド・レルムに追加されています。Advanced セルの WSRR クラスターの各ホストが、Governance Master のトラステッド・レルムに追加されています。
   d. 所定の入力でステージング環境または実動環境としてセルが指定された場合は、プロモーション・プロパティー・ファイルが構成されています。

現時点の構成で、以下を行うことができます。

1. サービスとポリシーを作成し、WSRR で SOA ポリシー・ライフサイクルを介してそれらのガバナンスを実施します (ステージング環境と実動環境が設定された場合)。これは、デフォルトのガバナンス有効化プロファイル (GEP) を使用して行います。
2. サブスクリプションを作成するために、事前に作成された WSRR サーバー定義を使用できる、Web サービス・プロキシーを作成します。

次に、追加のステップを実行して、完全にセキュアな実動環境を完成させる必要があります。詳しくは、55 ページの『IBM SOA Policy Gateway Pattern パターンのセキュリティー』を参照してください。

Basic Runtime パターンおよび Advanced Runtime パターンで作成される DataPower オブジェクト

SOA Policy Gateway Basic Runtime パターンおよび SOA Policy Gateway Advanced Runtime パターンで作成される DataPower オブジェクトとそれぞれの機能の概要。

表 37. DataPower パターン・オブジェクト

オブジェクト	説明
ドメイン	ユーザー・アプリケーション用に使用できるドメイン。
WSRR サーバー	指定された WSRRSVR。 SOAP URL、ユーザー、パスワード、および妥当性検査の資格情報のある SSL プロキシー・プロファイルが構成されます。
SSL プロキシー・プロファイル	指名された WSRRPP。これはフォワード (クライアント) プロファイルです。これは暗号プロファイル WSRRCP を使用します。他のすべてのデフォルトが使用されます。

表 37. *DataPower* パターン・オブジェクト *(続き)*

オブジェクト	説明
暗号プロファイル	WSRRCP には、パターン・スクリプトの一部としてアップロードされた署名者証明書を含む、妥当性検査の資格情報オブジェクト WSRRVC があります。
妥当性検査の資格情報	WSRR 妥当性検査の資格情報には、暗号証明書 WSRRCERT が含まれます。その他すべての設定はデフォルトです。
暗号証明書	WSRRCERT は、署名者の証明書を利用します。この証明書は、単一サーバー用のデフォルトの証明書である NodeDefaultKeyStore から抽出されたものか、 IBM HTTP Server が存在した ND 環境の場合は CMSKeyStore デフォルト証明書です。

Web サービス・プロキシーでの WSRR サーバー定義の使用例:

1. DataPower 制御パネルで「**Web サービス・プロキシー (Web Service Proxy)**」をクリックします。
2. 「**追加**」をクリックして、プロキシーの「**名前**」を入力します。
3. 次に、「**WSRR サブスクリプション (WSRR Subscription)**」タブを選択します。
4. メニューから WSRR サーバーを選択します。 WSRRSVR オブジェクトが選択可能です。
5. フォント・サイズ、ハンドラー、名前空間、オブジェクト名などの情報を提供して、Web サービス・プロキシーの構成を作成します。

サービスの作成およびガバナンス

WSRR Business Space ユーザー・インターフェースを使用して、ビジネス・サービスおよびそれぞれに関連するオブジェクトを作成および制御します。

ポリシーを作成するには、その前にビジネス・スペースに SOA ガバナンス・スペースを作成しておく必要があります。 SOA ガバナンス・スペースを作成していない場合は、 100 ページの『初回使用時の Business Space の構成』を参照し、スペースを作成するための手順に従います。

新しい制御されたサービスの作成について詳しくは、IBM WebSphere Service Registry and Repository バージョン 8.0 インフォメーション・センター - チュートリアル: 新規サービスの管理を参照してください。

既存サービスの制御について詳しくは、IBM WebSphere Service Registry and Repository バージョン 8.0 インフォメーション・センター - チュートリアル: 既存サービスの管理を参照してください。

関連タスク:

98 ページの『WSRR への接続 - Business Space』
Business Space ユーザー・インターフェースを使用して、ポリシーを管理します。

ポリシー

メディエーション・ポリシーを作成する際に、WSRR を「ポリシー・オーサリング・ポイント (Policy Authoring Point)」として、また WebSphere DataPower を「ポリシー実施ポイント (Policy Enforcement Point)」として使用するための実装の詳細を説明します。

WSRR のポリシー

WSRR を使用して、SLA (サービス・レベル・アグリーメント) ポリシー、メディエーション・ポリシー、モニタリング・ポリシー、カスタム・ポリシーなどのすべての SOA ポリシーと、今後サポートされる他のポリシー・ドメインを作成することができます。 Business Space ユーザー・インターフェースを使用すると、WSRR でポリシー文書を作成、更新、または削除することができます。ポリシー文書には、特定のポリシー・ドメインに対していくつかのポリシーを指定するポリシー式を含めることができます。あるいは、他の文書から既存のポリシーをアセンブルするポリシー文書を作成することもできます。個々のポリシーは、ポリシーを文書に追加する際に指定したポリシー ID を使用して参照されます。ポリシー式はポリシーの宣言を表し、WS-Policy 文書の `<wsp:Policy>` 要素に相当します。

Business Space でメディエーション・ポリシーを作成する手順については、 114 ページの『新しいポリシーのオーサリング』を参照してください。

メディエーション・ポリシー・アサーション

サービス・レベル・アグリーメント (SLA) は、サービスの提供するサービス品質が指定された標準に合致することを必須とするビジネスの要件に基づいています。サービスが設計される間に、サービスの動作のロジックをガイドするための機能要件が作成されます。それと同時に、サービスの分析や設計の一環として非機能要求を指定して、サービスに期待されるサービスの品質を指定する必要があります。例えば、ビジネスに、顧客のインターネット照会に応じて情報を提供するサービスがあるとします。目標は、3 秒以内に応答を返すことです。エンドツーエンド・トランザクションの設計の一環として、ビジネスの非機能要件を満たすためには、このサービスが 2 秒以内に情報を返す必要があると判断されます。

