IBM SOA
Policy Gateway Pattern

目次

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。

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、「ポリシー管理ポイント (PAP) (Policy Administration 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。パターンでは、PAP は WSRR から提供され、PEP は WebSphere® DataPower® から提供され、PMP は DataPower モニタリング・コンポーネントから得られます。

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。

- **ポリシー管理ポイント**。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。 PAP にはポリシーを格納するためのリポジトリーが含まれます。PAP は WSRR から提供されます。
- **ポリシー実施ポイント**。「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す。これは以下のアクションを実行します。
  - 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、WSRR 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、PEP は WebSphere DataPower から提供されます。

- **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。 PDP は、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**。「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**。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。これは以下のアクションを実行します。
  - 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。

  このパターンでは、PMP は DataPower モニタリング・コンポーネントから提供されます。

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 のパターンのフローを示します。

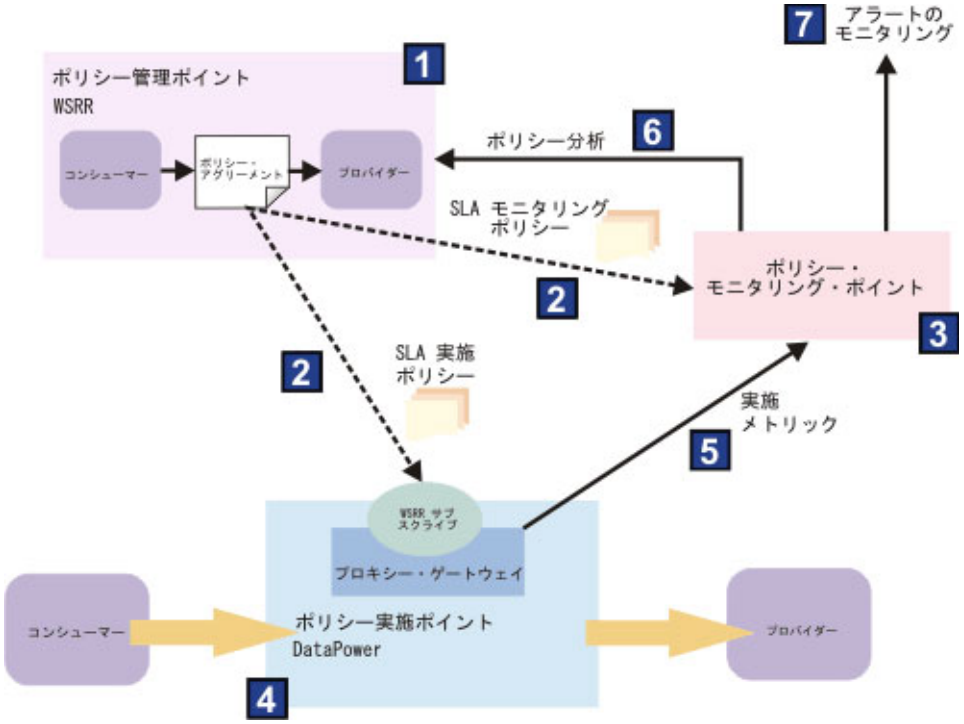


図 1. サービス・レベル・アグリーメント (SLA) ポリシー - SOA デプロイメント・モデル

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。

1. 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。このアクションは「ポリシー管理ポイント (Policy Administration Point)」の一部です。
2. 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「ポリシー管理ポイント (Policy Administration Point)」に作成されます。
   - 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 「ポリシー管理ポイント (Policy Administration 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。

1. セットアップの一環として、モニタリング・サービスは WSRR からモニタリング・ポリシーにサブスクライブします。このアクションは 1 回だけ行われます。
2. 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 DataPower アプライアンス (または仮想アプライアンス) ごとに、プロキシー・ゲートウェイが作成されます。このアクションは 1 回だけ行われ、必要に応じて追加または変更されます。
3. 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。このアクションは 1 回だけ行われ、必要に応じて追加または変更されます。

4. 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。このアクションは 1 回だけ行われ、必要に応じて追加または変更されます。
5. 「ポリシー・モニタリング・ポイント (Policy Monitoring Point)」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。
6. 「ポリシー・モニタリング・ポイント (Policy Monitoring Point)」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。
7. 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。
8. 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。
9. 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。

 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:

1. モニタリング・ポリシーは、「ポリシー・モニタリング・ポイント (Policy Monitoring Point)」シチュエーション・ポリシーでアクティブです。
2. 「ポリシー・モニタリング・ポイント (Policy Monitoring Point)」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。

 SOA Policy の実施

1. 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。
2. 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。

 「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。

 「ポリシー・モニタリング・ポイント (Policy Monitoring Point)」は「ポリシー管理ポイント (Policy Administration Point)」にモニタリング・イベントを送信します。

1. 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「ポリシー管理ポイント (Policy Administration Point)」でセットアップされます。このアクションは 1 回だけ行われ、必要に応じて追加または変更されます。
2. 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。

 アラートのモニタリング:

- 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

ポリシーは SOA Policy ライフサイクルによって制御されます。このライフサイクルとは、ポリシーが最初に識別された時点から、ポリシーが実動環境にデプロイされ、最終的に不要になって非推奨になる時点までです。

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標準を作成しました。

- **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/WSMediationPolicy1.7-20130506.pdfを参照してください。

WS-Policy データ・モデルには以下のエンティティーが含まれます。

- **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。このエンティティーは、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。こ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

図 3 は、ポリシー定義を示しています。

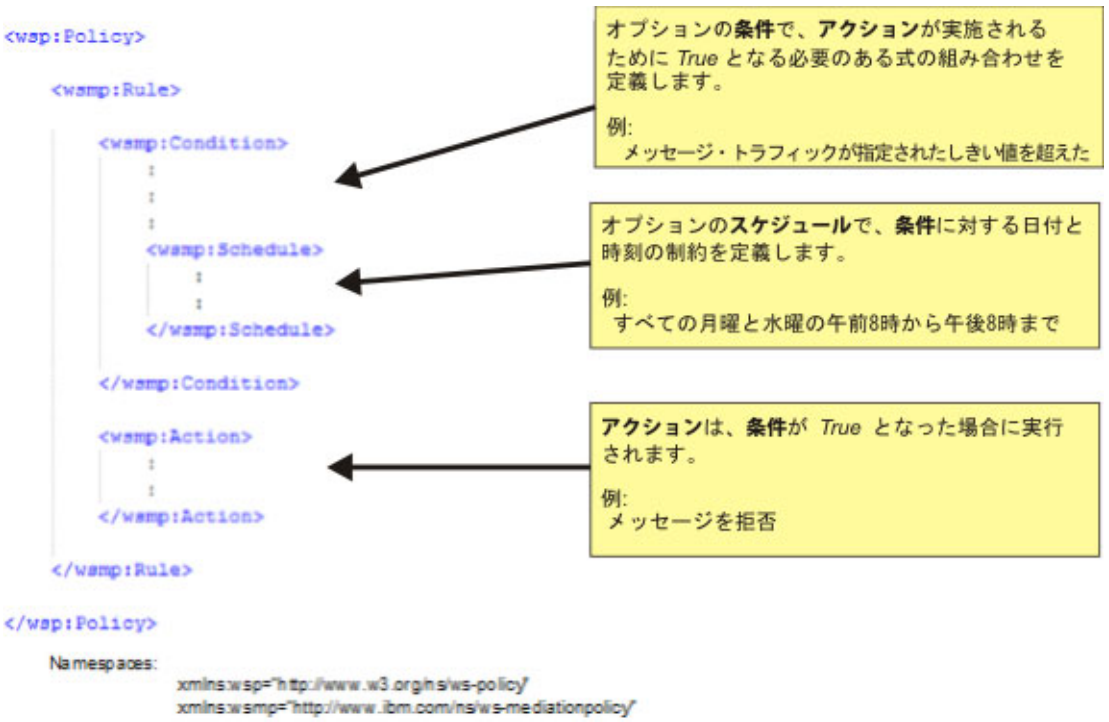


図 3. ポリシー構造の概要

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。

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) が入ります。その後に、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) が続きます。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。

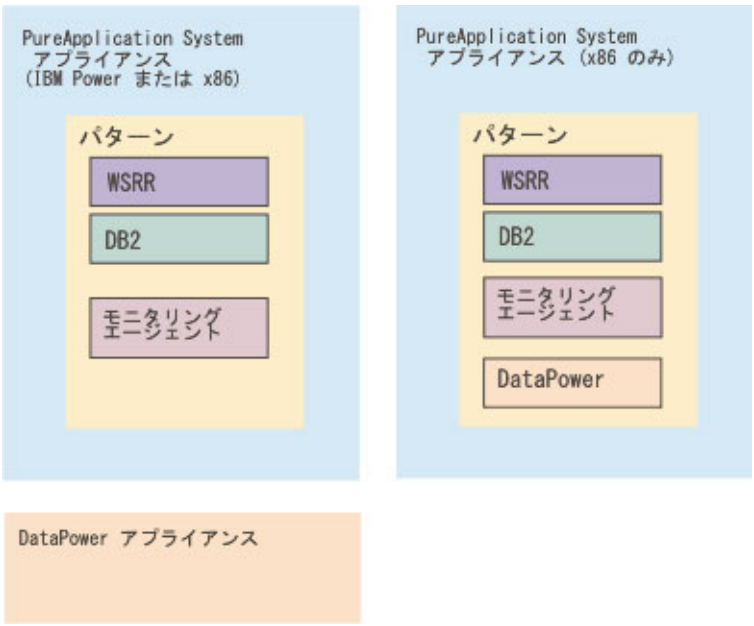
第 2 章 パターンの概要

IBM SOA Policy Gateway Pattern は、ポリシー適用ポイント、ポリシー管理ポイント、およびポリシー・モニター・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。

IBM Power® または x86 アーキテクチャー上の IBM PureApplication™ System アプライアンスに IBM SOA Policy Gateway Pattern をインストールできます。

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。ポリシー実施ポイントは、WebSphere DataPower アプライアンスによって提供できます。それに対して、x86 では、PureApplication System は仮想 DataPower イメージをデプロイできます。どちらも場合でも、ドメインは仮想システム・パターンのデプロイメント中に作成されます。ポリシー・モニター・ポイントは、PureApplication System モニター・サービスに対するアドオンをモニターすることによって提供されます。

次の図に、IBM SOA Policy Gateway Pattern から得られる機能を示します。



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。これらの合意を実施するために、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。パターンを使用して、SLD と SLA のポリシーの定義を、効率的に管理、定義、および統制された方法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、以下のポリシーが含まれます。

- **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**: サンプルは、XACML アクセス制御セキュリティー・ポリシーの実施を示します。現時点で、これらのポリシーはポリシー管理ポイント内で統制されません。
- **モニター・ポリシー**: PureApplication System デプロイメントにモニター・ポリシーを定義できます。

IBM SOA Policy Gateway Pattern 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 (x86 のみ)
- SOA Policy Gateway Governance Master
- SOA Policy Gateway Basic Runtime
- SOA Policy Gateway Basic Runtime External DataPower
- SOA Policy Gateway Advanced Runtime
- SOA Policy Gateway Advanced Runtime External DataPower
- SOA Policy Gateway Pattern 2.5 のシステム・モニター (共用サービス)

これらの仮想システム・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。

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。

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。

24 ページの『SOA Policy Gateway Basic Runtime External DataPower』
SOA Policy Gateway Basic Runtime External DataPower パターンは Basic Runtime パターンと同じですが、デプロイメントで外部 DataPower アプライアンスを指定することが必要です。

19 ページの『SOA Policy Gateway Basic Runtime Sample (x86)』
SOA Policy Gateway Basic Runtime Sample は、Basic Runtime パターンに、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の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。

21 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。

28 ページの『SOA Policy Gateway Advanced Runtime External DataPower』
SOA Policy Gateway Advanced Runtime External DataPower は Advanced Runtime パターンと同じですが、デプロイメントで外部 DataPower アプライアンスを指定することが必要です。

30 ページの『SOA Policy Gateway のシステム・モニター』
SOA Policy Gateway 共用サービスのシステム・モニターは、SOA Policy Gateway にモニタリング・コンポーネントを提供します。

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。パターンをダウンロードしてインストールする方法、インストール後にパターンを検証し、ライセンスを承諾する方法、および関係するユーザーの役割を理解するには、このセクションのトピックを検討してください。

パターンのダウンロードおよびインストール

IBM PureApplication System で使用する IBM SOA Policy Gateway Pattern は、Passport Advantage®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

IBM SOA Policy Gateway Pattern を一時システム (Linux または Microsoft Windows システム) にダウンロードします。その後、一時システムでインストーラーを実行して、IBM PureApplication System にパターンをインストールします。

`CIQ1LML.tar.gz` ファイル (Power 用) または `CIQ1VML.tar.gz` ファイル (x86 用) のために 16 GB の空きスペースがあり、解凍するファイル用にさらに 40 GB があることを確認してください。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。JRE 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、`CIQ1LML.tar.gz` ファイル (Power システム用)、または `CIQ1VML.tar.gz` ファイル (x86 システム用) 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。ファイルの名前は `CIQ1LML.tar.gz` (Power 用) または `CIQ1VML.tar.gz` (x86 用) 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、アーカイブ・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. アーカイブ・ファイルの内容をローカル・ファイル・システムに解凍します。Linux では、以下に示す解凍コマンドが使用されます。

```
tar xvzf archive_file
```