サービスがその SLA に合致することを保証するため、サービスのパフォーマンスに関するランタイム・チェックを実装し、SLA に合致しない場合にはアクションを実行するポリシーを作成することができます。例えば、通常 (全体の時間の 95%) は 2 秒以内にサービス応答を提供できる、サービスの 1 次エンドポイントがあるとします。 SOA 設計者は、2 次エンドポイントを別のサーバー上に作成しました。通常、この 2 次エンドポイントは、1 次エンドポイントで障害が発生した際のホット・スタンバイとして使用されますが、1 次エンドポイントがトランザクションの負荷に対応しきれない場合に、オーバーフローしたトラフィックに対して使用されることも許可されています。サービス応答時間を検査して、SLA に合致する必要がある場合にトラフィックを再経路指定するポリシーを作成できます。

ランタイム・ポリシーによって SLA が保守されるもう 1 つの例は、それぞれ優先順位レベルが異なる多様なコンシューマーを持つトランザクションにサービスが応答している場合です。単純な例として、「Gold」および「Bronze」の顧客がいて、「Gold」の顧客に対してのみ特定のサービスの品質を保証する場合を考えます。この例では、コンシューマーが「Gold」であるかどうかを検査し、そうであれば 2 次エンドポイントへ再経路指定します。「Bronze」の顧客は、それより低速の応答時間で対応することになります。ビジネスでこの決定が下される理由は、「Bronze」の顧客に「Gold」の顧客の SLA に合致する応答時間を提供するための費用に対して、得られる増分収益が不十分であるためです。

3 つ目の例として、サービスが可能な限り十分機能しても、負荷がかかっていると判断される場合には、優先順位の低いコンシューマー・サービスからのメッセージをキューに入れたり、拒否したりする場合があります。例えば、予期しない時間のコンシューマー要求で、バッチ・ルーチンによってシステムがフラッディングしてしまう場合が挙げられます。サービスの品質を守るために、営業時間中にのみ有効になるランタイム・ポリシーを作成して、この時間内はすべてのバッチ要求を拒否することができます。

より一般的には、メディエーション・ポリシーを使用して、クライアント (コンシューマー) からの着信メッセージに対して妥当性検査と変換を行ってから、サーバー (プロバイダー) に表示することができます。

ポリシーはこのタイプのメッセージの妥当性検査や変換をサポートします。ポリシーは、プロバイダー・サービスに対してのみ指定することも、特定のコンシューマーとプロバイダーのペアや、プロバイダー・サービスの匿名コンシューマーに対して指定することもできます。匿名の顧客に対するポリシーによって、他のポリシーが適用されないコンシューマーに対してのみ適用されるデフォルト・ポリシーを定義することができます。このフィーチャーを使用すると、自身を明らかにしない不正なコンシューマーに対してポリシーを指定することができます。それによって、そのようなコンシューマー・サービスのトランザクションを拒否することができます。これは、プロバイダー・サービスをダウンさせる目的でシステムをトランザクションでフラッディングさせようとするコンシューマー・ハッカーからのサービス妨害攻撃を防ぐのに役立ちます。

メディエーション・ポリシーの条件

メディエーション・アサーションを作成して、ランタイム・ポリシーによって、サービスの SLAを制御したり、コンシューマーからプロバイダーへのメッセージを変換したり、コンシューマー・メッセージのメッセージ・スキーマを妥当性検査したりすることができます。

メディエーション・ポリシーの特殊なタイプである SLA ポリシー条件は、条件を指定した従来の if-then-else 構造を効率的に使用して、その条件の評価に基づいて一連のアクションが実行されるようにします。条件の指定はオプションです。条件が指定されない場合は、True に評価される論理条件と同等と評価され、指定されたアクションがそれに応じて実施されます。

条件が指定される場合、その条件はブール式またはスケジュール仕様のいずれかで構成する必要があります。これら両方を含むこともできます。

スケジュール

スケジュールを指定する場合、そのスケジュールはポリシーが有効になる時点を特定します。指定される日時はローカルの「ポリシー実施ポイント (Policy Enforcement Point)」によって評価され、使用されるタイム・ゾーンはその「ポリシー実施ポイント (Policy Enforcement Point)」のタイム・ゾーンになります。スケジュールが指定されない場合、ポリシーは「ポリシー・オーサリング・ポイント (Policy Authoring Point)」から「ポリシー実施ポイント (Policy Enforcement Point)」にダウンロードされるとすぐに開始し、無期限に続行されます。

スケジュールでは、オプションの開始日とオプションの停止日、オプションの日次時間フレーム、およびオプションの曜日のリストを定義します。例えば、2012 年 10 月 1 日から 2012 年 10 月 30 日までの毎週水曜日と日曜日に、午前 8 時から午後 5 時まで有効になるようにスケジュールを定義できます。

このスケジュールに指定可能なパラメーターは、以下のとおりです。

- **StartDate** - このオプション属性は、スケジュールが有効になる日付を xs:date 形式で指定します。「StartDate」に指定された日付から有効になり、この属性が指定されない場合、スケジュールは即日有効になります。

  注: xs:date ハイパーリンクをクリックして、この業界標準について理解してください。
- **StopDate** - このオプション属性は、スケジュールが有効でなくなる日付を xs:date 形式で指定します。「StopDate」に指定された日付は有効期間には含まれないため、開始日よりも後の日付を指定する必要があります。停止日が開始日と同じかそれより前の日付である場合、スケジュールは有効になりません。この属性が指定されない場合、スケジュールは無期限で有効になります。
- **Daily** - このオプション要素は、スケジュールが有効になる日次時間フレームを指定します。この要素が指定されない場合、スケジュールは終日有効になります。
  - **StartTime** –「Daily」を指定した場合、この属性は必須です。この属性は、スケジュールの日次開始時刻を xs:time 形式で指定します。 (注: xs:time ハイパーリンクをクリックして、この業界標準について理解してください。)
  - **StopTime** -「Daily」を指定した場合、この属性は必須です。この属性は、スケジュールの日次停止時刻を xs:time 形式で指定します。「StopTime」に指定された時刻は有効期間に含まれないため、日次開始時刻と同じかそれより前の時刻が指定された場合、スケジュールは翌日の指定された停止時刻に停止します。
- **Weekdays** - このオプション・エレメントは、スケジュールに組み込まれる曜日を指定します。この要素が指定されない場合、すべての曜日がスケジュールに組み込まれます。この要素は、スケジュールで午前 0 時を過ぎた実行が許可されている場合、日次時間フレームの開始にのみ影響を与えます。例えば、スケジュールが毎週水曜日の午後 11 時に開始し、2 時間実行するように設定されている場合、そのスケジュールは実際には木曜日の午前 1 時に終了します。
  - **Days** -「Weekdays」を指定した場合、この属性は必須です。スケジュールに組み込まれる曜日を、正符号 (「+」) で区切った名前としてリストします。例: 「Monday+Tuesday+Wednesday+Thursday+Friday+Saturday+Sunday」。