Windows では、追加でアーカイブ解凍ソフトウェアを使用して、アーカイブ・ファイルの内容を解凍します。

5. 次のように installer ディレクトリーに移動します。

```
cd installer
```

6. IBM SOA Policy Gateway Pattern をIBM PureApplication System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IBM PureApplication System、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 drivensnow.hillesden.ibm.com -u cbadmin -p cbadmin
```

7. 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。
8. 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 2.5.0.0 - Governance Master" ...
Import pattern "SOA Policy Gateway 2.5.0.0 - 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 PureApplication System で、使用を許諾します。を参照してください。

インストールを検証するには、『インストール済みのパターンの検証』を参照してください。

インストール済みのパターンの検証

パターンが正常にインストールされたことを検証できます。

始める前に

13 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に、パターンのインストール済み環境を検証して、すべての部品が正常にインストールされていることを確認できます。

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たアプライアンスで、ワークロード・コンソールを開きます。
2. 「**カタログ (Catalog)**」 > 「**仮想イメージ (Virtual Images)**」とナビゲートして仮想イメージを確認し、以下の項目を探します。
   - DB2® Enterprise 10.1.0.2
   - WebSphere Service Registry and Repository 8.0.0.2
   - WebSphere DataPower X152 Virtual Edition (x86 システムのみ)
3. 「**カタログ (Catalog)**」 > 「**スクリプト・パッケージ (Script Packages)**」とナビゲートし、以下を探します。
   - SOA Policy Gateway 2.5.0.0 - DataPower Domain
   - SOA Policy Gateway 2.5.0.0 - DataPower Monitoring (x86 のみ)
   - SOA Policy Gateway 2.5.0.0 - External DataPower Monitoring
   - SOA Policy Gateway 2.5.0.0 - Promotion
   - SOA Policy Gateway 2.5.0.0 - Sample (x86 only)
   - SOA Policy Gateway 2.5.0.0 - Security
   - SOA Policy Gateway 2.5.0.0 - Add_Named_Queries
   - SOA Policy Gateway 2.5.0.0 - Tear Down

   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. 「**パターン (Patterns)**」 > 「**仮想システム (Virtual Systems)**」とナビゲートします。x86 システムで、以下を探します。
   - SOA Policy Gateway 2.5.0.0 - Advanced Runtime
   - SOA Policy Gateway 2.5.0.0 - Advanced Runtime External DataPower
   - SOA Policy Gateway 2.5.0.0 - Basic Runtime
   - SOA Policy Gateway 2.5.0.0 - Basic Runtime External DataPower
   - SOA Policy Gateway 2.5.0.0 - Basic Runtime Sample
   - SOA Policy Gateway 2.5.0.0 - Governance Master

   Power システムで、以下を探します。
   - SOA Policy Gateway 2.5.0.0 - Advanced Runtime
   - SOA Policy Gateway 2.5.0.0 - Basic Runtime
   - SOA Policy Gateway 2.5.0.0 - 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。

5. 「**クラウド (Cloud)**」 > 「**パターン・タイプ (Pattern Types)**」とナビゲートして、以下の項目を探します。
   - SOA Policy Gateway Pattern 2.5.0.0 のシステム・モニター

   このパターンは、正常に完了したインストール済み環境に存在します。

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

インストールが正常に完了した場合、使用許諾に進むことができます。『ご使用条件の同意』を参照してください。正常にインストールされていない場合は、 13 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。

ご使用条件の同意

パターンで作業を開始する前に、新しくインストールした部品のご使用条件に同意する必要があります。

始める前に

13 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

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

ご使用条件に同意するには、以下の手順を実行します。

1. パターンがインストールされたアプライアンスで、ワークロード・コンソールを開きます。
2. 「**カタログ (Catalog)**」 > 「**仮想イメージ (Virtual Images)**」を選択します。
3. 「**仮想イメージ (Virtual Images)**」リストで以下のイメージを探して、詳細ペインでご使用条件が同意されていることを確認します。同意されていない場合、「同意する (accept)」をクリックして、ご使用条件を表示して、同意します。
   x86 システムの場合:
   - WebSphere DataPower XI52 Virtual Edition バージョン 6.0.0.0 - イメージ参照番号: XI52.6.0.0.0231528 (2013/06/16 14:14:19)
   - WebSphere Service Registry and Repository 8.0.0.2 - イメージ参照番号: 201309062038
   - DB2 Enterprise 10.1.0.2 - イメージ参照番号: 39
   - IBM OS Image for Red Hat Linux Systems バージョン 2.0.0.3 - イメージ参照番号: 136

Power システムの場合:

- WebSphere Service Registry and Repository 8.0.0.2 - イメージ参照番号: 201309080001
- DB2 Enterprise 10.1.0.2 - イメージ参照番号: 50
- IBM OS Image for AIX® Systems バージョン 2.0.0.2 - イメージ参照番号: 126

4. 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。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。状況に「**読み取り専用 (Read-only)**」と表示され、完了すると、ご使用条件に「**同意 (Accepted)**」と表示されます。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。

タスクの結果

IBM SOA Policy Gateway Patternのご使用条件に同意しました。

次のタスク

インストールが正常に完了し、すべてのご使用条件に同意した場合、パターンでの作業に進むことができます。 47 ページの『第 5 章 IBM SOA Policy Gateway Pattern による作業』を参照してください。正常にインストールされていない場合は、 13 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。これをシステム・コンソールを使用して行います。

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。
   - コンソールの「ユーザー (Users)」ウィンドウで、ユーザーを追加および構成します。
     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。ワークロード・コンソールに切り替え、「**パターン (Patterns)**」 > 「**仮想システム (Virtual systems)**」をクリックして、仮想システム・パターン・ウィンドウを開きます。IBM SOA Policy Gateway Pattern 仮想イメージを選択して、その詳細情報を表示します。ユーザーまたはグループを、「**アクセス権限を付与する対象 (Access granted to)**」フィールドに追加します。

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

第 4 章 パターン、パーツ、およびスクリプト・パッケージ

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。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。

パターン

仮想イメージが IBM PureApplication System にロードされ、アクセス権限がユーザーに割り当てられると、ユーザーは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 Sample (x86)

SOA Policy Gateway Basic Runtime Sample は、Basic Runtime パターンに、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の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 パターンは x86 システムのみで使用可能です。

SOA Policy Gateway Basic Runtime Sample パターンには以下のパーツがあります。

- WSRR スタンドアロン・サーバー
- DB2 Enterprise
- DataPower

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。このパターンは、サンプル・サービスを実装し、サンプル WSDL および添付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、61 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。

以下の図に、Basic Runtime サンプルを示します。

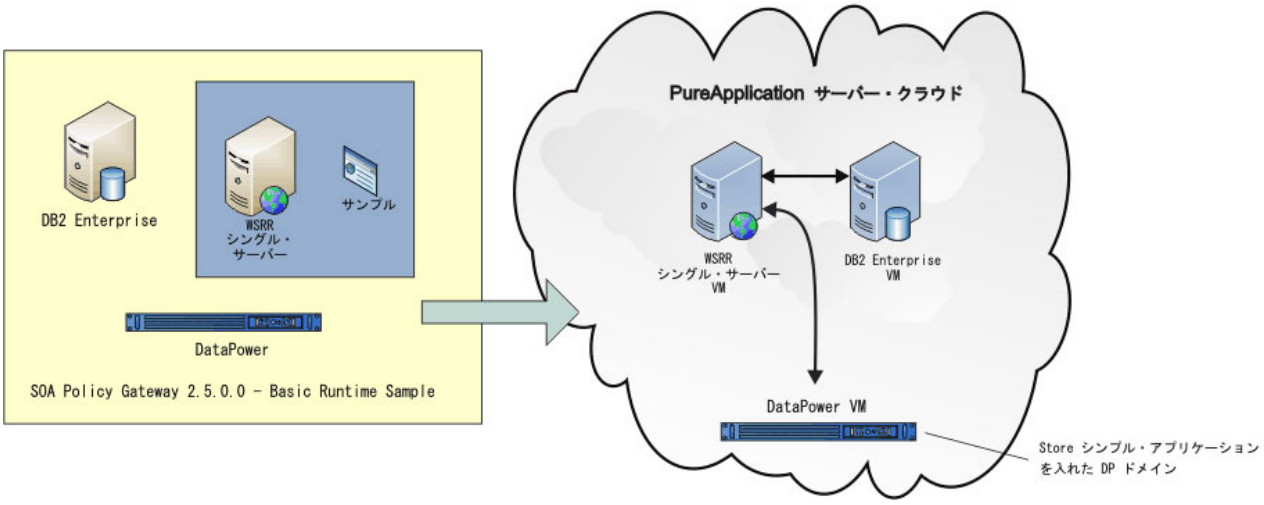


図 5. DataPower VM を使用した PureApplication Server 構成 (x86 のみ)

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

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 2.5.0.0 - 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。

- 31 ページの『DB2 Enterprise パーツ』
- 36 ページの『WSRR スタンドアロン・サーバー・パーツ』
- 39 ページの『DataPower 部品』

- 42 ページの『スクリプト: SOA Policy Gateway 2.5.0.0 - Sample』

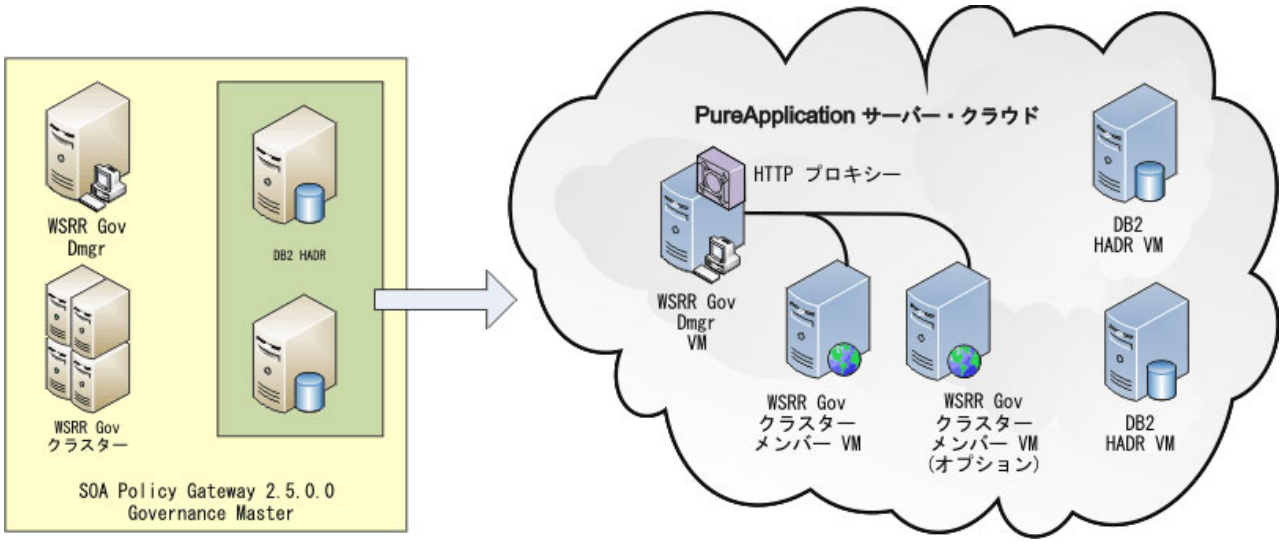
SOA Policy Gateway Governance Master

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。



パーツのパラメーター

パーツのパラメーターを参照してください。

- 33 ページの『DB2 Enterprise HADR Primary パーツ』
- 35 ページの『DB2 Enterprise HADR Standby パーツ』
- 37 ページの『WSRR デプロイメント・マネージャー・パーツ』
- 38 ページの『WSRR カスタム・ノード・パーツ』
- 44 ページの『スクリプト: SOA Policy Gateway 2.5.0.0 - Security』
- 41 ページの『スクリプト: SOA Policy Gateway 2.5.0.0 - Promotion』

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。Basic Runtime パターンまたは 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。プロモーション・ターゲットの構成方法の詳細については、58 ページの『付加的なランタイム環境の追加』を参照してください。

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 - ガバナンス有効化プロファイル

SOA Policy Gateway Basic Runtime

SOA Policy Gateway Basic Runtime パターンは、SOA Policy Gateway ランタイムを提供するための最も単純な手段であり、2 つの DataPower インスタンス (x86 のみ)、スタンドアロン WSRR インスタンス、スタンドアロン DB2 インスタンス、および Base OS インスタンス (DataPower モニタリング・エージェントのホスティング用) が含まれています。

注: このトピックでは、x86 で使用できるパターンを説明します。IBM Power パターンについては、24 ページの『SOA Policy Gateway Basic Runtime External DataPower』を参照してください。

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
- WebSphere DataPower X152 Virtual Edition
- SOA monitoring for DataPower (Core OS パーツ内)

以下の図に、SOA Policy Gateway Basic Runtime パターンの構成を示します。

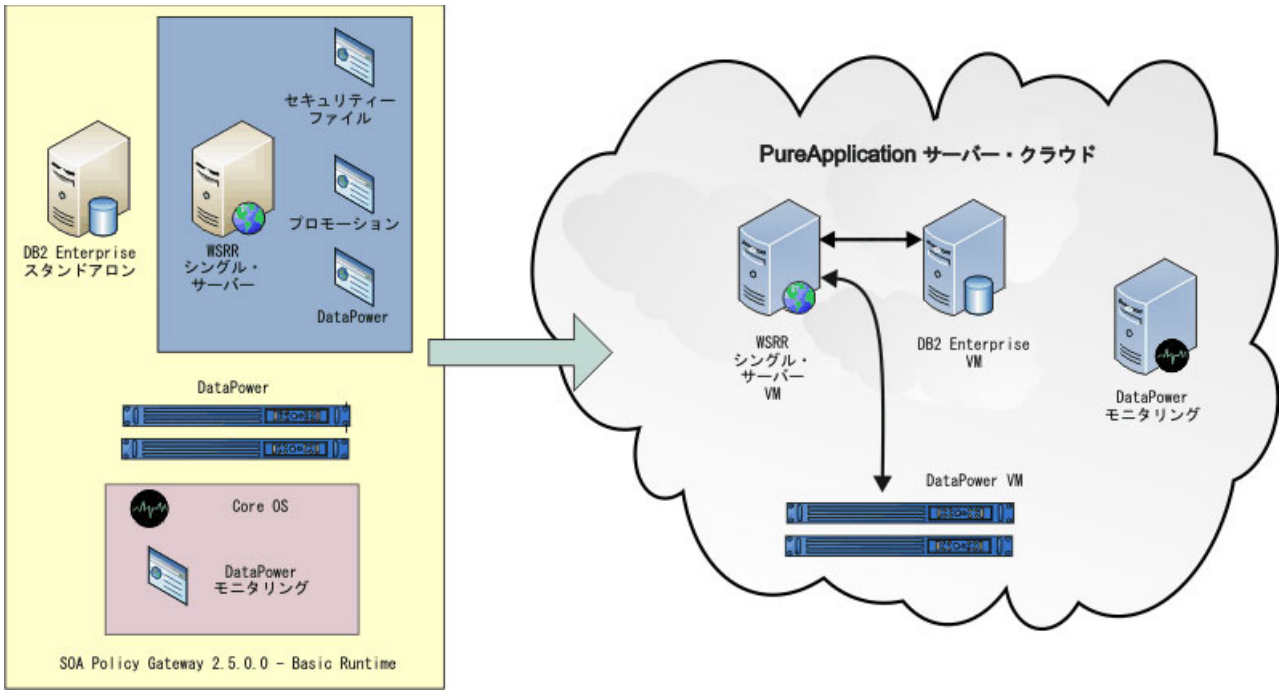


図 6. DataPower VM を使用した PureApplication Server 構成

スクリプトおよび拡張オプション

このパターンでは、デプロイ時に以下のスクリプトへのユーザー入力が必要です。

WSRR スタンドアロン・サーバー・パーツで:

- SOA Policy Gateway 2.5.0.0 - Security
- SOA Policy Gateway 2.5.0.0 - Promotion
- SOA Policy Gateway 2.5.0.0 - DataPower Domain

Core OS パーツで:

- SOA Policy Gateway 2.5.0.0 - DataPower Monitoring

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。

- 36 ページの『WSRR スタンドアロン・サーバー・パーツ』
- 31 ページの『DB2 Enterprise パーツ』
- 39 ページの『DataPower 部品』
- 44 ページの『スクリプト: SOA Policy Gateway 2.5.0.0 - Security』
- 41 ページの『スクリプト: SOA Policy Gateway 2.5.0.0 - Promotion』
- 40 ページの『スクリプト: SOA Policy Gateway 2.5.0.0 - DataPower Domain』
- 44 ページの『スクリプト: SOA Policy Gateway 2.5.0.0 - DataPower Monitoring (x86 のみ)』

Governance Master を使用した Basic Runtime の構成

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

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。 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。

注: このパターンは、Governance Master がないスタンドアロン・システムのプロビジョンに使用できます。これを行うには、パターンのデプロイ時に Governance Master パラメーターを「Unset」として指定します。このように設定すると、デプロイメント中にプロモーション・スクリプトでエラーが生成され、デプロイメントは「**失敗 (failed)**」として表示されますが、このエラーは無視できます。

SOA Policy Gateway Basic Runtime External DataPower

SOA Policy Gateway Basic Runtime External DataPower パターンは Basic Runtime パターンと同じですが、デプロイメントで外部 DataPower アプライアンスを指定することが必要です。

注: この説明は、IBM Power システムのパターンに適用されます。

SOA Policy Gateway Basic Runtime External DataPower パターンには以下のパーツがあります。

- WSRR スタンドアロン・サーバー
- DB2 Enterprise
- SOA monitoring for DataPower (Core OS パーツ内)

以下の図に、SOA Policy Gateway Basic Runtime External DataPower パターンの構成を示します。

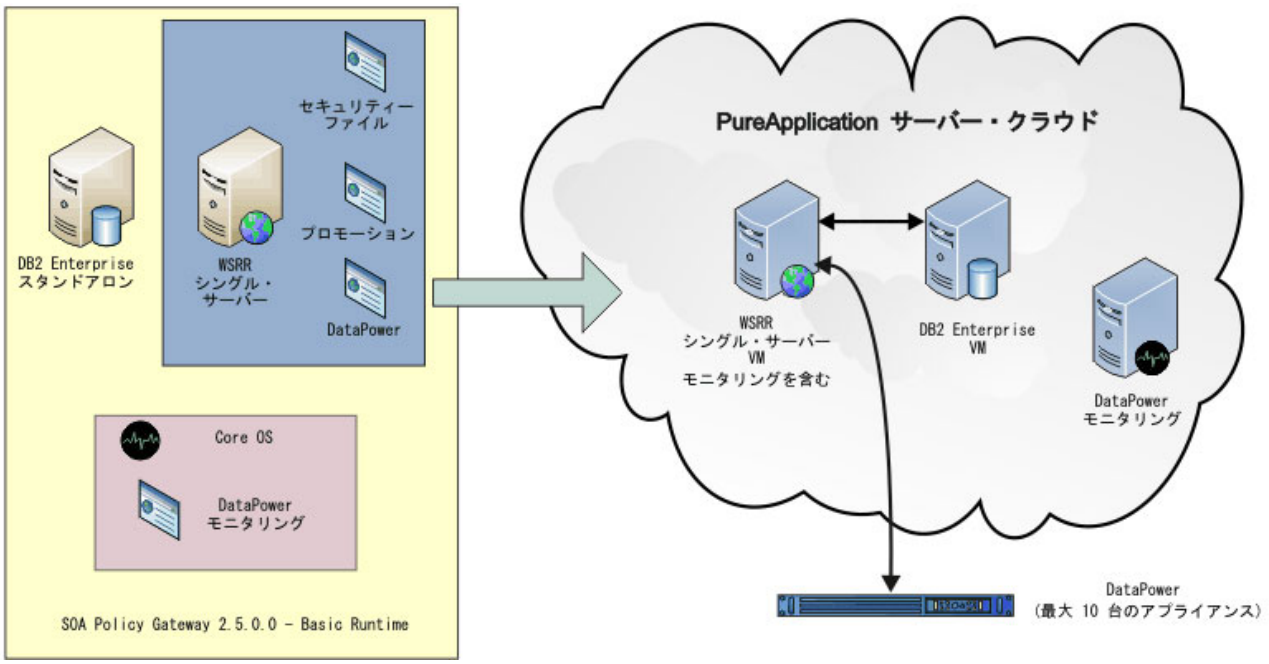


図 7. DataPower アプライアンスを使用した PureApplication Server 構成

スクリプトおよび拡張オプション

このパターンでは、デプロイ時に以下のスクリプトへのユーザー入力が必要です。

WSRR スタンドアロン・サーバー・パーツで:

- SOA Policy Gateway 2.5.0.0 - Security
- SOA Policy Gateway 2.5.0.0 - Promotion
- SOA Policy Gateway 2.5.0.0 - DataPower Domain

Core OS パーツで:

- SOA Policy Gateway 2.5.0.0 - DataPower Monitoring

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。

- 36 ページの『WSRR スタンドアロン・サーバー・パーツ』
- 31 ページの『DB2 Enterprise パーツ』
- 44 ページの『スクリプト: SOA Policy Gateway 2.5.0.0 - Security』
- 41 ページの『スクリプト: SOA Policy Gateway 2.5.0.0 - Promotion』
- 40 ページの『スクリプト: SOA Policy Gateway 2.5.0.0 - DataPower Domain』
- 44 ページの『スクリプト: SOA Policy Gateway 2.5.0.0 - DataPower Monitoring (x86 のみ)』

Governance Master を使用した Basic Runtime の構成

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

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。

注: このパターンは、Governance Master がないスタンドアロン・システムのプロビジョンに使用できます。これを行うには、パターンのデプロイ時に Governance Master パラメーターを「Unset」として指定します。このように設定すると、デプロイメント中にプロモーション・スクリプトでエラーが生成され、デプロイメントは「**失敗 (failed)**」として表示されますが、このエラーは無視できます。

SOA Policy Gateway Advanced Runtime

SOA Policy Gateway Advanced Runtime には、HADR 構成内の 2 つの DB2 サーバー・インスタンス、および単一のデプロイメント・マネージャーと 2 つのカスタム・ノードを含む WSRR クラスターが含まれています。

注: このトピックでは、x86 で使用できるパターンを説明します。IBM Power パターンについては、 28 ページの『SOA Policy Gateway Advanced Runtime External DataPower』を参照してください。

パターンには、以下のパーツが必要です。

- WSRR デプロイメント・マネージャー
- WSRR カスタム・ノード
- DB2 HADR Primary
- DB2 HADR Standby
- WebSphere DataPower X152 Virtual Edition
- SOA monitoring for DataPower (Core OS パーツ内)

以下の図に、Advanced Runtime システムの構成を示します。

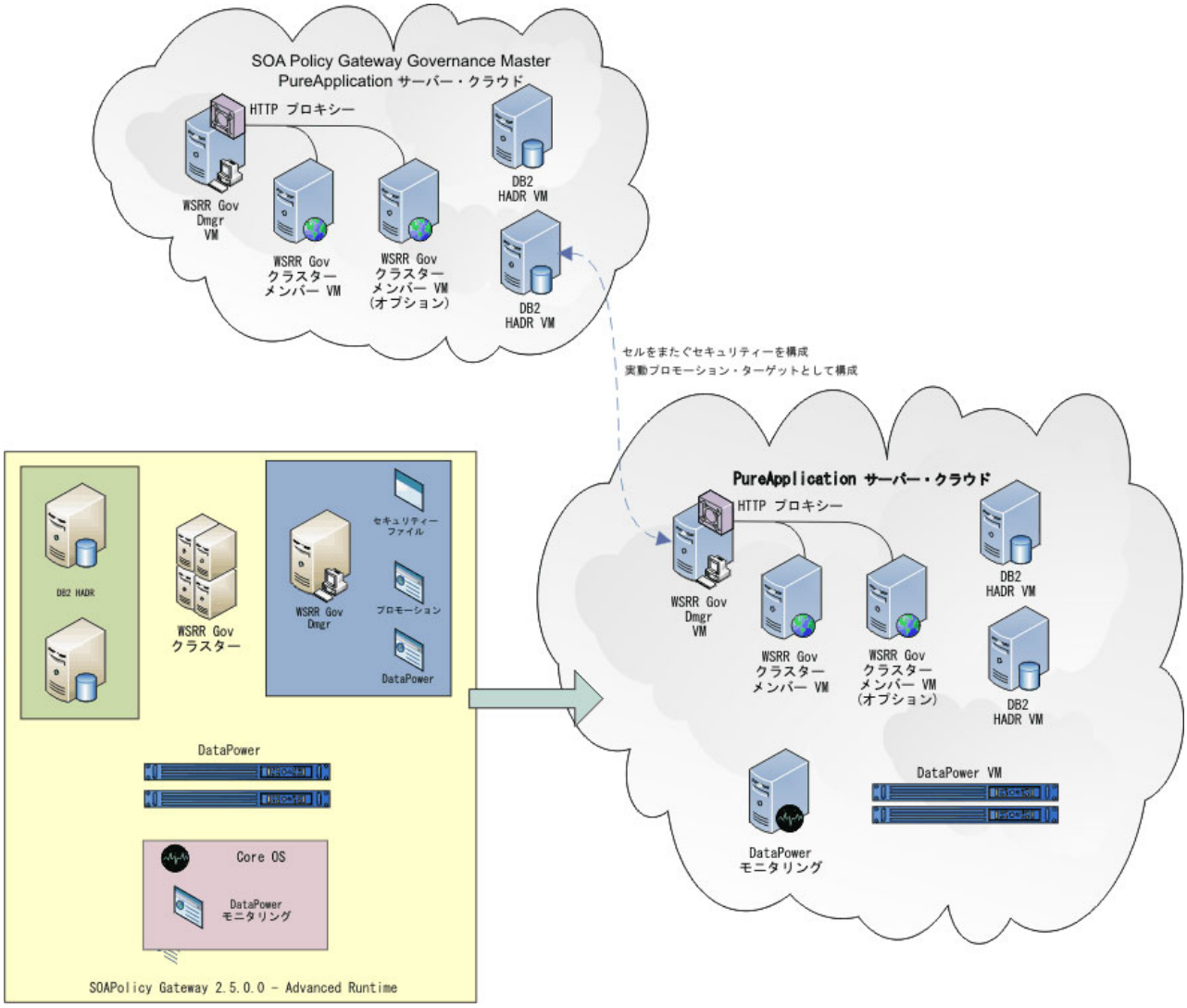


図 8. DataPower VM を使用した PureApplication Server 構成

スクリプトおよび拡張オプション

このパターンでは、デプロイ時に以下のスクリプトへのユーザー入力が必要です。

WSRR デプロイメント・マネージャー・パーツで:

- SOA Policy Gateway 2.5.0.0 - Security
- SOA Policy Gateway 2.5.0.0 - Promotion
- SOA Policy Gateway 2.5.0.0 - DataPower Domain

Core OS パーツで:

- SOA Policy Gateway 2.5.0.0 - DataPower Monitoring

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。

- 33 ページの『DB2 Enterprise HADR Primary パーツ』
- 35 ページの『DB2 Enterprise HADR Standby パーツ』
- 37 ページの『WSRR デプロイメント・マネージャー・パーツ』

- 38 ページの『WSRR カスタム・ノード・パーツ』
- 41 ページの『スクリプト: SOA Policy Gateway 2.5.0.0 - Promotion』
- 40 ページの『スクリプト: SOA Policy Gateway 2.5.0.0 - DataPower Domain』
- 44 ページの『スクリプト: SOA Policy Gateway 2.5.0.0 - DataPower Monitoring (x86 のみ)』

Governance Master を使用した Advanced Runtime の構成

Advanced Runtime パターンが Governance Master パターンと共に構成されると、以下のアクションが実行されます。

- 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

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。 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 Advanced Runtime External DataPower

SOA Policy Gateway Advanced Runtime External DataPower は Advanced Runtime パターンと同じですが、デプロイメントで外部 DataPower アプライアンスを指定することが必要です。

注: この説明は、IBM Power システムの SOA Policy Gateway Advanced Runtime パターンに適用されます。

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

- WSRR デプロイメント・マネージャー
- WSRR カスタム・ノード
- DB2 HADR Primary
- DB2 HADR Standby
- SOA monitoring for DataPower (Core OS パーツ内)

以下の図に、Advanced Runtime システムの構成を示します。

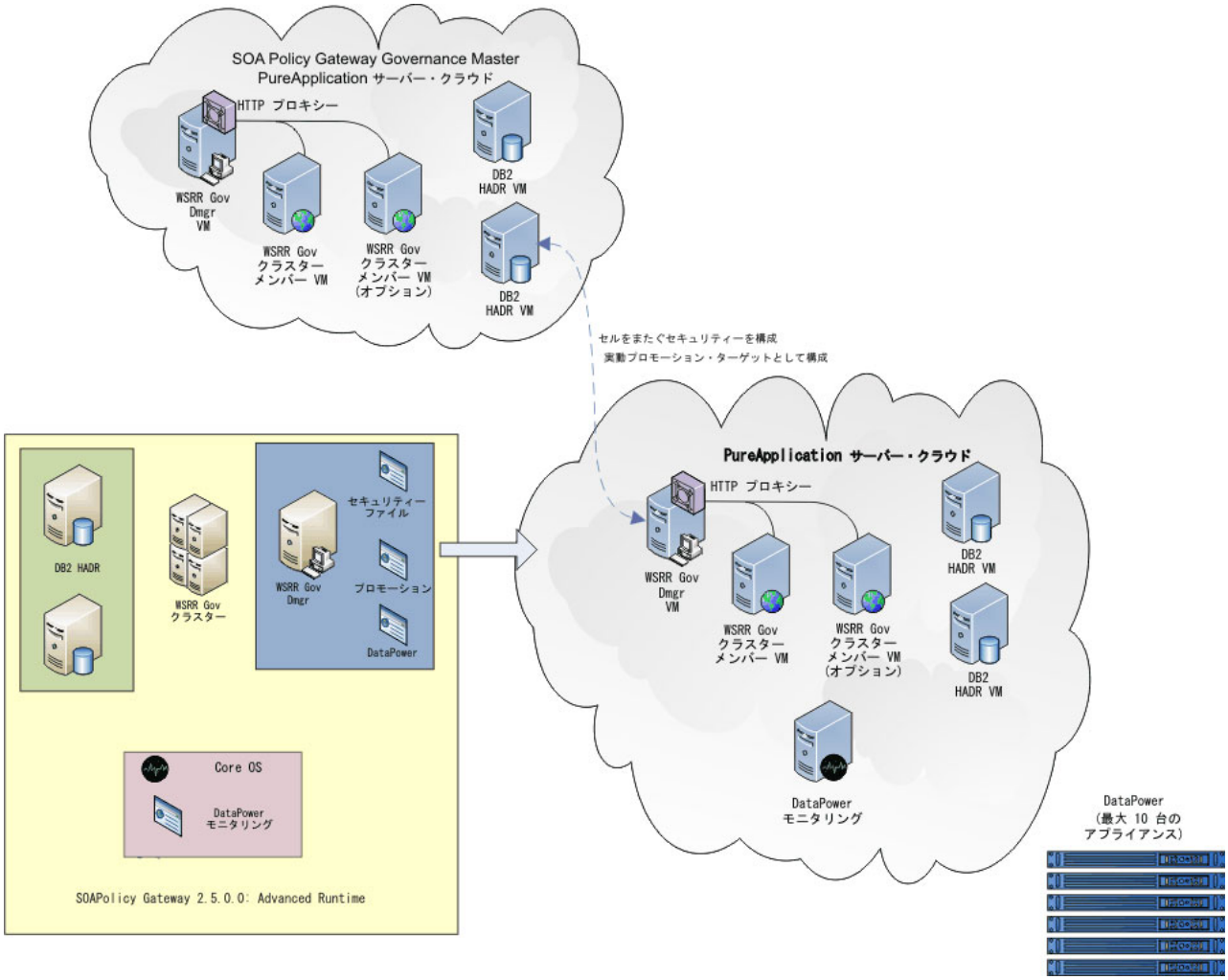


図 9. DataPower アプライアンスを使用した PureApplication Server 構成

スクリプトおよび拡張オプション

このパターンでは、デプロイ時に以下のスクリプトへのユーザー入力が必要です。

WSRR デプロイメント・マネージャー・パーツで:

- SOA Policy Gateway 2.5.0.0 - Security
- SOA Policy Gateway 2.5.0.0 - Promotion
- SOA Policy Gateway 2.5.0.0 - DataPower Domain

Core OS パーツで:

- SOA Policy Gateway 2.5.0.0 - DataPower Monitoring

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。

- 33 ページの『DB2 Enterprise HADR Primary パーツ』
- 35 ページの『DB2 Enterprise HADR Standby パーツ』
- 37 ページの『WSRR デプロイメント・マネージャー・パーツ』
- 38 ページの『WSRR カスタム・ノード・パーツ』

- 41 ページの『スクリプト: SOA Policy Gateway 2.5.0.0 - Promotion』
- 40 ページの『スクリプト: SOA Policy Gateway 2.5.0.0 - DataPower Domain』
- 44 ページの『スクリプト: SOA Policy Gateway 2.5.0.0 - DataPower Monitoring (x86 のみ)』

Governance Master を使用した Advanced Runtime の構成

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

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。 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。

共用サービス

パターンには、デプロイされたパターンがモニタリングを提供するために使用する共用サービスが組み込まれています。

SOA Policy Gateway のシステム・モニター

SOA Policy Gateway 共用サービスのシステム・モニターは、SOA Policy Gateway にモニタリング・コンポーネントを提供します。

Basic Runtime パターンおよび Advanced Runtime パターンのモニターは、Core OS パーツで実行している DataPower モニタリング・サービスによって提供されます。モニタリング・サービス自体は、SOA Policy Gateway パターンのシステム・モニターに含まれる ITCAM for SOA コンポーネントを使用します。WSRR インスタンスのモニターでは、WebSphere Application Server 共用サービスのシステム・モニターが実行されていることも必要です。

ITCAM for SOA の詳細な資料については、関連リンクを参照してください。

関連情報:

ITCAM for SOA 7.2.1 資料 (Fix Central 提供)

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 10.1.0.2 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	デフォルト値	説明
仮想 CPU 数	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)	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)。
インスタンス所有者グループ (Instance owner group)	db2iadm1	DB2 インスタンス所有者が属するグループ。
インスタンス所有者	db2inst1	DB2 インスタンス所有者の ID。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 (インスタンス所有者)(Password (Instance owner))	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。
パスワードの確認	パスワード	インスタンス所有者のパスワードを確認します。
fenced ユーザー・グループ (Fenced user group)	db2fadm1	DB2 fenced 所有者が属するグループ。
fenced ユーザー (Fenced user)	db2fenc1	DB2 fenced ユーザーの ID。fenced ユーザー ID は、DB2 データベースで使用されるアドレス・スペース外でユーザー定義関数 (UDF) やストアード・プロシージャーを実行するために使用されます。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「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。
パスワード (db2fenc1)		fenced ユーザー ID のパスワード。
パスワードの確認		fenced ユーザーのパスワードを確認します。
DAS ユーザー・グループ (DAS user group)	dasadm1	DB2 DAS 所有者が属するグループ。

表 2. 構成可能なパラメーター (続き)

パラメーター名	デフォルト値	説明
DAS ユーザー	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。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 (DAS ユーザー)(Password (DAS user))	パスワード	DAS ユーザーのパスワード。
パスワードの確認	パスワード	dasusr1 パスワードを確認します。
DB2 サービス・ポート	50000	ポートはロックされていて、変更できません。
データベースの作成 (Database creation)	Create-new-database	この値はロックされていて、変更できません。
新規データベースの名前 (Name for the new database)	WSRR	この値はロックされていて、変更できません。
新規データベースのコード・セット (Codeset for the new database)	UTF-8	
新規データベースのテリトリー (Territory for the new database)	US	
新規データベースの照合順序 (Collation for the new database)	SYSTEM	
新規データベースのページ・サイズ (Pagesize for the new database)	32768	この値はロックされていて、変更できません。
DB2 互換モード (DB2 compatibility mode)	Default	この値はロックされていて、変更できません。
すべてのロー・ディスクを DB2 が使用するように構成 (Configure all raw disks for use by DB2)	NO	
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。
VNC を使用可能に設定 (Enable VNC)	True	この値はロックされていて、変更できません。

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 3. 構成可能なパラメーター

パラメーター名	デフォルト値	説明
仮想 CPU 数	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)	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)。
インスタンス所有者グループ (Instance owner group)	db2iadm1	DB2 インスタンス所有者が属するグループ。
インスタンス所有者	db2inst1	DB2 インスタンス所有者の ID。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 (インスタンス所有者)(Password (Instance owner))	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。
パスワードの確認	パスワード	インスタンス所有者のパスワードを確認します。
fenced ユーザー・グループ (Fenced user group)	db2fadm1	DB2 fenced 所有者が属するグループ。
fenced ユーザー (Fenced user)	db2fenc1	DB2 fenced ユーザーの ID。fenced ユーザー ID は、DB2 データベースで使用されるアドレス・スペース外でユーザー定義関数 (UDF) やストアード・プロシージャーを実行するために使用されます。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「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。
パスワード (db2fenc1)		fenced ユーザー ID のパスワード。
パスワードの確認		fenced ユーザーのパスワードを確認します。
DAS ユーザー・グループ (DAS user group)	dasadm1	DB2 DAS 所有者が属するグループ。

表 3. 構成可能なパラメーター (続き)

パラメーター名	デフォルト値	説明
DAS ユーザー	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。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 (DAS ユーザー)(Password (DAS user))	パスワード	DAS ユーザーのパスワード。
パスワードの確認	パスワード	dasusr1 パスワードを確認します。
DB2 サービス・ポート	50000	ポートはロックされていて、変更できません。
データベースの作成 (Database creation)	Create-new-database	この値はロックされていて、変更できません。
新規データベースの名前 (Name for the new database)	WSRR	この値はロックされていて、変更できません。
新規データベースのコード・セット (Codeset for the new database)	UTF-8	
新規データベースのテリトリー (Territory for the new database)	US	
新規データベースの照合順序 (Collation for the new database)	SYSTEM	
新規データベースのページ・サイズ (Pagesize for the new database)	32768	この値はロックされていて、変更できません。
DB2 互換モード (DB2 compatibility mode)	Default	この値はロックされていて、変更できません。
すべてのロー・ディスクを DB2 が使用するように構成 (Configure all raw disks for use by DB2)	NO	
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。
VNC を使用可能に設定 (Enable VNC)	True	この値はロックされていて、変更できません。

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。

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 4. 構成可能なパラメーター

パラメーター名	デフォルト値	説明
仮想 CPU 数	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)	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)。
インスタンス所有者グループ (Instance owner group)	db2iadm1	DB2 インスタンス所有者が属するグループ。
インスタンス所有者	db2inst1	DB2 インスタンス所有者の ID。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 (インスタンス所有者)(Password (Instance owner))	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。
パスワードの確認	パスワード	インスタンス所有者のパスワードを確認します。
fenced ユーザー・グループ (Fenced user group)	db2fadm1	DB2 fenced 所有者が属するグループ。
fenced ユーザー (Fenced user)	db2fenc1	DB2 fenced ユーザーの ID。fenced ユーザー ID は、DB2 データベースで使用されるアドレス・スペース外でユーザー定義関数 (UDF) やストアード・プロシージャーを実行するために使用されます。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「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。
パスワード (db2fenc1)		fenced ユーザー ID のパスワード。
パスワードの確認		fenced ユーザーのパスワードを確認します。
DAS ユーザー・グループ (DAS user group)	dasadm1	DB2 DAS 所有者が属するグループ。
DAS ユーザー	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。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。

表 4. 構成可能なパラメーター (続き)

パラメーター名	デフォルト値	説明
パスワード (DAS ユーザー)(Password (DAS user))	パスワード	DAS ユーザーのパスワード。
パスワードの確認	パスワード	dasusr1 パスワードを確認します。
DB2 サービス・ポート	50000	ポートはロックされていて、変更できません。
データベースの作成 (Database creation)	Create-new-database	この値はロックされていて、変更できません。
新規データベースの名前 (Name for the new database)	WSRR	この値はロックされていて、変更できません。
新規データベースのコード・セット (Codeset for the new database)	UTF-8	
新規データベースのテリトリー (Territory for the new database)	US	
新規データベースの照合順序 (Collation for the new database)	SYSTEM	
新規データベースのページ・サイズ (Pagesize for the new database)	32768	この値はロックされていて、変更できません。
DB2 互換モード (DB2 compatibility mode)	Default	この値はロックされていて、変更できません。
すべてのロー・ディスクを DB2 が使用するように構成 (Configure all raw disks for use by DB2)	NO	
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。
VNC を使用可能に設定 (Enable VNC)	True	この値はロックされていて、変更できません。

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。