メディエーション・ポリシーの条件式

条件式が指定される場合、それはブール式を指定する非反復要素になります。

この式は、「Attribute」、「Operator」、および「Value」の 3 つの必須パラメーターと、オプションの「Interval」および「Limit」で構成されます。「Attribute」および「Value」(該当する場合は、これらに加えて「Interval」および「Limit」) への「Operator」の適用が True に評価されると、式は True に評価されます。「Limit」要素は、「HighLow」演算子および「TokenBucket」演算子と一緒にのみ使用されます。「Limit」が指定されない場合、値は 0 になります。「Interval」が指定されない場合、デフォルトは 60 秒になります。

式に指定可能なパラメーターは、以下のとおりです。

- **Attribute** - 以下の表に、定義される属性とそれぞれのタイプをまとめます。

表 38. 定義される属性

属性	**説明とタイプ**
ErrorCount	モニタリング間隔の間に確認された障害の数。
MessageCount	モニタリング間隔の間にインターセプトされたメッセージの実際の数。
InternalLatency	秒単位の内部待ち時間 (処理時間)。
BackendLatency	秒単位のアプライアンスからサーバーに対する待ち時間。
TotalLatency	秒単位のバックエンドと内部待ち時間の合計。

- **Operator** - 以下の表に、使用可能な演算子とそれぞれの意味をまとめます。

表 39. 演算子

演算子	**意味**
GreaterThan	定義された「Value」よりも「Attribute」が大きい場合に True に評価される、単純な数値アルゴリズム。
LessThan	定義された「Value」よりも「Attribute」が小さい場合に True に評価される、単純な数値アルゴリズム。
TokenBucket	バーストを許容するレート・ベースのアルゴリズム。このアルゴリズムは、トークンの最大容量「Limit」を持つバケットで構成されます。「Attribute」単位ごとにトークンが 1 つ除去される一方で、バケットには「Interval」ごとに一定レートで「Value」個のトークンが入れられます。このアルゴリズムは、バケットにトークンが入っていない場合に True に評価され、それ以外の場合は False に評価されます。このアルゴリズムの説明に役立つ例を示します。 Limit=100、Value=5、Interval=1 秒、および Attribute=MessageCount と想定します。 1. バケットは、最大容量 100 トークンによる満杯状態で開始されます。 2. メッセージが到着すると、アルゴリズムはバケットにトークンが入っているかどうかを検査します。 a. 入っている場合、アルゴリズムは False に評価され、バケットから 1 つのトークンが除去されます。 b. 入っていない場合、アルゴリズムは True に評価されます。 3. その間、アルゴリズムは容量の許す限りバケットに毎秒 5 つのトークンを追加します。
HighLow	「Attribute」が「Value」として指定された上限しきい値に達すると True に評価され、「Attribute」が「Limit」として指定された下限しきい値に達するまで True に評価され続けるアルゴリズム。

- **Value** – これは正整数要素です。「0」は有効です。
- **Interval** - このオプション要素は、式を評価するときに「wsme:Attribute」を測定するためにスライディング・ウィンドウとして使用される時間間隔を xs:duration の形式で定義します。これを指定しない場合、60 秒の間隔が使用されます。指定する場合は、構成される「ポリシー実施ポイント (Policy Enforcement Point)」の機能も考慮して、合理的な値を指定してください。つまり、この値が大きいほど、「ポリシー実施ポイント (Policy Enforcement Point)」が属性を追跡するために必要とするメモリーの量が多くなります。

  注: xs:duration ハイパーリンクをクリックして、この業界標準について理解してください。
- **Limit** - このオプション整数要素は、「wsme:Operator」が「TokenBucket」または「HighLow」である場合に必要な、追加の「Limit」引数を定義します。単位は、指定された「wsme:Operator」に応じて決まります。

  「wsme:Operator」が「HighLow」である場合、この要素で下限しきい値を、「wsme:Value」で上限しきい値を定義します。「wsme:Value」のしきい値よりも小さいしきい値を指定してください。指定されない場合のデフォルトの「Limit」の値は「0」です。

  「wsme:Operator」が「TokenBucket」である場合、このエレメントでバーストの最大サイズ、つまりバケット内のトークンの最大数を定義します。一方、「Value」でバケットが入れられるレートを「Interval」ごとのトークン数として指定します。指定されない場合のデフォルトの「Limit」の値は「0」であり、その場合「TokenBucket」は「GreaterThan」演算子に相当します。

メディエーション・ポリシーのアクション

メディエーション・アクション要素は、実行されるアクションを指定します。構文ではさまざまな組み合わせが許可されますが、それらのすべてが必ずしも意味を持つわけではなく、矛盾するアクション (メッセージをキューに入れることと拒否することがいずれも要求されるなど) が指定された場合は、「ポリシー・オーサリング・ポイント (Policy Authoring Point)」でその振る舞いが拒否されます。許可されるメディエーション・ポリシー・アクションは、以下のとおりです。

- **QueueMessage** – このアクションは、論理条件が合致したときにトランザクションがキューに入れられることを指定します。メッセージ処理は、論理条件が合致しなくなるまで再開されません。キューの方法とそれに関連するタイムアウトは、「ポリシー実施ポイント (Policy Enforcement Point)」(この場合は WebSphere DataPower) によって定義されます。単一の「Action」要素で複数のアクションが指定される場合、「QueueMessage」は最初のアクションでなければなりません。
- **RejectMessage** – このアクションは、論理条件が合致したときにトランザクションが拒否されることを指定します。トランザクションは、論理条件が合致しなくなるまで、拒否され続けます。トランザクションが拒否されると、クライアント (コンシューマー) サービスに SOAP 障害が返されます。単一の「Action」要素で複数のアクションが指定される場合、「RejectMessage」は最初のアクションでなければなりません。「QueueMessage」と「RejectMessage」を同時に指定することはできません。