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 5. 構成済みパラメーター

パラメーター名	デフォルト値	説明
仮想 CPU 数	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)	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)。
セル名	以下のいずれかの値に設定します。 • SOAPolicySampleCell (Basic Runtime Sample パターン) • SOAPolicyBasicCell (Basic Runtime パターン) • SOAPolicyBasicCell (Basic Runtime External DataPower パターン)	
ノード名	以下のいずれかの値に設定します。 • SOAPolicySampleNode (Basic Runtime Sample パターン) • SOAPolicyBasicNode (Basic Runtime パターン) • SOAPolicyBasicNode (Basic Runtime External DataPower パターン)	
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	virtuser	WebSphere Application Server の管理ユーザー名。この値を変更してはなりません。
WebSphere 管理パスワード		WebSphere Application Server の管理ユーザー・パスワード。
パスワードの確認		WebSphere Application Server 管理者パスワードのユーザー入力を確認します。
VNC を使用可能に設定 (Enable VNC)	True	この値はロックされていて、変更できません。

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 6. 構成可能なパラメーター

パラメーター名	デフォルト値	説明
仮想 CPU 数	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)	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)。
セル名	SOAPolicyAdvancedCell	Advanced Runtime パターン用のセル名。
ノード名	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、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	virtuser	WebSphere Application Server の管理者ユーザー名。この値を変更してはなりません。
WebSphere 管理パスワード		WebSphere Application Server の管理者ユーザー・パスワード。
パスワードの確認		WebSphere Application Server 管理者パスワードのユーザー入力を確認します。
VNC を使用可能に設定 (Enable VNC)	True	この値はロックされていて、変更できません。

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 7. 構成可能なパラメーター

パラメーター名		説明
仮想 CPU 数	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)	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)。
セル名	CloudBurstCell	カスタム・ノード・パーツ構成のセル名値は無視されます。
ノード名	SOAPolicyAdvancedNode	Advanced Runtime パターン内のカスタム・ノード仮想マシンにある、ノードのノード名。

表 7. 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 (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	virtuser	WebSphere Application Server 環境の管理者ユーザー名。この値を変更してはなりません。
WebSphere 管理パスワード		WebSphere Application Server 環境の管理者ユーザー・パスワード。
パスワードの確認		WebSphere Application Server 管理者パスワードのユーザー入力を確認します。
VNC を使用可能に設定 (Enable VNC)	True	この値はロックされていて、変更できません。

DataPower 部品

DataPower 部品には、いくつかの構成オプションが含まれています。

DataPower 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、以下の表で説明します。

表 8. 構成済みパラメーター

パラメーター名	デフォルト値	説明
仮想 CPU 数	4	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)	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)。
管理パスワード (admin password)		DataPower 管理者のパスワード。
パスワードの確認 (Verify password)		admin password に対するユーザー入力を確認します。
SSH を有効にする (Enable SSH)	True (はい)	SSH (DataPower コマンド行インターフェースを使用する場合) を有効にします。
SSH ポート (SSH port)	22	SSH のポート。
XML 管理インターフェースを有効にする (Enable XML Management interface)	True (はい)	XML 管理インターフェースを有効にします。このインターフェースを有効にすると、管理者は標準の SOAP インターフェースを使って状況要求と構成要求を DataPower アプライアンスに送信できるようになります。
XML 管理インターフェース・ポート (XML Management Interface port)	5550	XML 管理インターフェースのポート。

表 8. 構成済みパラメーター (続き)

パラメーター名	デフォルト値	説明
Web 管理サービスを使用可能にする (Enable Web Management Service)	True (はい)	DataPower アプライアンスとの対話について WebGUI を有効にします。
Web 管理サービス・ポート (Web Management Service port)	9090	WebGUI のポート。
RAID ディレクトリー (RAID directory)	raid0	DataPower 補助データ・ストレージ内のファイルにアクセスできるディレクトリー。

スクリプト・パッケージ

IBM SOA Policy Gateway Pattern には、7 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 2.5.0.0 - DataPower Domain
- SOA Policy Gateway 2.5.0.0 - Promotion
- SOA Policy Gateway 2.5.0.0 - Samples
- SOA Policy Gateway 2.5.0.0 - Security
- SOA Policy Gateway 2.5.0.0 - DataPower Domain
- SOA Policy Gateway 2.5.0.0 - Add Named Queries
- SOA Policy Gateway 2.5.0.0 - Tear Down

Add Named Queries スクリプトと Tear Down スクリプトには、ユーザーが構成できるパラメーターは含まれていません。

スクリプト: SOA Policy Gateway 2.5.0.0 - 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。このスクリプトは、WSRR ランタイムと最大 10 台の DataPower (仮想) アプライアンスとの間の接続を構成します。

パラメーター

表 9. 構成可能なパラメーター

パラメーター名	デフォルト値	説明
DataPower_hostname	*この値はロックされていて、変更できません。*	モニター対象の DataPower インスタンスまたはアプライアンスのホスト名。
DataPower_admin_id	*この値はロックされていて、変更できません。*	インスタンスまたはアプライアンスの管理者ユーザー ID。
DataPower_XML_mgmt_port	*この値はロックされていて、変更できません。*	DataPower インスタンスまたはアプライアンスの XML 管理インターフェースとの通信用ポート。

表 9. 構成可能なパラメーター (続き)

パラメーター名	デフォルト値	説明
DataPower_admin_password	*この値はロックされていて、変更できません。*	管理者ユーザー ID のパスワード。
パスワードの確認	*この値はロックされていて、変更できません。*	管理者ユーザー ID のパスワードを繰り返します。
DataPower2_hostname	*この値はロックされていて、変更できません。*	
DataPower2_admin_id	*この値はロックされていて、変更できません。*	
DataPower2_XML_mgmt_port	*この値はロックされていて、変更できません。*	
DataPower2_admin_password	*この値はロックされていて、変更できません。*	
パスワードの確認	*この値はロックされていて、変更できません。*	
...		...
DataPower10_hostname	*この値はロックされていて、変更できません。*	
DataPower10_admin_id	*この値はロックされていて、変更できません。*	
DataPower10_XML_mgmt_port	*この値はロックされていて、変更できません。*	
DataPower10_admin_password	*この値はロックされていて、変更できません。*	
パスワードの確認	*この値はロックされていて、変更できません。*	
New_DataPower_domain	デフォルト値はパターン・タイプによって異なります。 • SOAPolicyAdvancedRuntime • SOAPolicyBasicRuntime	各 DataPower アプライアンスまたはインスタンスで作成する新規ドメイン名。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	True	サポート用の場合、この設定は無視してかまいません。

スクリプト: SOA Policy Gateway 2.5.0.0 - Promotion

Promotion スクリプトにより、Basic Runtime または 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 パターンと 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 10. 構成可能なパラメーター

パラメーター名	デフォルト値	説明
WSRR_GOV_DMGR_hostname		WSRR クラスター用の Dmgr のホスト名。
WSRR_GOV_DMGR_cellname	SOAPolicyGMCell	WSRR クラスター用のセル名。
WSRR_GOV_admin_user	virtuser	WSRR Governance Cell の管理 ID。
WSRR_GOV_admin_password		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、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ます。この鍵は Governance Master に由来し、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。

スクリプト: SOA Policy Gateway 2.5.0.0 - 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

これらのパラメーターはどれもユーザーが設定することはできません。

表 11. 構成可能なパラメーター

パラメーター名		説明
SCP_host	*この値はロックされていて、変更できません。*	
SCP_user	*この値はロックされていて、変更できません。*	
SCP_password	*この値はロックされていて、変更できません。*	
パスワードの確認	*この値はロックされていて、変更できません。*	
SCP_zip_location	*この値はロックされていて、変更できません。*	

表 11. 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_file	この値はロックされていて、変更できません。	
CLIENT_PUBLIC _KEY_password	この値はロックされていて、変更できません。	
パスワードの確認		
CLIENT_PRIVATE_KEY_file	この値はロックされていて、変更できません。	
CLIENT_PRIVATE_KEY_password	この値はロックされていて、変更できません。	
パスワードの確認		
CLI_FILE_file	この値はロックされていて、変更できません。	
パスワードの確認	この値はロックされていて、変更できません。	
DataPower_hostname	この値はロックされていて、変更できません。	DataPower インスタンスのホスト名。
DataPower_XML_mgmt_port	この値はロックされていて、変更できません。	DataPower XML Management Interface に使用されるポート。
DataPower_admin_id	この値はロックされていて、変更できません。	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	この値はロックされていて、変更できません。	DataPower_admin_id のパスワード。
パスワードの確認	この値はロックされていて、変更できません。	DataPower_admin_password のユーザー入力を確認します。
SOAPolicySample_DataPower_domain	この値はロックされていて、変更できません。	サンプル・ドメイン名。 DataPower インスタンスの既存のどのドメインとも一致しないものでなければなりません。
SamplePolicySample_starting_port	この値はロックされていて、変更できません。	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。スクリプトは、ポートが空いているかどうかを検査しません。
LDAP_hostname	この値はロックされていて、変更できません。	WSRR スタンドアロン・パーツのホスト名。ここで LDAP サーバーもホストされます。
LDAP_port	この値はロックされていて、変更できません。	LDAP サーバーのポート。
LDAP_password	この値はロックされていて、変更できません。	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	この値はロックされていて、変更できません。	LDAP_password のユーザー入力を確認します。

表 11. 構成可能なパラメーター (続き)

パラメーター名		説明
LDAP_DN	この値はロックされていて、変更できません。	LDAP へのバインドに使用される識別名。

スクリプト: SOA Policy Gateway 2.5.0.0 - Security

Security スクリプトは、パターン内の DataPower と WSRR システムの間でセキュリティー情報 (証明書など) をコピーします。

Security スクリプト・ファイルの構成パラメーターはサポート用です。これらはデフォルト値設定のままにしておいてください。

スクリプト: SOA Policy Gateway 2.5.0.0 - DataPower Monitoring (x86 のみ)

DataPower Monitoring スクリプトは、DataPower モニタリング共用サービスの接続パラメーターを指定します。ITCAM DataPower データ・コレクターとエージェントは、Core OS パーツで実行されます。

パラメーター

モニタリング・サービスは最大 10 台の DataPower 仮想アプライアンスをモニターできます。

表 12. 構成可能なパラメーター

パラメーター名	デフォルト値	説明
DataPower1_hostname		モニター対象の DataPower 仮想アプライアンスのホスト名。
DataPower1_admin_id	admin	仮想アプライアンスの管理者ユーザー ID。
DataPower1_XML_mgmt_port	5550	DataPower 仮想アプライアンスの XML 管理インターフェースとの通信用ポート。
DataPower1_admin_password		管理者ユーザー ID のパスワード。
パスワードの確認		管理者ユーザー ID のパスワードを繰り返します。
DataPower2_hostname		
DataPower2_admin_id	admin	
DataPower2_XML_mgmt_port	5550	
DataPower2_admin_password		
パスワードの確認		
...		...
DataPower10_hostname		
DataPower10_admin_id	admin	
DataPower10_XML_mgmt_port	5550	
DataPower10_admin_password		

表 12. 構成可能なパラメーター (続き)

パラメーター名	デフォルト値	説明
パスワードの確認		

スクリプト: SOA Policy Gateway 2.5.0.0 - External DataPower Monitoring

DataPower Monitoring スクリプトは、DataPower モニタリング共用サービスの接続パラメーターを指定します。ITCAM DataPower データ・コレクターとエージェントは、Core OS パーツで実行されます。

パラメーター

モニタリング・サービスは最大 10 台の DataPower アプライアンスをモニターできます。

表 13. 構成可能なパラメーター

パラメーター名	デフォルト値	説明
DataPower1_hostname		モニター対象の DataPower アプライアンスのホスト名。
DataPower1_admin_id	admin	アプライアンスの管理者ユーザー ID。
DataPower1_XML_mgmt_port	5550	DataPower アプライアンスの XML 管理インターフェースとの通信用ポート。
DataPower1_admin_password		管理者ユーザー ID のパスワード。
パスワードの確認		管理者ユーザー ID のパスワードを繰り返します。
DataPower2_hostname		
DataPower2_admin_id	admin	
DataPower2_XML_mgmt_port	5550	
DataPower2_admin_password		
パスワードの確認		
...		...
DataPower10_hostname		
DataPower10_admin_id	admin	
DataPower10_XML_mgmt_port	5550	
DataPower10_admin_password		
パスワードの確認		

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

IBM SOA Policy Gateway Pattern には、繰り返し可能なデプロイメントのパターン定義が用意されています。以下のトピックでは、パターンをデプロイする方法について説明します。

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、 49 ページの『パターンのデプロイ』を参照してください。パターンについては、 19 ページの『第 4 章 パターン、パーツ、およびスクリプト・パッケージ』で説明します。

関連タスク:

13 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。パターンをダウンロードしてインストールする方法、インストール後にパターンを検証し、ライセンスを承諾する方法、および関係するユーザーの役割を理解するには、このセクションのトピックを検討してください。

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。パターンのデプロイメントは、Governance Master から始まり、次に 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

- 外部 DataPower アプライアンスを使用している場合、アプライアンスでリモート管理できるように準備します。詳しくは、 48 ページの『IBM SOA Policy Gateway Pattern のための DataPower アプライアンスの構成』を参照してください。

次のようにして Governance Master パターンをデプロイします。

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、ランタイム・パターンをデプロイします。詳しくは、 53 ページの『Governance Master パターンのデプロイ』を参照してください。

次のようにしてランタイム・パターンをデプロイします。

1. スタンドアロン環境を持つ Basic Runtime パターンと、クラスター環境を持つ Advanced Runtime パターンのどちらが必要かを判断します。
2. ランタイム・パターンで必要とする DataPower インスタンスまたはアプライアンスの数を判断します。

DataPower を含むパターンには、デフォルトで 2 つの DataPower インスタンスがあります。最大 10 個の DataPower インスタンスを構成できます。詳しくは、 59 ページの『パターンへの DataPower インスタンスの追加』を参照してください。

外部 DataPower を持つパターンは、最大 10 台の DataPower アプライアンスを処理するように構成できます。 60 ページの『Basic および Advanced External DataPower パターンのデプロイ』を参照してください。

注: この構成の完了後に、さらに DataPower インスタンスおよびアプライアンスを追加することはできません。

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、 54 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。スタンドアロン・システムをデプロイする場合、必要に応じて Governance Master パターン情報は省略できます (この場合、デプロイメントでエラーが表示されますが、そのエラーは無視してかまいません)。
4. ランタイム・システムがステージングか、実動かを指定します。
5. パターンをデプロイします。詳しくは、 56 ページの『Advanced Runtime パターンのデプロイ』または 55 ページの『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・パターン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. 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、 49 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。
2. DataPower ドメインでゲートウェイ構成の準備が整いました。仮想 DataPower アプライアンスを使用している場合、まず最新のフィックスパックを適用する必要があります。 57 ページの『デプロイ済みインスタンスの DataPower の更新』を参照してください。

IBM SOA Policy Gateway Pattern のための DataPower アプライアンスの構成

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. DataPower アプライアンス WebGUI 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

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は相互認証が実行されます。必要な証明書交換はスクリプトで実行されます。パターンと共に提供されるデフォルトの SSL 証明書は、パターンの作成に使用されたホストで作成されたことに注意してください。

セキュリティーの向上

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。保護の高い環境を生成するには、WebSphere Application Server の標準セキュリティー技法を使用できます。

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

パターンのデプロイ

IBM PureApplication System を含んだパターンをクラウドにデプロイすると、稼働する SOA ポリシー・ゲートウェイ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。PureAS システム管理者からデプロイ先の環境、クラウド・グループ、および IP グループの詳細情報を入手する必要があります。

このタスクについて

ワークロード・コンソールを使用して、パターンをデプロイします。

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

システム・モニター共用サービスのデプロイ

SOA Policy Gateway のシステム・モニターの共用サービスをデプロイすると、仮想システムのモニター・コンポーネントが提供されます。

始める前に

PureAS システム管理者はシステム・モニター共用サービスを開始して、そのサービスを開始したクラウド・グループと環境について知らせる必要があります。SOA Policy Gateway システム・モニター共用サービスをデプロイし、ランタイム・パターンとガバナンス・パターンをデプロイするには、同じクラウド・グループと環境を使用する必要があります。

WSRR インスタンスをモニターするには、WebSphere Application Server のシステム・モニターの共用サービスが開始される必要があるため、このサービスが PureAS システムに設定されていることを確認する必要があります。

手順

ワークロード・コンソールで以下のステップを実行します。

1. 「**インスタンス (Instances)**」 > 「**共用サービス (Shared Services)**」をクリックします。
2. パターンがデプロイされるクラウド・グループでシステム・モニター・サービスが実行されていることを確認します。実行されていない場合、PureAS 管理者に開始を依頼してください。
3. DataPower モニター共用サービスを使用可能にする方法
   a. 「**クラウド (Cloud)**」 > 「**パターン・タイプ (Pattern Types)**」をクリックします。
   b. 「パターン・タイプ (Pattern Types)」ペインで、「**System Monitoring for SOA Policy Gateway Pattern 2.5.0.0**」エントリーを選択します。
   c. 「**状況 (Status)**」フィールドで「**使用可能 (Enable)**」をクリックして、状況フィールドが「**使用不可 (Disable)**」に変わるのを待ちます。
4. WebSphere Application Server モニター共用サービスを開始する方法
   a. 「**インスタンス (Instances)**」 > 「**共用サービス (Shared Services)**」をクリックします。
   b. 「共用サービス・インスタンス (Shared Service Instances)」ペインの正符号をクリックして、「共用サービスのデプロイ (Deploy Shared Service)」ウィンドウを開きます。
   c. 「**WebSphere Application Server のシステム・モニター (System Monitoring for WebSphere Application Server)**」を選択して、「**OK**」をクリックします。
   d. 「共用サービスの構成とデプロイ (Configure and Deploy a Shared Service)」ウィンドウで、下部の 2 つのチェック・ボックスを選択して、以前にデプロイしたパターンでサービスを開始するかどうかを指定します。「**OK**」をクリックします。
   e. 「仮想アプリケーションのデプロイ (Deploy Virtual Application)」ウィンドウで、PureAS システム管理者からの通知に従って「**ターゲット・クラウド・グループ (Target cloud group)**」、「**IP グループ (IP group)**」、および「**プロファイル (Profile)**」を指定します。これらは、仮想システムのデプロイ先と同じ設定にする必要があります。
5. WebSphere DataPower モニター共用サービスを開始する方法
   a. メニュー・バーで、「**インスタンス (Instances)**」 > 「**共用サービス (Shared Services)**」をクリックします。
   b. 「共用サービス・インスタンス (Shared Service Instances)」ペインの正符号をクリックして、「共用サービスのデプロイ (Deploy Shared Service)」ウィンドウを開きます。
   c. リストから「**WebSphere DataPower のシステム・モニター (System Monitoring for WebSphere DataPower)**」を選択して、「**OK**」をクリックします。

d. 「共用サービスの構成とデプロイ (Configure and deploy a shared service)」ウィンドウで、下部の 2 つのチェック・ボックスを選択して、以前にデプロイしたパターンでモニターを開始するかどうかを指定します。「**OK**」をクリックします。

e. 「仮想アプリケーションのデプロイ (Deploy Virtual Application)」ウィンドウで、PureAS システム管理者からの通知に従って「**ターゲット・クラウド・グループ (Target cloud group)**」、「**IP グループ (IP group)**」、および「**プロファイル (Profile)**」を指定します。これらは、仮想システムのデプロイ先と同じ設定にする必要があります。

f. モニター共用サービスへのデバッグ・アクセスが必要な場合は、SSH 鍵を生成して保存します。

g. 「**OK**」をクリックします。

タスクの結果

WebSphere DataPower のシステム・モニターの共用サービスが実行中であると表示されます。WebSphere Application Server のシステム・モニターの共用サービスが実行中であると表示されます。

次のタスク

デプロイメントを検証するには、58 ページの『デプロイメントの検証』を参照してください。

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。このパターンは、x86 システム上でのみ使用できます。

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 Basic Runtime Sample パターンをデプロイするには、以下の手順を実行します。

1. ワークロード・コンソールで、「**パターン (Patterns)**」 > 「**仮想システム (Virtual Systems)**」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 2.5.0.0 - 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. 「**環境の選択 (Choose Environment)**」セクションを展開し、PureAS システム管理者からの通知に従って「**プロファイル (Profile)**」を指定します。

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。PureAS システム管理者からの通知に従って「**クラウド・グループ (Cloud group)**」と「**IP グループ (IP group)**」を指定します。パターン固有の構成パラメーターおよびスクリプト固有の構成パラメーターの詳細については、以下のトピックを参照してください。

注: このパターンのパスワードはすべて、デフォルトで `password` に設定されています。

- 39 ページの『DataPower 部品』
- 31 ページの『DB2 Enterprise パーツ』.
- 36 ページの『WSRR スタンドアロン・サーバー・パーツ』
- 42 ページの『スクリプト: SOA Policy Gateway 2.5.0.0 - Sample』

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、58 ページの『デプロイメントの検証』を参照してください。

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。

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. ワークロード・コンソールで、「**パターン (Patterns)**」 > 「**仮想システム (Virtual Systems)**」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 2.5.0.0 - 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. 「**環境の選択 (Choose Environment)**」セクションを展開し、PureAS システム管理者からの通知に従って「**プロファイル (Profile)**」を指定します。
   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。PureAS システム管理者からの通知に従って「**クラウド・グループ (Cloud group)**」と「**IP グループ (IP group)**」を指定します。パターン固有

の構成パラメーターおよびスクリプト固有の構成パラメーターの詳細については、以下のトピックを参照してください。

- 33 ページの『DB2 Enterprise HADR Primary パーツ』
- 37 ページの『WSRR デプロイメント・マネージャー・パーツ』
- 38 ページの『WSRR カスタム・ノード・パーツ』
- 35 ページの『DB2 Enterprise HADR Standby パーツ』

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、58 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

ランタイム・パターンをデプロイする前に、Governance Master がデプロイされている必要があります。

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。

   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、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

   Runtime パターンをスタンドアロン・システムとしてデプロイする場合、これらのパラメーターを「Unset」に設定します。このように設定すると、プロモーション・スクリプト・パッケージが失敗するため、「**仮想システム (Virtual System)**」 > 「**インスタンス (Instances)**」で、デプロイメントは「**失敗 (failed)**」と表示されます。しかし、デプロイメントは引き続き使用可能です。

Basic Runtime パターンのデプロイ

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、以下のタスクを実行します。

- 外部 DataPower を使用して Basic Runtime パターンをデプロイする場合、DataPower アプライアンスを IBM SOA Policy Gateway Pattern に合わせて構成します。 48 ページの『IBM SOA Policy Gateway Pattern のための DataPower アプライアンスの構成』を参照してください。Power システムでは、外部 DataPower のみがサポートされています。
- Governance Master デプロイメント情報を取得します。 54 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、ランタイム・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。この制限の原因は、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ことです。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

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 2.5.0.0 - Basic Runtime External DataPower**」または「**SOA Policy Gateway 2.5.0.0 - Basic 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. 「**環境の選択 (Choose Environment)**」セクションを展開し、PureAS システム管理者からの通知に従って「**プロファイル (Profile)**」を指定します。
   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。PureAS システム管理者からの通知に従って「**クラウド・グループ (Cloud group)**」と「**IP グループ (IP group)**」を指定します。パターン固有の構成パラメーターおよびスクリプト固有の構成パラメーターの詳細については、以下のトピックを参照してください。

注: Governance Master を使用せずにパターンをデプロイする場合、Governance Master のホスト名パラメーターとして「Unset」と入力します。こうすると、デプロイメントでプロモーション・スクリプト・パッケージに障害が発生していると報告されますが、他に影響はありません。

- 39 ページの『DataPower 部品』
- 31 ページの『DB2 Enterprise パーツ』
- 36 ページの『WSRR スタンドアロン・サーバー・パーツ』
- 44 ページの『スクリプト: SOA Policy Gateway 2.5.0.0 - Security』
- 41 ページの『スクリプト: SOA Policy Gateway 2.5.0.0 - Promotion』
- 40 ページの『スクリプト: SOA Policy Gateway 2.5.0.0 - DataPower Domain』
- 44 ページの『スクリプト: SOA Policy Gateway 2.5.0.0 - DataPower Monitoring (x86 のみ)』

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、58 ページの『デプロイメントの検証』を参照してください。

Advanced Runtime パターンのデプロイ

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、以下のタスクを実行してください。

- 外部 DataPower を使用して Advanced Runtime パターンをデプロイする場合、パターンに接続するように DataPower アプライアンスを構成します。48 ページの『IBM SOA Policy Gateway Pattern のための DataPower アプライアンスの構成』を参照してください。Power システムでは、外部 DataPower のみがサポートされています。
- Governance Master デプロイメント情報を取得します。54 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、ランタイム・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。この制限の原因は、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ことです。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

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 2.5.0.0 -Advanced Runtime External DataPower**」または「**SOA Policy Gateway 2.5.0.0 - 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. 「**環境の選択 (Choose Environment)**」セクションを展開し、PureAS システム管理者からの通知に従って「**プロファイル (Profile)**」を指定します。