- **Notify** - このオプション要素は、論理条件が合致したときに、通知を生成することを指定します。 WebSphere DataPower の場合、メッセージは DataPower システム・ログに書き込まれます。
- **RouteMessage** - このオプション要素は、論理条件が合致したときに、指定のエンドポイント宛先にメッセージを経路指定することを指定します。メッセージは、論理条件が合致しなくなるまで、指定のエンドポイント宛先に引き続き経路指定されます。
  - **EndPoint** – このパラメーターは、「RouteMessage」のアクションが指定された場合に必須です。サポートされるエンドポイントの値には、IP アドレス、ホスト名、または仮想ホスト (ロード・バランサー・グループなど) があります。
- **ValidateMessage** - このオプション要素は、指定の文法に照らしてメッセージを妥当性検査することを指定します。妥当性検査が失敗すると、メッセージは拒否されます。「ValidateMessage」を指定する場合は、サブパラメーターとして「XSD」または「WSDL」のいずれかを指定する必要があります。「SCOPE」はオプションであり、指定されない場合は「SOAPBody」が妥当性検査に使用されます。
  - **XSD** - メッセージに含まれる URI で識別される XML スキーマに照らしてメッセージを妥当性検査することを指定します。
  - **WSDL** - メッセージに含まれる URI で識別される Web サービス記述 (WSDL) に照らしてメッセージを妥当性検査することを指定します。
  - **SCOPE** – メッセージのどの部分を妥当性検査するかを指定します。以下の表に、指定可能な値とそれぞれの意味をリストします。

表 40. 「ValidateMessage」要素

値	説明
SOAPBody	SOAP Body 要素の内容。SOAP 障害に関する特別な処理はありません。(デフォルト)
SOAPBodyOrDetails	SOAP 障害の詳細要素の内容。それ以外の場合は、Body の内容。
SOAPEnvelope	SOAP メッセージ全体 (エンベロープも含む)。
SOAPIgnoreFaults	メッセージが SOAP 障害の場合は妥当性検査なし。それ以外の場合は SOAP Body の内容。

- **ExecuteXSL** - 指定されたスタイル・シートおよびパラメーターを使用して XSL 変換を実行することを指定します。実行が失敗するとトランザクションは拒否されます。「Stylesheet」情報の指定は必須ですが「Parameters」はオプションであり、指定された特定のスタイル・シートの必要に応じて指定します。
  - **Stylesheet** - 変換操作で、含まれる URI で指定されるスタイル・シートが使用されることを指定します。スタイル・シートは、XSLT ファイルでなければなりません。
  - **Parameter** - このオプションの反復要素は、ExecuteXSL 操作に使用するスタイル・シート・パラメーターを指定します。
    - **Name** – この属性は、対応する「Parameter」パラメーターごとに必要であり、パラメーターの名前を指定します。
    - **Value** - この属性は、対応する「Name」パラメーターごとに必要であり、パラメーターの値を指定します。

新しいポリシーのオーサリング

Business Space ユーザー・インターフェースでメディエーション・ポリシーをオーサリングする場合、ポリシーの条件とアクションを指定します。

始める前に

Business Space へのアクセスについて詳しくは、 98 ページの『WSRR への接続 - Business Space』を参照してください。

SOA ガバナンス・スペースは、ポリシーの作成前に作成する必要があります。SOA ガバナンス・スペースを作成していない場合は、 100 ページの『初回使用時の Business Space の構成』を参照し、スペースを作成するための手順に従います。

このタスクについて

SOA ガバナンス・スペースを使用して、新しいポリシーをオーサリングします。

手順

1. SOA ガバナンス・スペースを開きます。
   a. 「**スペースに移動 (Go To Spaces)**」をクリックします。「スペースに移動 (Go To Spaces)」ダイアログが表示されます。
   b. SOA ガバナンス・ユーザーのスペースをクリックします。具体的な名前は、スペースの作成時に指定された内容に基づきます。
2. 「概要 (Overview)」タブで、「**メディエーション・ポリシーの作成 (Create a Mediation Policy)**」をクリックします。
3. 意味のある名前とオプションの説明を入力します。
4. 必要に応じて、条件とアクションを追加します。 条件とアクションについて詳しくは、 108 ページの『ポリシー』および IBM WebSphere Service Registry and Repository バージョン 8.0 インフォメーション・センター - メディエーション・ポリシーの作成を参照してください。
5. 「**終了 (Finish)**」をクリックします。

タスクの結果

ポリシーが作成され、WSRR に保存されました。今作成したポリシーのポリシー文書を表示するには、画面の左下にある「サービス・レジストリー・ナビゲーター (Service Registry Navigator)」ウィジェットで、ポリシー文書を選択します。または、指定した名前を、最後の `.xml` も含めて検索します。ポリシー文書が、右側の「サービス・レジストリーの詳細 (Service Registry Detail)」ウィジェットに表示されます。

関連概念:

108 ページの『ポリシー』
メディエーション・ポリシーを作成する際に、WSRR を「ポリシー・オーサリング・ポイント (Policy Authoring Point)」として、また WebSphere DataPower を「ポリシー実施ポイント (Policy Enforcement Point)」として使用するための実装の詳細を説明します。

関連情報:

IBM WebSphere Service Registry and Repository バージョン 8.0 インフォメーション・センター - メディエーション・ポリシーの作成