   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。PureAS システム管理者からの通知に従って「**クラウド・グループ (Cloud group)**」と「**IP グループ (IP group)**」を指定します。パターン固有の構成パラメーターおよびスクリプト固有の構成パラメーターの詳細については、以下のトピックを参照してください。

      注: Governance Master を使用せずにパターンをデプロイする場合、Governance Master のホスト名パラメーターとして「Unset」と入力します。こうすると、デプロイメントでプロモーション・スクリプト・パッケージに障害が発生していると報告されますが、他に影響はありません。

      - 39 ページの『DataPower 部品』
      - 33 ページの『DB2 Enterprise HADR Primary パーツ』
      - 37 ページの『WSRR デプロイメント・マネージャー・パーツ』
      - 41 ページの『スクリプト: SOA Policy Gateway 2.5.0.0 - Promotion』
      - 40 ページの『スクリプト: SOA Policy Gateway 2.5.0.0 - DataPower Domain』
      - 38 ページの『WSRR カスタム・ノード・パーツ』
      - 35 ページの『DB2 Enterprise HADR Standby パーツ』
      - 44 ページの『スクリプト: SOA Policy Gateway 2.5.0.0 - DataPower Monitoring (x86 のみ)』
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、58 ページの『デプロイメントの検証』を参照してください。

デプロイ済みインスタンスの DataPower の更新

WebSphere DataPower コンポーネントを含むパターンのデプロイ後、DataPower を最新のフィックスパックに更新する必要があります。

このタスクについて

Fix Central からフィックスパックをダウンロードして、DataPower WebGUI に適用することによって、DataPower を更新します。

手順

1. 以下のようにして、Fix Central から更新パッケージをダウンロードします。
   a. Fix Central で、WebSphere DataPower SOA Appliances を探します。
   b. パッケージ XI52-virtual-6.0.0.1-Firmware を選択してダウンロードします。
2. デプロイ済みのパターンの DataPower 仮想マシンのために WebGUI 接続します。 92 ページの『仮想 DataPower のコンソールへの接続』を参照します。
3. コントロール・パネルで、「**システム制御 (System Control)**」を選択します。
4. 「**ブート・イメージ (Boot Image)**」セクションを見つけます。
5. ダウンロードしたフィックスパックから `xi6001.scrypt4` ファイルを DataPower アプライアンスにアップロードします。DataPower WebGUI でファイル・マネージャーを使用します。
6. 「**ファームウェア・ファイル (Firmware File)**」リストで、アップロードしたスクリプトを選択します。
7. ご使用条件に同意して、「**ブート・イメージ (Boot Image)**」をクリックします。
8. プロンプトに従って、フィックスパックをインストールします。

デプロイメントの検証

パターンのデプロイ後、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、 111 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。 64 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。

付加的なランタイム環境の追加

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。ステージング環境および実稼働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環境への制御されたプロモーションが可能になります。この手順は、ユーザーの組織が環境を同じ方法で定義し、「ステージング」を実動前の環境として、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するのを可能に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、 47 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、 53 ページの『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 の詳細を使用して、Basic Runtime パターンまたは Advanced Runtime パターンを構成します。詳しくは、 54 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. 事前定義の 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、 55 ページの『Basic Runtime パターンのデプロイ』および 56 ページの『Advanced Runtime パターンのデプロイ』を参照してください。

パターンへの DataPower インスタンスの追加

内部 DataPower インスタンスを持つ基本パターンと拡張パターンは、デフォルトで 2 つのインスタンスを持ちます。各パターンは、最大で合計 10 の DataPower インスタンスを持つことができます。

このタスクについて

パターンそのものは編集できません。パターンのコピーを作成して、それを編集することによって、Basic Runtime パターンまたは Advanced Runtime パターンに DataPower インスタンスを追加できます。

手順

1. ワークロード・コンソールでパターンを開きます。
2. 「**クローン (Clone)**」をクリックして、パターンのコピーの名前を指定します。
3. 「**編集 (Edit)**」をクリックします。
4. 部品リストから DataPower 部品をドラッグして、パターンに追加します。
5. 「**編集の完了**」をクリックします。

パターンからの DataPower インスタンスの削除

必要に応じて、パターンから内部の DataPower インスタンスを削除できます。

このタスクについて

パターンそのものは編集できません。パターンのコピーを作成し、それを編集することによって、Basic Runtime パターンまたは Advanced Runtime パターンから DataPower インスタンスを削除できます。

手順

1. ワークロード・コンソールでパターンを開きます。
2. 「**クローン (Clone)**」をクリックして、パターンのコピーの名前を指定します。
3. 「**編集 (Edit)**」をクリックします。
4. 削除アイコンをクリックして、DataPower インスタンスを削除します。

注: DataPower インスタンスは、番号と逆の順番で削除する必要があります。キャンバス上の各 DataPower インスタンスには、その名前フィールドに番号が含まれています。このフィールドは、プロパティー・アイコンをクリックすると表示されます。名前の形式は、「DataPower_XI52*x*」です。ここで、*x* は番号です (最初の DataPower インスタンスには番号がなく、名前は「DataPower_XI52」となります)。最も大きい番号が付けられている DataPower インスタンスが通常キャンバスの左上に置かれます。

5. 「**編集の完了**」をクリックします。

Basic および Advanced External DataPower パターンのデプロイ

SOA Policy Gateway Basic Runtime External DataPower および SOA Policy Gateway Advanced Runtime External DataPower パターンは、最大 10 の DataPower アプライアンスにデプロイできます。

このタスクについて

パターンのデプロイについて詳しくは、55 ページの『Basic Runtime パターンのデプロイ』または 56 ページの『Advanced Runtime パターンのデプロイ』を参照してください。値を設定する必要のある構成パラメーターの詳細については、36 ページの『WSRR スタンドアロン・サーバー・パーツ』、37 ページの『WSRR デプロイ

メント・マネージャー・パーツ』、および 44 ページの『スクリプト: SOA Policy Gateway 2.5.0.0 - DataPower Monitoring (x86 のみ)』を参照してください。

手順

1. パターンをデプロイして、「**仮想部品の構成 (Configure virtual parts)**」をクリックします。
2. WSRR スタンドアロンまたは WSRR デプロイメント・マネージャー部品については、アプライアンスごとに以下の情報を入力します。
   - DataPower_hostname
   - DataPower_XML_mgmt_port
   - DataPower_admin_id
   - DataPower_admin_password
   - パスワードの確認
   - New_DataPower_domain

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 Web サービスと RESTful API で構成され、これらは両方とも WSRR で記述され、管理されます。DataPower ドメインは WSRR を使用してゲートウェイとして構成され、サービスを実行するためのサンプル Web クライアントが提供されています。

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、およびモバイル向け操作の 1 つを再現する RESTful サービスです。 Store Web サービスには次の 3 つの操作があります。

- purchase
- findInventory
- returnProduct

ここに示した findInventory 操作は RESTful サービスとしても利用できます。

サンプル Web サービス

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・ポリシーが添付されます。

- 「Store.wsdl に対する妥当性検査 (Validation against Store.wsdl)」。このサンプルでは、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)」。デモンストレーションを簡単にするため、このしきい値は低く設定しています。

Store サービスのコンシューマーは StoreConsumer アプリケーションで、そのコンシューマー ID は「CEO」です。このコンシューマーは、Gold と Silver の 2 つのサービス・レベル・アグリーメント (SLA) を持ちます。コンシューマー ID が「CEO」でコンテキスト ID が「Silver」である要求が DataPower に着信すると、Silver SLA が実施されているのでその要求はパススルーを許可されます。コンシューマー ID が「CEO」でコンテキスト ID が「Gold」の場合、Gold SLA が一致し

ます。この SLA には再経路指定ポリシーが添付されているので、要求はこのポリシーで提示された代替エンドポイントに再経路指定されます。

コンシューマー ID が「CEO」以外である要求が着信した場合、このコンシューマー ID を持つアプリケーション・バージョンは存在しません。それで、一致可能な SLA も存在しないので、これは匿名コンシューマーからの要求になります。それで、匿名 SLA に添付されたポリシーが適用されます。この場合は、ログに通知が現れるようになります。サンプルでは「CEO」以外のコンシューマー ID を指定した要求を送信する手段は提供していないことに注意してください。

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。 LDAP サーバーにはユーザー資格情報を正しいグループにマッピングするためのサンプルが提供されます。

サンプル・アプリケーションのフロー・ダイアグラムはアプリケーションのフローを示し、各ボックスはそれぞれ異なる DataPower ゲートウェイを表しています。

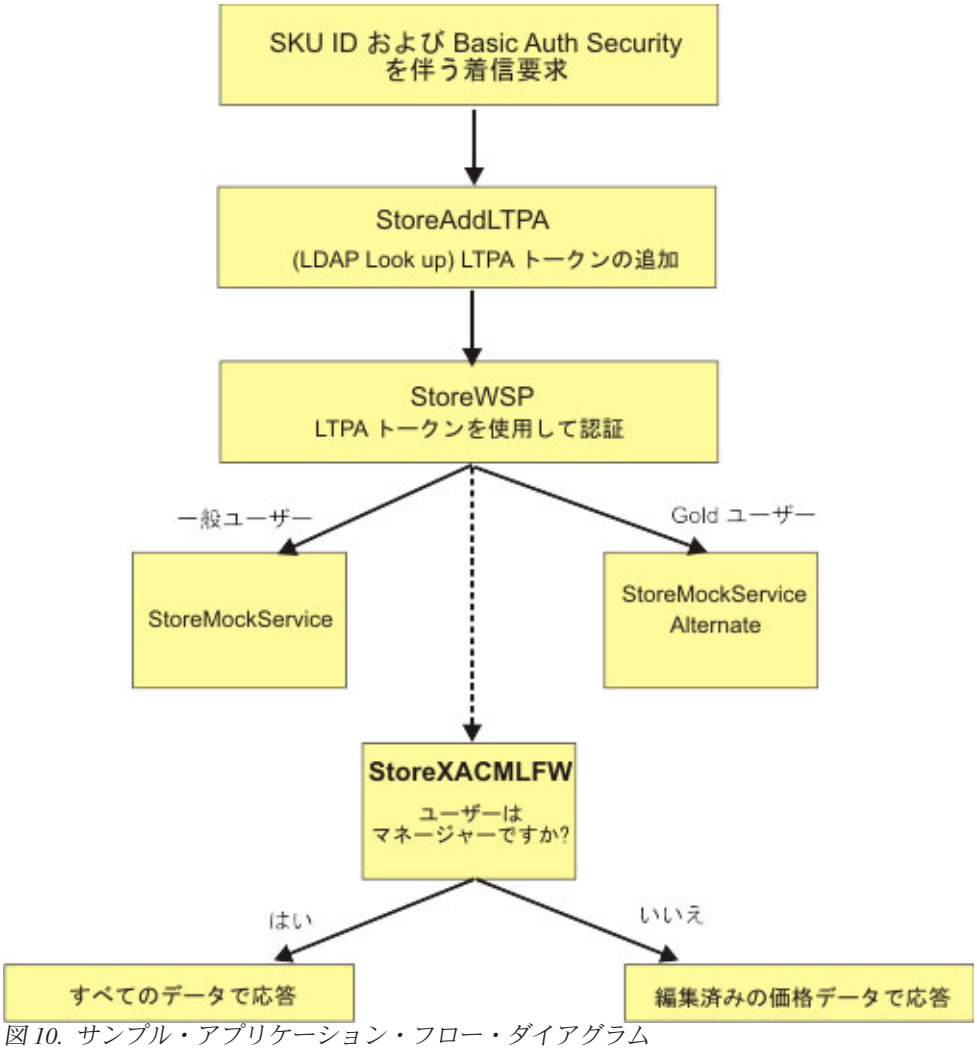


図 10. サンプル・アプリケーション・フロー・ダイアグラム

サンプル RESTful サービス

RESTful サービスは、ポリシーをどのように使用するかを除いては、Web サービスと同様の方法で管理されます。Web サービスの場合、Silver カスタマー用と Gold カスタマー用の 2 つの SLA があります。一方、REST サービスでは SLD レベルで (すべての要求に適用される) 添付されるポリシーはありません。その代わりに、SLA にはそれぞれ 1 つのポリシーが添付されます。Gold SLA には、90 秒に 5 件を超える要求が出されるとその後のメッセージを拒否するポリシーがあり、Silver では 90 秒で 2 件の要求を許可した後で拒否されます。

サンプルの WSRR 成果物の概要

Store サービスを記述する WSRR 成果物をここに記載します。REST サービスの成果物は同様のパターンに従います。

Bob's Warehouse は、提供する Store サービスとコンシュームする StoreConsumer アプリケーションの両方を所有する組織です。

Warehouse Business サービスというオブジェクトの下に、すべてのバージョンの Store サービスが置かれています。Store サービスのバージョンは Store サービスの特定のバージョンを表します。このバージョンは再利用のために提供されるサービスです。Store サービス・レベル定義 (SLD) には 2 つのポリシーが添付されています。最初のポリシーは、90 秒以内に 5 件のメッセージがあるとその後、メッセージを拒否します。 2 つ目のポリシーは、Store.wsdl スキーマに照らした妥当性検査を実行します。これらのポリシーは、要求元がだれであるかにかかわらず、Store サービスへの要求は妥当性検査され、任意の 90 秒間にサービスに対して最大 5 件の要求が許可されることを意味します。SLD には、匿名サービス・レベル・アグリーメント (SLA) もあります。一致する SLA がない要求が着信すると、この SLA に添付されたどのポリシーも適用されます。以下の条件が満たされると、SLA が一致します。

- 要求内のコンシューマー ID に一致する、コンシュームするアプリケーション・バージョンが存在する。
- このコンシュームするアプリケーション・バージョンとコンシュームされるサービスの SLD の間で実施されている SLA で、要求内のコンテキスト ID と一致するものが存在する。

StoreConsumer ビジネス・アプリケーションは StoreConsumer アプリケーションを表し、一方、StoreConsumer アプリケーション・バージョンはこのアプリケーションの特定のバージョンです。このアプリケーションはコンシューマーであり、Store サービスを再利用しています。このコンシューマー ID は「CEO」です。このアプリケーションで実施されている SLA は 2 つ存在し、これらが、このアプリケーションによる Store サービスのコンシュームを許可するアグリーメントを構成します。1 つはコンテキスト ID が「Gold」であり、これは、要求のコンテキスト ID が「Gold」の StoreConsumer アプリケーションからの要求と一致することを意味します。もう 1 つは Silver と一致します。Gold SLA には再経路指定要求に添付されたポリシーがあるので、コンテキスト ID に Gold が設定された StoreConsumer アプリケーションからの要求はどれも、そのポリシーで指定されたエンドポイントに再経路指定されます。Silver SLA には添付されたポリシーがないので、Silver SLA が

存在すると、コンテキスト ID が Silver である StoreConsumer アプリケーションからの要求はパススルーを許可されますが、どのポリシーも適用されません。

このサンプルでは、匿名 SLA に添付された通知ポリシーがあります。

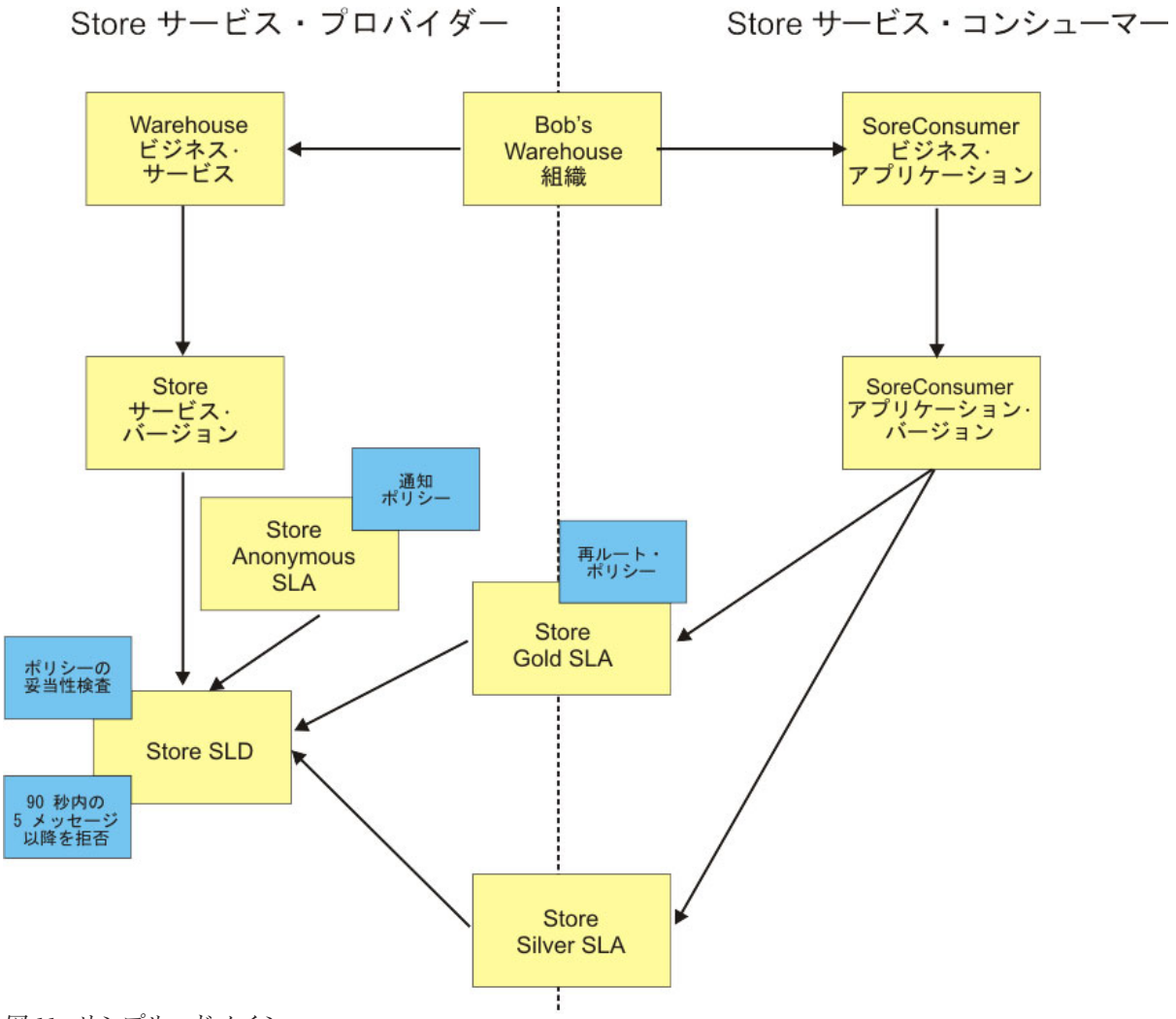


図 11. サンプル・ドメイン

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は 6 種類のコマンド・ライン・テストを実行できます。

Basic Sample Runtime をデプロイするには、52 ページの『Basic Runtime Sample パターンのデプロイ』を参照してください。

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。ホスト名を検索するには、「**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. 使用可能なオプションは次のとおりです。
   - **標準要求 (Standard Request)** - Store サービスに findInventory 要求を送信します。コンテキスト ID は Silver です。コンシューマー ID は CEO です。正常な結果が得られると、テキスト「Part: SKU10 Price: 401.73」が表示されます。
   - **ルーティング・ポリシー・テスト (Routing Policy Test)** - 標準要求と同様ですが、コンテキスト ID に Gold を使用します。要求は、サービスを実行する代替エンドポイントに経路指定されます。正常な結果が得られると、「Part: GOLDSKU10 Price: 401.73」が返されます。
   - **妥当性検査ポリシー・テスト (Validation Policy Test)** - 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、要求の妥当性検査を行い、無効なメッセージを拒否するため、DataPower が必要です。正常な結果が得られると、DataPower からの応答メッセージ「`Internal Error (from client)`」が返されます。
   - **REST Gold** - コンシューマー ID CEO およびコンテキスト ID Gold を使用して、SKU RESTful サービスに要求を送信します。Gold 要求は 90 秒に 5 件のメッセージのみを許可するポリシーに従います。要求が成功すると、結果「Part: SKU33 Price: 136.43」が表示されます。
   - **REST Silver** - Rest GOLD と同様ですが、コンテキスト ID に Silver を使用します。 Silver 要求では、90 秒間に 3 件の別個の要求が許可されます。要求が成功すると、結果「Part: SKU33 Price: 136.43」が表示されます。
   - 「**ユーザー ID**」- ユーザー ID オプションには 2 つの値「フル・コンテンツ (Full Content)」と「編集済みコンテンツ (Redacted Content)」のいずれかを指定できます。それぞれのオプションにより、別のユーザーからの要求が発生します。サンプルでは XACML ポリシーが利用されます。このポリシーは価格の参照をマネージャーのみに許可します。「フル・コンテンツ (Full Content)」が選択されなかった場合、応答メッセージの価格の値は編集されます。「編集済みコンテンツ (Redacted Content)」が選択された場合、要求が成功するとその結果には「Price: 0.0」が含められます。RESTful サービスは編集をサポートしません。どのユーザーが選択されたかは影響を与えません。
4. 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、88 ページの『WSRR への接続 - Business Space』を参照してください。

サンプルはコマンド・ラインを使用して実行することもできます。これは、匿名 SLA を使用するトラフィックを送信する唯一の方法です。

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>
```

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 コマンドを入力します。

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

この例では、ConsumerX はマネージャーなので、応答には次のような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>
```

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 コマンドを入力します。

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

応答では価格が編集されていることに注目してください。価格は 0.0 として以下のように表示されます。

```
<?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: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

Gold SLA に添付されたルーティング・ポリシーを実施するには、コンテキスト ID とコンシューマー ID が一致している必要があります。このケースでは、Gold カスタマーの SLA のコンテキスト ID は Gold であり、コンシュームするサービス・バージョンのコンシューマー ID は CEO です。サンプル要求の内容を以下に示します (要件どおりコンテキスト ID とコンシューマー ID が一致していることが確認できます)。

```
<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">Gold</store:ContextIdentifier>
</soapenv:Header><soapenv:Body>
<stor:findInventory><findInventoryReq>
  <sku>SKU10</sku>
  </findInventoryReq>
</stor:findInventory>
</soapenv:Body></soapenv:Envelope>
```

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 コマンドを入力します。

```
curl -k --data-bin @./gold.xml -H "Content-Type: text/xml"
-u ConsumerX:passw0rd http://<yourDataPowerHostName>:62005/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.wsdl 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 要求を入力する場合:

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

次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>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>:62005/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 はマネージャーなので、最初の 5 回の実行では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>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

匿名 SLA に通知ポリシーが添付されます。これは、SLA が実施されていないコンシューマーから要求が着信した場合に実施されます。このサンプルでは、SLA が実施されている唯一のコンシューマーは CEO なので、他のいずれかの値が設定されたコンシューマー ID を含む要求では匿名 SLA にポリシーが実施されます。このケースでは ConsumerX はマネージャーなので、完全な価格情報が表示されます。

コマンド・ラインを使用してこの機能をテストするには、以下の XML を内容とする anon.xml というファイルを作成します。

```
<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">ABC</store:ConsumerIdentifier>
  <store:ContextIdentifier xmlns:store="http://store.com">Gold</store:ContextIdentifier>
</soapenv:Header><soapenv:Body>
<stor:findInventory><findInventoryReq>
```

```
  <sku>SKU10</sku>
  </findInventoryReq>
</stor:findInventory>
</soapenv:Body></soapenv:Envelope>
```

次に、以下のコマンドを入力します。

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

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「通知 (notice)」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「通知 (notice)」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、「制御パネル (Control Panel)」に戻って「**ログの表示 (View Logs)**」アイコンをクリックします。

コマンド・ラインを使用した RESTful サービスのテスト

RESTful インターフェースには、コマンド・ラインから curl を使用してアクセスすることもできます。Web クライアントの場合と同様に、コンテキスト ID Gold では 90 秒ごとに 5 件のメッセージが、Silver では 2 件のメッセージのみが許可されます。

コマンド・ラインを使用してこの機能をテストするには、以下の XML を内容とする restRequest.xml というファイルを作成します。

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

次に、コンテキスト ID Gold を使用してテストするため、以下のコマンドを入力します。

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

コンテキスト ID Silver を使用してテストするには同じコマンドを使用しますが、Gold を Silver に置き換えます。

正常な応答を以下に示します。

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

```
<returns>0</returns>
<supplierID>ABB</supplierID>
<purchaseID/>
</getRequest>
</a:WarehouseSKUGet>
```

しきい値を超えると、以下のメッセージを受け取ります。

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

RESTful サービスに対して匿名 SLA を実行するには (これは単に通知ポリシーを添付するだけですが)、登録されていないいずれかのコンテキスト ID とコンシューマー ID を使用します。Web サービス・サンプルで先に記載したように、DataPower ログに通知が現れます。

関連タスク:

52 ページの『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。このパターンは、x86 システム上でのみ使用できます。

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 (Policy Decision Point (PDP)) を別の DataPower ボックスに移動するため、SSL プロキシー・プロファイルを作成して、url-open 呼び出しで使用することができました。

```
<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 ファイルについて、以下の点に注意してください。