ポリシーの管理

Business Space ユーザー・インターフェースを使用して、ポリシーを編集または削除できます。

始める前に

SOA ガバナンス・スペースを構成します。詳しくは、100 ページの『初回使用時の Business Space の構成』を参照してください。

手順

1. ポリシーのポリシー文書を開くには、画面の左下にある「サービス・レジストリー・ナビゲーター (Service Registry Navigator)」ウィジェットで、ポリシー文書を選択します。または、指定した名前を、最後の `.xml` も含めて検索します。ポリシー文書が、右側の「サービス・レジストリーの詳細 (Service Registry Detail)」ウィジェットに表示されます。
2. ポリシーの詳細を変更するには、次のようにします。
   a. このウィジェットの「編集 (Edit)」アイコンをクリックして、ポリシー文書を編集します。 ポリシーの詳細を編集するためのオプションを含むウィンドウが表示されます。
   b. ポリシーに条件やアクションがある場合、それも表示されます。必要に応じて、条件とアクションを作成して変更します。
   c. 「**終了 (Finish)**」をクリックして保存し、ポリシー・エディターを閉じます。「サービス・レジストリーの詳細 (Service Registry Detail)」ウィジェットが最新表示され、加えられた変更が表示されます。
3. ポリシーを削除するには、次のようにします。
   a. ポリシーを、ポリシー文書の編集または削除が可能なガバナンス状態に遷移します。SOA ポリシーのライフサイクルを通じたポリシーの遷移について詳しくは、116 ページの『ポリシーのライフサイクルの管理』を参照してください。
   b. 「**アクション (Action)** 」 > 「**削除 (Delete)**」をクリックします。 メニューに「削除 (Delete)」オプションがリストされます。
   c. ポリシーを削除するには、「**削除 (Delete)**」を選択します。
   d. 「**はい**」をクリックして、削除を確認します。

関連情報:

IBM WebSphere Service Registry and Repository バージョン 8.0 インフォメーション・センター

IBM WebSphere Service Registry and Repository バージョン 8.0 インフォメーション・センター - ガバナンス有効化プロファイルのポリシー

ポリシーのライフサイクルの管理

Business Space ユーザー・インターフェースを使用して、ポリシーのガバナンス状態を遷移できます。

このタスクについて

ガバナンスの詳細については、5 ページの『SOA Policy ライフサイクル』を参照してください。

手順

ポリシーを別のライフサイクル状態に遷移させるには、以下のステップを実行します。目的のライフサイクル状態に達するまで、必要な回数だけこの手順を繰り返します。

1. Business Space で、画面の左下にある「サービス・レジストリー・ナビゲーター」ウィジェットにおいて、当該ポリシーのポリシー文書を選択してそのポリシー文書を開きます。または、指定した名前を、最後の `.xml` も含めて検索します。 ポリシー文書が、右側の「サービス・レジストリーの詳細 (Service Registry Detail)」ウィジェットに表示されます。「**ガバナンス状態 (Governance state)**」プロパティーに、プロファイルの現在のガバナンス状態が表示されます。
2. 「**アクション (Action)**」をクリックします。 使用可能なライフサイクル遷移のリストが、使用可能な他の操作と共に表示されます。
3. 必要なライフサイクル遷移を選択し、ポリシーを必要な状態に移動します。 ポリシーの「**ガバナンス状態 (Governance state)**」プロパティーが更新され、新しいライフサイクル状態が表示されます。

関連概念:

5 ページの『SOA Policy ライフサイクル』
メディエーション・ポリシーは、SOA Policy ライフサイクルを使用して制御されます。 このライフサイクルは、ポリシーが最初に識別されたときから、ポリシーが実動環境にデプロイされて、ポリシーが最終的に不要になって非推奨になるときまでです。

関連情報:

IBM WebSphere Service Registry and Repository バージョン 8.0 インフォメーション・センター - SOA ポリシー・ライフサイクル

サービスに接続されたポリシー

ポリシーは、WSRR を使用してサービスに接続できます。

詳しくは、IBM WebSphere Service Registry and Repository バージョン 8.0 インフォメーション・センター - ポリシー接続タスクを参照してください。

第 7 章 トラブルシューティング

パターンのデプロイメントの前、最中、および後に発生する可能性のある問題を診断するのに役立つ情報が得られます。

以下のリンクから、パターンでの問題に関連するトピックを見つけてください。

デプロイメントの問題のトラブルシューティング

パターンを IBM SOA Policy Gateway Pattern にデプロイする際の共通する問題をトラブルシューティングできます。

デプロイメント中の DataPower への接続障害

以下の解決方法を試してみてください。

- DataPower 管理者に依頼して、ユーザーおよびパスワードが有効であることを確認してください。
  - DataPowerで、「**制御パネル (Control Panel)**」 > 「**ユーザー・アカウントの管理 (Manage User Accounts)**」と移動し、ユーザーが存在することを確認します。
  - アカウントが存在することを確認します。
  - ユーザーに、XML Management Interface を使用する特権 (例えば、システム管理者) があることを確認します。
  - DataPower 管理者は、ユーザー・アカウントがユーザー・エージェント設定 (例えば、基本認証設定など) で有効になっているかどうかを確認する必要があります。
- DataPower ホスト名が正しいことを確認します。
- DataPower XML 管理インターフェースが有効になっていることを確認します。
- 以下の SSL 接続障害に関する手順を確認し、証明書が `DomainZipFile.zip` および DataPower アプライアンスの両方に正しくインストールされていることを検証します。

相互認証クライアント認証の障害のトラブルシューティング

以下の解決方法を試してみてください。

- `DomainZipFile.zip` に正しい証明書が含まれていることを確認します。
- XML 管理インターフェースのポートの暗号プロファイルが、チェーン内のすべての証明書を備えた妥当性検査の資格情報を保持していることを確認します。
- クライアント公開鍵とクライアント公開証明書のパスワードが正しいことを確認します。

サーバー認証の障害のトラブルシューティング

以下の解決方法を試してみてください。

- 使用中の DominZipFile.zip ファイルの *yourDataPowerHostName* ディレクトリーに、チェーン内のすべての証明書が存在することを確認します。
- SSL プロキシー・プロファイルに、証明書チェーンを持つ ID 資格情報を含んだリバース暗号プロファイルがあることを確認します。

既存ドメインのエラーのトラブルシューティング

以下の解決方法を試してみてください。

- DataPower 制御パネルで、アプリケーション・ドメインを開きます。ドメインが既存であるかどうかを確認します。

サンプル・アプリケーションのポート・オーバーラップ・エラーのトラブルシューティング

サンプル・サービスの 1 つが使用不可になっている場合、ドメイン内のポートが他のドメインと競合していないかどうかを確認します。

以下の解決方法を試してみてください。

- DataPower にサインインして、サンプル・ドメインに切り替えます。次に、「制御パネル (Control Panel)」を開いて、「XML ファイアウォール」アイコンをクリックします。「XML ファイアウォール」がすべて「稼働 (Up)」状態にあることを確認します。
- 「HTTP フロント・サイド・ハンドラー (HTTP Front Side Handler)」を探します。単一の「HTTP フロント・サイド・ハンドラー (HTTP Front Side handler)」が「稼働 (Up)」状態にあることを確認します。

SCP への接続障害のトラブルシューティング

以下の解決方法を試してみてください。

- SCP ホスト名が正しいことを確認します。
- SCP ユーザーが正しいことを確認します。
- SCP パスワードが正しいことを確認します。
- 指定された情報を使用して、IBM Workload Deployer または IBM PureApplication System 環境のノードから手動で SCP をテストします。

SCP からの DomainZipFile.zip ファイルの取得または欠落成果物のデバッグの際の障害のトラブルシューティング

以下の解決方法を試してみてください。

- URI に DomainZipFile.zip が存在することを確認します。
- ログ障害で指摘されたファイルが DomainZipFile.zip ファイルの正しい場所にあることを確認します。特に、必要な証明書が正しいディレクトリーにあることを確認してください。

プロモーション障害のトラブルシューティング

デプロイメント時に Governance Master への接続に失敗するなど、プロモーション中に発生する可能性のある問題は多数あります。

以下の解決方法を試してみてください。

- 以下のようにしてパラメーターを確認します。
  - Governance Master WSRRCELL のユーザーを確認します。
  - Governance Master WSRR Cell のユーザーのパスワードを確認します。
  - WSRR Governance Master Cell のホスト名を確認します。
  - WSRR Governance Master Cell のセル名を確認します。
- 以下のようにして、署名者証明書の交換を確認します。
  - 「Governance Master Cell」の「セルのデフォルト・トラストストア (Cell Default Trust Store)」に移動し、ランタイム環境 SOA Policy Gateway Basic Runtime または SOA Policy Gateway Advanced Runtime の Dmgr またはスタンドアロン・サーバーの証明書エントリーがあることを確認します。
  - それぞれのランタイム環境 SOA Policy Gateway Basic Runtime または SOA Policy Gateway Advanced Runtime に移動し、「CellDefaultTrust ストア (CellDefaultTrust store)」(ND 環境の場合) または「NodeDefaultTrustStore」(WSRR スタンドアロン・サーバーの場合) で Governance Master の Dmgr の証明書があることを確認します。
  - 両方のセルから同じパスワードを使用して LTPA 鍵をエクスポートし、それらが同じである (例えば、バイト数など) ことを確認します。
- プロモーション・プロパティー・ファイルのサーバー・セクションに、適切なホストおよびポート、さらにユーザーおよびパスワードの情報が指定されていることを確認してください。この情報は、以下の手順で、Governance Master の ServiceRegistry コンソールで見つけることができます。
  - 「GovernanceMasterDMgrHost」または「ServiceRegistry」に移動して、「構成 (Configurations)」パースペクティブに切り替えます。「アクション (Actions)」セクションで、「**プロモーション (Promotion)**」を見つけてプロモーション・プロパティー・ファイルを開きます。環境ごとに、ステージング WSRR ノードまたはクラスターの各サーバーに関する XML 要素があります。実動のクラスターまたはノードがある場合は、それぞれに server:port エントリーがあり、さらにユーザーおよびパスワードの情報があるはずです。
- 「サービス・バージョン (Service Version)」と「SOAP エンドポイント (SOAP Endpoint)」の両方に、「ステージング (staging)」および「実動 (Production)」の「種別 (Classification)」があることを確認します。
  - サービス・レジストリー・コンソールで、「SOA ガバナンス (SOA Governance)」パースペクティブを選択します。「サービス・バージョン (Service Version)」を開き、「種別 (Classifications)」タブを選択します。「ステージング (Staging)」および「実動 (Production)」が有効になっていなければなりません。

カスタマイズした CLI の障害のトラブルシューティング

以下の解決方法を試してみてください。

- DataPower ドメインで、defaultLog でエラー・メッセージを確認します。
- CLI デバッグを有効にして、追加の CLI を実行する前に、これらのログを確認します。

DataPower 証明書欠落が原因の SSL 障害のトラブルシューティング

DomainZipFile.zip ファイル内に、DataPower 証明書ディレクトリーの正しいホスト名が提供されていない場合、DataPower ホストで相互認証またはサーバー認証が有効になっていると、スクリプト・パッケージの WSRR サーバーへの接続が失敗します。

WSRR/DataPower 接続問題のトラブルシューティング

Web サービス・プロキシーの WSDL の状況が、「ダウン (Down)」または「同期中 (Synchronizing)」状態であり「良好 (Okay)」に切り替わらない場合は、以下を確認してください。

1. 暗号証明書が WSRR サーバー (WSRRSVR) に対して有効であることを確認します。
2. DataPower で、WSRR サーバーまたは Dmgr のホスト名を認識するように DNS が正しくセットアップされていることを確認します。
3. DNS に誤りがある場合の一時的な回避策は、WSRR サーバー定義の URL を、その URL 内のホスト名の IP に置き換えて、直接 IP を指すように変更することです。
4. 「WSRR サブスクリプション」に移動し、以下の手順で手動による同期を行います。
   a. default.log で、WSRR サーバーの接続に関するエラーを調べます。
5. 必要な証明書が、DataPower Appliances XMLManagement Interface SSL プロキシー・プロファイルの暗号プロファイルに関する ID 資格情報の証明書と一致することを確認します。

デプロイされたインスタンスの問題のトラブルシューティング

デプロイされたインスタンスに共通する問題をトラブルシューティングできます。

LDAP への接続障害

サンプルで LDAP 障害を診断する場合には、以下の解決方法を試してみてください。

- DataPower 制御パネルの「トラブルシューティング (Troubleshooting)」で、トレースがデバッグ・モードであることを確認します。
- 「StoreAddLTPA」に移動して「プローブの詳細 (Probe details)」を開き、プローブを有効にします。
- クライアント・テストを実行します。
- プローブでログを表示します。LDAP バインド障害メッセージを探します。
- LDAP ホスト名を確認します。
- LDAP DN (例: cn=root,dc=ibm.com) を探します。
- LDAP パスワード (例: passw0rd) を確認します。
- LDAP ポートが 389 (非セキュア) であることを確認します。

- ConsumerX、ConsumerA、ConsumerB の入力パスワードがすべて passw0rd であることを確認します。 LDIF ファイルのインポートに正しいパスワードが転記されていることを確認します。

LDAP サーバーまたは DataPower StoreWSP ポートへの接続障害

DataPower ログに、LDAP または StoreWSP ゲートウェイに対する接続エラーが示されており、ホスト別名を使用している (例えば、スクリプト・パッケージの以下のパラメーターのいずれか 1 つに、完全修飾ホスト名 xyz.company.com の代わりに xyz を使用している) 場合、ドメイン設定時に問題が生じる可能性があります。

- DataPower ホスト名
- LDAP ホスト名

以下の解決方法を試してみてください。

1. DataPower 管理コンソールで、デフォルト・ドメインに切り替えます。
2. 「DNS 設定の構成 (Configure DNS Settings)」を検索します。
3. 「ドメインの検索 (Search Domains)」タブをクリックします。
4. ご使用のドメイン (例: company.com) がリストに表示されていることを確認します。表示されていない場合は、「追加」をクリックしてリストに追加してください。

診断情報の収集

ログを使用すると、問題の検出と解決に役立ちます。ログはアプライアンス上に保管され、ユーザー・インターフェースからそれらを表示したり、ローカル・ファイル・システムにダウンロードしたりすることができます。

手順

診断情報を収集するには、以下のステップを実行します。

1. 仮想インスタンスを表示します。
   a. 「**インスタンス**」 > 「**仮想システム**」をクリックします。
   b. 「仮想システム・インスタンス」ウィンドウ内のインスタンスのリストから、インスタンスを選択します。
2. WSRR 仮想マシンの場合:
   a. 「**仮想マシン**」セクションで、WSRR 仮想マシンを展開し、「**スクリプト・パッケージ**」セクションでエラーがないかどうか調べます。スクリプト・パッケージにエラーがある場合は、そのスクリプト・パッケージ名の横にある **remote_std_out.log** および **remote_std_err.log** のログ・リンクをクリックしてください。
   b. WSRR インスタンスにログインし、サーバーのエラーを確認します。
   c. 次の WSRR トラブルシューティング・ガイドを参照してください。
      http://pic.dhe.ibm.com/infocenter/sr/v8r0/topic/com.ibm.sr.doc/cwsr_troubleshootingandsupport.html
3. DataPower の場合:
   a. パターンによって作成されたドメインの **default.log** ファイルを取得します。

b. デフォルト・ドメインの **default.log** ファイルを取得します。

第 8 章 保守およびサポート

緊急フィックスの適用などの保守機能を実行できます。

緊急フィックスのカタログへの追加

インテリム・フィックスおよびフィックスパックは、緊急フィックスとして仮想システム・インスタンスに適用されます。緊急フィックスをカタログに追加して、仮想イメージに適用されるようにすることができます。

始める前に

以下のステップを実行するには、*「新規カタログ・コンテンツの作成」*権限が割り当てられているか、またはすべての権限を持つ IBM Workload Deployer アプライアンスの*管理者* ロールが割り当てられている必要があります。

このタスクについて

フィックスは IBM またはイメージ・プロバイダーから提供されており、ダウンロードする必要があります。新しいフィックスは、IBM Fix Central からダウンロードします。その後、フィックスをカタログにアップロードし、該当するすべての仮想システム・インスタンスに適用することができます。

手順

以下のステップを実行して、カタログに緊急フィックスを追加します。

1. Fix Central で、緊急フィックスを探してダウンロードします。
2. オプション: 一度に複数のインテリム・フィックスを追加できます。複数のフィックスを一度に追加するには、Fix Central から複数の圧縮ファイルをダウンロードし、それらを 1 つの圧縮ファイルにパッケージします。
3. メニューから、**「カタログ」** > **「緊急フィックス」**を選択します。
4. 左パネルで追加アイコンをクリックします。
5. 追加するフィックスの名前を入力します。オプションで、追加するフィックスの説明を追加することもできます。「緊急フィックス」ウィンドウの左パネルにフィックスが表示され、右パネルにそのフィックスに関する情報が表示されます。
6. フィックスを保管した場所を参照し、**「アップロード」**をクリックします。セキュリティー上、アップロード可能なファイルは .zip、tgz、および pak に限定されています。Red Hat RPM もサポートされています。
7. フィックスに関する情報を入力します。アクセス権をユーザーに付与し、重大度のレーティングを設定することができます。**「適用対象」**フィールドを使用して、このフィックスを適用する仮想イメージ (複数可) を指定します。

タスクの結果

緊急フィックスはカタログ内にあり、仮想システム・イメージに適用可能です。

緊急フィックスの適用

インテリム・フィックスおよびフィックスパックは、緊急フィックスとして仮想システム・インスタンスに適用されます。緊急フィックスは、ご使用の仮想システム・イメージに適用できます。

始める前に

以下のステップを実行するには、仮想システム・インスタンスに対するすべてのアクセス権限が割り当てられているか、またはすべての権限を持つアプライアンス管理者ロールが割り当てられている必要があります。サービスをスケジュールしたり適用したりするには、仮想システム・インスタンスを始動する必要があります。緊急フィックスは、カタログに追加してから、仮想システムに適用してください。

このタスクについて

新しい緊急フィックスを追加する際は、フィックスを適用可能な仮想イメージを定義します。サービス要求のスケジュール時に使用可能なフィックスのリストが、仮想システム・インスタンスの作成に使用された仮想イメージに適用可能なすべてのフィックスを使用して作成されます。フィックスが既に仮想システムに適用済みの場合、そのフィックスは「**ヒストリー**」リストに示され、使用可能なフィックスのリストにはありません。

手順

以下のステップを実行してインテリム・フィックスを適用します。

1. 「仮想システム・インスタンス」ウィンドウから、フィックスを適用する仮想システム・インスタンスを選択します。
2. 「サービスの適用」アイコンをクリックします。
3. オプション: サービス要求をスケジュールに入れます。デフォルトでは、フィックスは即時に適用されます。フィックスを後で適用するようにスケジュールするには、「**サービスのスケジュール**」をクリックして、必要な情報を入力します。
4. 「**フィックスまたはサービス・レベルを選択してください**」をクリックします。
5. 「**緊急フィックスを適用**」をクリックして、適用するフィックスを確認し、選択します。緊急フィックスは、仮想システム・インスタンス内のすべての仮想マシンに適用されます。仮想システム・インスタンスの状況で、サービスが仮想システムに適用されていることが示されます。
6. エラーがないか確認します。 以下のファイルを調べて、緊急フィックスの適用プロセスの間にエラーが発生していないことを確認します。
   - Remote_std_out.log
   - Remote_std_err.log

   これらのログ・ファイルには、「仮想システム・インスタンス」ウィンドウからアクセスできます。

第 9 章 付録

特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。

本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。 本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、または サービスのみが使用可能であることを意味するものではありません。これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。 実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒103-8510
東京都中央区日本橋箱崎町19番21号
日本アイ・ビー・エム株式会社
法務・知的財産
知的財産権ライセンス渉外

以下の保証は、国または地域の法律に沿わない場合は、適用されません。 IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態で提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示 もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。 本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。 IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、 改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、 便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものでは ありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部では ありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、 自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムと その他のプログラム (本プログラムを含む) との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、 本プログラムに関する情報を必要とする方は、下記に連絡してください。

IBM Corporation
Software Interoperability Coordinator, Department 49XA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

本プログラムに関する上記の情報は、適切な使用条件の下で使用すること ができますが、有償の場合もあります。

本書で説明されているライセンス・プログラムまたはその他のライセンス資料は、IBM 所定のプログラム契約の契約条項、IBM プログラムのご使用条件、 またはそれと同等の条項に基づいて、IBM より提供されます。

この文書に含まれるいかなるパフォーマンス・データも、管理環境下で 決定されたものです。 そのため、他の操作環境で得られた結果は、異なる可能性があります。一部の測定が、開発レベルのシステムで行われた可能性がありますが、 その測定値が、一般に利用可能なシステムのものと同じである保証はありません。さらに、一部の測定値が、推定値である可能性があります。 実際の結果は、異なる可能性があります。お客様は、お客様の特定の環境に適したデータを確かめる必要があります。

IBM 以外の製品に関する情報は、その製品の供給者、出版物、 もしくはその他の公に利用可能なソースから入手したものです。IBM は、それらの製品のテストは行っておりません。したがって、他社製品に関する実行性、互換性、またはその他の要求については確証できません。IBM 以外の製品の性能に関する質問は、それらの製品の供給者にお願いします。

IBM の将来の方向または意向に関する記述については、 予告なしに変更または撤回される場合があり、単に目標を示しているものです。

本書には、日常の業務処理で用いられるデータや報告書の例が含まれています。 より具体性を与えるために、それらの例には、個人、企業、ブランド、あるいは製品などの名前が含まれている場合があります。 これらの名称はすべて架空のものであり、 名称や住所が類似する企業が実在しているとしても、それは偶然にすぎません。

著作権使用許諾:

本書には、様々なオペレーティング・プラットフォームでのプログラミング手法を例示するサンプル・アプリケーション・プログラムがソース言語で掲載されています。お客様は、サンプル・プログラムが書かれているオペレーティング・プラットフォームのアプリケーション・プログラミング・インターフェースに 準拠したアプリケーション・プログラムの開発、使用、販売、配布を目的として、いかなる形式においても、IBM に対価を支払うことなくこれを複製し、改変し、配布することができます。このサンプル・プログラムは、あらゆる条件下における完全なテストを

経ていません。従って IBM は、これらのサンプル・プログラムについて信頼性、利便性もしくは機能性があることをほのめかしたり、保証することはできません。

この情報をソフトコピーでご覧になっている場合は、写真やカラーの図表は 表示されない場合があります。

プログラミング・インターフェース情報

プログラミング・インターフェース情報は、プログラムを使用して アプリケーション・ソフトウェアを作成する際に役立ちます。

ただし、この情報には、診断、修正、および調整情報が含まれている場合が あります。診断、修正、調整情報は、お客様のアプリケーション・ソフトウェアのデバッグ支援のために提供されています。

重要: 診断、修正、調整情報は、変更される場合がありますので、 プログラミング・インターフェースとしては使用しないでください。

商標

IBM、IBM ロゴ、および ibm.com® は、世界の多くの国で登録された International Business Machines Corp. の商標です。 他の製品名およびサービス名等は、それぞれ IBM または各社の商標である場合があります。 現時点での IBM の商標リストについては、http://www.ibm.com/legal/copytrade.shtml をご覧ください。

この製品には、Eclipse Project (http://www.eclipse.org/) により 開発されたソフトウェアが含まれています。

Java およびすべての Java 関連の商標およびロゴは Oracle やその関連会社の米国およびその他の国における商標または登録商標です。

IBM へのコメントの送付

本書に対するご意見ご感想は、以下にリストされているいずれかの方法を使用して、IBM へお送りください。

具体的なエラーまたは脱落と考えられるものや、本書に関する正確性、編成、主題、または完全性について、お気軽にコメントをお寄せください。

本書の情報に対するご意見、情報の提示方法に限らせていただきます。

IBM 製品やシステムの機能に関するご意見は、IBM 担当員または IBM 指定販売員にご連絡ください

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

以下のいずれかの方法で、IBM へコメントを送付することができます。

- 郵送の場合は以下の宛先へお送りください。

User Technologies Department (MP095)
IBM United Kingdom Laboratories
Hursley Park
WINCHESTER,
Hampshire
SO21 2JN
United Kingdom

- FAX の場合は以下の番号へお送りください。
  - 英国以外の国の場合、お住まいの国の国際アクセス・コードを前に付けて、44-1962-816151 を使用してください。
  - 英国内では、01962-816151 を使用してください。
- 電子メールの場合は、以下の該当するネットワーク ID を使用してください。
  - IBM Mail Exchange: GBIBM2Q9 at IBMMAIL
  - IBMLink: HURSLEY(IDRCF)
  - インターネット: idrcf@hursley.ibm.com

どの手法を使用する場合も、以下が記載されていることを確認してください。

- 資料タイトルおよび資料番号
- コメント対象のトピック
- お客様のお名前、ご住所、電話番号、FAX 番号、ネットワーク ID