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。

StorePrivateDataXACML.xml

以下のコードに、編集用ポリシー・スタイル・シートを示します。

```
<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

編集スタイル・シート noPriceInfo.xsl を変更できます。

手順

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、以下に示すコードが含まれており、これは任意の価格値をゼロに置き換えます。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。

新規ポリシー文書の追加または既存の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、新規ポリシー文書を追加したり、既存のポリシー文書を編集したりできます。

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、89 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、105 ページの『新規メディエーション・ポリシーのオーサリング』を参照してください。
2. 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、108 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。
3. ポリシーを添付します。Business Space で、ポリシーを添付する SLD または SLA を探します。サンプルには、これを行う 4 つの場所があります。

- Store SLD - Store サービスの使用に適用するポリシーを添付します。
- Gold SLA - CEO コンシューマーからの Gold 要求にのみ適用するポリシーを添付します。
- Silver SLA - CEO コンシューマーからの Silver 要求にのみ適用するポリシーを添付します。
- Anonymous SLA - CEO 以外のコンシューマーからの要求に適用するポリシーを添付します。

関連タスク:

105 ページの『新規メディエーション・ポリシーのオーサリング』
Business Space ユーザー・インターフェースを使用して、新規メディエーション・ポリシーを作成できます。メディエーション・ポリシーを作成する場合、ポリシーの条件とアクションを指定します。

108 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。ポリシーは、DataPower によって適用できるように承認状態になっている必要があります。

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 4 つのサポート用ゲートウェイがあり、サポート用ゲートウェイは、Store Gateway が呼び出すサンプル・バックエンド、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を提供します。

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、 63 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。認証では以下のアクションが実行されます。
   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 (例えば LTPA を使用せず) 基本認証のみを使用して呼び出せるポートを備えたフロントエンドを提供することです。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. 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、ルーティング・ポリシーの実施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 で保護して 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、以下のタスクを実行します。

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発生し、クライアントに拒否応答を返します。

注: 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。このサンプルでは、2 つのタイプのリソースが使用されます。1

つ目のタイプは Web サービスにおける操作であり、2 つ目のタイプは応答のデータ (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確認できます。 findInventory 操作はこれら 3 つのグループのすべてでの使用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わかります。

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、以下の点に注目してください。

1. storeSendToPDP.xsl スタイル・シートが組み込まれています。このスタイル・シートには storeXAMLFW を呼び出すロジックが含まれています。
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 の構造である storePrivateDataXACML.xml は、StoreWSP シナリオで使用される構造とほぼ同じです。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 14. 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。これは、Store サービスを所有するビジネス・エリアです。
ビジネス・ケイパビリティー	ウェアハウス。これは、すべてのバージョンの Store サービスを表し、Bob's Warehouse がこれを所有します。
サービスのバージョン	Store。これは、Store サービスのバージョン 1.0 を表します。
WSDL	Store.wsdl
XSD	Company.xsd
ポリシー	• Validate.xml • RouteForGold.xml • LogEveryTime.xml • RejectAfter5MsgIn90Seconds.xml
SLD	Store SLD。ここで添付されるポリシーはどれも、このサービスへのすべての要求に適用されます。
Gold SLA	Gold SLA。この SLA が存在するということは、コンシューマー CEO からの Gold 要求が匿名とはみなされないことを意味します。ここで添付されるポリシーはどれも、コンシューマー CEO からの Gold 要求に実施されます。
Silver SLA	Silver SLA。この SLA が存在するということは、コンシューマー CEO からの Silver 要求が匿名とはみなされないことを意味します。添付されるポリシーはなく、要求は通過を許可されます。
匿名 SLA	匿名ユーザー。ここで添付されるポリシーは、実施中の SLA に一致しないどの要求にも実施されます。このサンプルでは、CEO 以外のコンシューマーからの要求、および、CEO からの要求であっても Gold でも Silver でもない要求には、匿名 SLA ポリシーが実施されます。

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 15. 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 の基本認証と 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、または、IBM HTTP Server が存在した ND 環境の場合は CMSKeyStore デフォルト証明書から抽出したものです。

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。この妥当性検査は、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 16. 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 16. 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 17. 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。

表 17. XSL スタイル・シートを使用する DataPower オブジェクト (続き)

スタイル・シート	目的
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 のいずれかがデプロイされた後、ワークロード・コンソールで「**インスタンス (Instances)**」 > 「**仮想システム (Virtual systems)**」をクリックすることにより、デプロイ済みのインスタンスを表示できます。

インスタンスの詳細の表示

デプロイ済みの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 (Virtual System Instances)」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が表示されます。この詳細には、そのデプロイメントのためにクラウド・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、および仮想マシンの状況が含まれます。

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。スクリプト・ログは、「**スクリプト・パッケージ (Script Packages)**」セクションで表示できます。どのコンソールにも、「**コンソール (Consoles)**」セクションのリンクを使用して接続できます。

デプロイ済みのインスタンスへのアクセス

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して、IBM SOA Policy Gateway Pattern 環境を把握し、そのコンポーネント部品にアクセスできます。

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。以下が含まれます。
   - WebSphere Application Server 管理コンソール
   - WSRR Web UI
   - WSRR Business Space
   - DataPower WebGUI

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、WSRR との作業を実行します。

このタスクについて

Business Space は、WSRR との作業に使用できる、2 つのグラフィカル・インターフェースの 1 つです。Business Space を WSRR とともに使用するための詳細な情報については、WSRR インフォメーション・センター (関連するリンクを参照) にあります。

デプロイ済みのパターンにある WSRR インスタンスの Business Space への接続は、ワークロード・コンソールのリンクをクリックするか、Web ブラウザーに URL を入力することによって行うことができます。

手順

1. ワークロード・コンソールから接続する方法
   a. 「**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。
   b. 「仮想システム・インスタンス (Virtual System Instances)」ウィンドウのインスタンスのリストから、デプロイ済みのシステムを選択します。
   c. デプロイ済みのシステムの詳細ビューで「**仮想マシン (Virtual machines)**」をクリックして、リストを展開します。
   d. 仮想マシンのリストで WSRR を見つけて、正符号をクリックして詳細情報を表示します。
   e. 「**コンソール (Consoles)**」セクションで、「**WSRR_Business_Space**」をクリックします。
   f. WSRR 管理ユーザー ID とパスワードを入力します。
2. Web ブラウザーから接続する方法

a. Web ブラウザーを開きます。
b. WSRR のホスト名とポート番号を確認します。ステップ 1 の説明に従って、デプロイメントの詳細情報を表示します。「**仮想マシン (Virtual machines)**」セクションを展開して、WSRR サーバーの仮想マシンを選択して、仮想マシンの詳細情報を表示します。「**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。
c. WSRR Web UI URL: http://*hostname*:9443/BusinessSpace を入力します。ここで、*hostname* は WSRR サーバーのホスト名です。
d. WSRR 管理ユーザー ID とパスワードを入力します。

タスクの結果

Business Space が表示されます。これを使用してメディエーション・ポリシーと他の WSRR 成果物を追加、編集、または削除できます。

次のタスク

WSRR システムにおける Business Space の初回使用時には、『初回使用時の Business Space の構成』を参照し、SOA ガバナンス・スペースの作成手順に従ってください。

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

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、88 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・スペースがまだ存在しない場合は、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

以下のようにして、「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。

WSRR への接続 - WSRR Web UI

WSRR Web UI を使用して、WSRR との作業を行います。

このタスクについて

WSRR Web UI は、WSRR との作業に使用できる、2 つのグラフィカル・インターフェースの 1 つです。WSRR Web UI の使用に関する詳細情報については、WSRR インフォメーション・センター (関連するリンクを参照) にあります。ほとんどの場合、Business Space インターフェースが使用されますが、WSRR Web UI で実行しなければならないタスク (モニター・ポリシーの作成など) もあります。

デプロイ済みのパターンにある WSRR インスタンスの WSRR Web UI への接続は、ワークロード・コンソールのリンクをクリックするか、Web ブラウザーに URL を入力することによって行うことができます。

手順

1. ワークロード・コンソールから接続する方法
   a. 「**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。
   b. 「仮想システム・インスタンス (Virtual System Instances)」ウィンドウのインスタンスのリストから、デプロイ済みのシステムを選択します。
   c. デプロイ済みのシステムの詳細ビューで「**仮想マシン (Virtual machines)**」をクリックして、リストを展開します。
   d. 仮想マシンのリストで WSRR を見つけて、正符号をクリックして詳細情報を表示します。
   e. 「**コンソール (Consoles)**」セクションで、「**WSRR_Web_UI**」をクリックします。
   f. WSRR 管理ユーザー ID とパスワードを入力します。
2. Web ブラウザーから接続する方法
   a. Web ブラウザーを開きます。
   b. WSRR のホスト名とポート番号を確認します。ステップ 1 の説明に従って、デプロイメントの詳細情報を表示します。「**仮想マシン (Virtual machines)**」セクションを展開して、WSRR サーバーの仮想マシンを選択して、仮想マシンの詳細情報を表示します。「**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。
   c. WSRR Web UI URL: http://*hostname*:9443/ServiceRegistry を入力します。ここで、*hostname* は WSRR サーバーのホスト名です。
   d. WSRR 管理ユーザー ID とパスワードを入力します。

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

WebSphere Application Server 管理コンソールへの接続

WebSphere Application Server 管理コンソールを使用して、セキュリティー設定を調整して、他の管理タスクを実行します。

このタスクについて

WebSphere Application Server 管理コンソールでの作業に関する詳細情報は、インフォメーション・センターにあります。関連するリンクを参照してください。

デプロイ済みのパターンの WebSphere Application Server 管理コンソールへの接続は、ワークロード・コンソールのリンクをクリックするか、Web ブラウザーに URL を入力することによって行えます。

手順

1. ワークロード・コンソールから接続する方法
   a. 「**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。

b. 「仮想システム・インスタンス (Virtual System Instances)」ウィンドウのインスタンスのリストから、デプロイ済みのシステムを選択します。

c. デプロイ済みのシステムの詳細ビューで「**仮想マシン (Virtual machines)**」をクリックして、リストを展開します。

d. 仮想マシンのリストで WSRR を見つけて、正符号をクリックして詳細情報を表示します。

e. 「**コンソール (Consoles)**」セクションで、「**WebSphere**」をクリックします。

f. WSRR 管理ユーザー ID とパスワードを入力します。

2. Web ブラウザーから接続する方法

a. Web ブラウザーを開きます。

b. WSRR のホスト名とポート番号を確認します。ステップ 1 の説明に従って、デプロイメントの詳細情報を表示します。「**仮想マシン (Virtual machines)**」セクションを展開して、WSRR サーバーの仮想マシンを選択して、仮想マシンの詳細情報を表示します。「**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。

c. WSRR Web UI URL: http://*hostname*:9043/ibm/console を入力します。ここで、*hostname* は WSRR サーバーのホスト名です。

d. WSRR 管理ユーザー ID とパスワードを入力します。

関連情報:

WebSphere Application Server V8.0 インフォメーション・センター

仮想 DataPower のコンソールへの接続

DataPower コンソールを使用して、ポリシー実施ポイントを構成します。

このタスクについて

ゲートウェイの構成に関する詳細情報は、WebSphere DataPower インフォメーション・センターにあります。関連するリンクを参照してください。

Web ブラウザーを使用してコンソールに接続します。ワークロード・コンソールのデプロイ済みパターンの詳細を表示することによって、接続の詳細情報を入手します。

手順

1. 以下に示すようにワークロード・コンソールを使用することによって、必要な詳細情報を入手します。

a. 「**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。

b. 「仮想システム・インスタンス (Virtual System Instances)」ウィンドウのインスタンスのリストから、デプロイ済みのシステムを選択します。

c. 詳細ビューで、「**仮想マシン (Virtual machines)**」セクションを展開し、DataPower アプライアンス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。

2. Web ブラウザーを開いて、URL `https://hostname:9090/dp` を入力します。ここで、*hostname* は仮想アプライアンスのホスト名です。

関連情報:

WebSphere DataPower V6.0 インフォメーション・センター

モニター・コンソールへの接続

モニター・コンソールを使用して、モニター情報を表示します。

このタスクについて

「仮想システム・インスタンス (Virtual System Instances)」ウィンドウからモニター・コンソールにアクセスします。

モニター機能は、ITCAM for SOA によって提供されます。詳細な情報については関連リンクから資料をダウンロードして、DataPower のインストールに関する情報を検索します。

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. 「**仮想マシン (Virtual machines)**」セクションを展開して、モニター対象の仮想マシンを選択します。
4. 「**一般情報 (General information)**」で、「**モニター (Monitoring)**」を探し、「**クリックして開く (Click to open)**」リンクをクリックします。

関連情報:

ITCAM for SOA 7.2.1 資料 (Fix Central 提供)

デプロイ済みのインスタンスの停止および開始

デプロイ済みのインスタンスをワークロード・コンソールから停止および開始できます。パターンで個々の仮想マシンを停止および開始することもできます。

実行中のデプロイ済みインスタンスを停止する方法

1. 「**インスタンス (Instances)**」 > 「**仮想システム (Virtual Systems)**」を選択して、「**仮想システム・インスタンス (Virtual System Instances)**」リストからインスタンスを選択します。
2. インスタンスのタイトル・バーで「**停止 (Stop)**」アイコンをクリックします。

停止しているデプロイ済みインスタンスの開始方法

1. 「**インスタンス (Instances)**」 > 「**仮想システム (Virtual Systems)**」を選択して、「**仮想システム・インスタンス (Virtual System Instances)**」リストからインスタンスを選択します。
2. インスタンスのタイトル・バーで「**開始 (Start)**」アイコンをクリックします。

注: DB2 10.1.0.2 では、インスタンスを停止してから再始動する場合に、DB2 プロセスが再始動しない場合があるという既知の問題があります。この場合、DB2 ノードに db2inst1 としてログインし、**db2start** を実行することによって、DB2 プロセスを手動で始動する必要があります。さらに、WSRR ノードで WSRR プロセスを再始動しなければならない場合もあります。

個々の仮想マシンを停止する方法

1. インスタンス・ビューの「**仮想計算機 (Virtual Machines)**」セクションを展開します。
2. 停止するマシンの「**管理 (Manage)**」リンクを選択します。
3. 管理バーの停止アイコンをクリックします。

個々の仮想マシンを開始する方法

1. インスタンス・ビューの「**仮想計算機 (Virtual Machines)**」セクションを展開します。
2. 開始するマシンの「**管理 (Manage)**」リンクを選択します。
3. 管理バーの開始アイコンをクリックします。

コマンド行から、WSRR と DB2 を停止および開始することもできます。SSH コンソールを使用して、「**ログイン (Login)**」リンクをクリックして接続します。

WebSphere Application Server プロファイルを停止および開始することによって、WSRR を停止および開始します。WebSphere Application Server インフォメーション・センターのコマンドを使用したプロファイルの管理を参照してください。

Advanced パターンでは、DMGR およびカスタム・ノードの再始動後に、WSRR クラスターを開始する必要があります。これを行うには、WebSphere Application Server 管理コンソールを開き、「**サーバー (Servers)**」 > 「**クラスター (Clusters)**」 > 「**WebSphere Application Server クラスター (WebSphere Application Server Clusters)**」を選択します。「**WSRRCluster_1**」を選択して、「**開始 (Start)**」をクリックします。

システム・コマンドを使用して、DB2 を停止および開始することができます。DB2 インフォメーション・センターのシステム・コマンドを参照してください。

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。

ポリシー実施ポイントの構成

DataPower アプライアンスまたはインスタンスは、IBM SOA Policy Gateway Pattern のポリシー実施ポイント (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

構成設定の段階で、各 DataPower アプライアンスに異なるドメイン・ネームが使用されていることを確認します。そうでない場合、SOA トポロジー・ワークスペースの ITCAM に正しいデータが表示されません。
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事前に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、使用される識別には 2 つの形式があります。StoreAddLTPA XML ファイアウォールでは、識別は基本認証を使用しました。 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、 75 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。

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

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

表 18. 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、ユーザー名、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。
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。

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。

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。(このトピックは外部 DataPower アプライアンスに適用されます。)

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 との間で機能する固有の証明書は、IBM SOA Policy Gateway Pattern で使用される「SOA Policy Gateway 2.5.0.0 - Security」スクリプト・パッケージや「SOA Policy Gateway 2.5.0.0 - 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。

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。このトピックは、外部 DataPower アプライアンスを持つデプロイ済みのパターンに適用されます。

このタスクについて

DataPower 証明書は、WSRR と DataPower の間でのポリシー更新のための同期更新を単純化するために WSRR トラストストアにアップロードされます。この機能が必要ない場合、DataPower 証明書を削除できます。証明書を変更する必要がある場合、新規 DataPower 証明書を追加することもできます。

手順

1. 証明書を削除する方法:
   a. `https://`*`hostname`*`:9043/ibm/console` で、WebSphere Application Server 管理コンソールにログインします。ここで、*hostname* は WSRR システムのホスト名です。管理ユーザー名とパスワードを入力してください。
   b. 「**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。

c. 「**鍵ストアと証明書 (Key Stores and Certificates)**」をクリックします。

d. デプロイメントが Basic Runtime パターンに基づいている場合は「**NodeDefaultTrustStore**」を、Advanced Runtime パターンをデプロイした場合は「**CellDefaultTruststore**」をクリックします。

e. 「**署名者証明書 (Signer Certificates)**」をクリックします。

f. 削除する証明書のチェック・ボックスを選択にします。

g. 「**削除 (Delete)**」 をクリックします。

h. 「**保存 (Save)**」をクリックします。

2. 新しい DataPower 証明書を追加するには、「**追加 (Add)** 」をクリックして、新しい証明書を追加します。

a. `https://`*`hostname`*`:9043/ibm/console` で、WebSphere Application Server 管理コンソールにログインします。ここで、*hostname* は WSRR システムのホスト名です。管理ユーザー名とパスワードを入力してください。

b. 「**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。

c. 「**鍵ストアと証明書 (Key Stores and Certificates)**」をクリックします。

d. デプロイメントが Basic Runtime パターンに基づいている場合は「**NodeDefaultTrustStore**」を、Advanced Runtime パターンをデプロイした場合は「**CellDefaultTruststore**」をクリックします。

e. 「**署名者証明書 (Signer Certificates)**」をクリックします。

f. 「**追加 (Add)**」をクリックして、新規証明書を指定します。

g. 「**保存 (Save)**」をクリックします。

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、パターン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、ステージングまたは実動などのランタイム環境にインポートされます。

このタスクについて

WebSphere Application Server 管理コンソールでこれらのアクションを実行します。詳細については、関連リンクを参照してください。

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. Runtime インスタンスが Advanced Runtime パターンに基づいている場合、以下のステップを順番に実行します。

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. WSRR システムが Advanced Runtime パターンに基づいている場合、逆順に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 (Basic Runtime パターンに基づく)、LTPA 鍵の変更を有効にするためにサーバーを停止して再始動する必要があります。

関連情報:


WebSphere Application Server V8.0 インフォメーション・センター

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・スペースが存在しない場合は、 89 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:

88 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、WSRR との作業を実行します。

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、105 ページの『新規メディエーション・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件を指定して、サービスに期待されるサービスの品質を指定します。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、要件を満たす場合に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す。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できますが、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す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、ビジネスでは「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を指定すると、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、その結果、指定されたどのアクションも実施されます。

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。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 という形式で指定します。「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。 (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。)

- **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 という形式で指定します。「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 という形式で指定します。 (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 という形式で指定します。「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 時をまたぐ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 つのパラメーターと、オプションの「Interval」および「Limit」のパラメーターで構成されます。「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 19. 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。

表 19. 定義される属性 (続き)

属性	説明とタイプ
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 20. 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。 (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。 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 21. 「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。

新規メディエーション・ポリシーのオーサリング

Business Space ユーザー・インターフェースを使用して、新規メディエーション・ポリシーを作成できます。メディエーション・ポリシーを作成する場合、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、88 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・スペースが存在しない場合は、 89 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。

さらに、Business Space を構成して、アクション・ウィジェットから WS-MediationPolicy 1.7 メディエーション・ポリシーを作成する必要もあります。「サービス・レジストリー・アクション」ウィジェットを参照してください。

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、 99 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。作成したポリシーのポリシー文書を表示するには、「サービス・レジストリー・ナビゲーター」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:

99 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

新規モニター・ポリシーのオーサリング

WSRR Web UI を使用して、新規モニター・ポリシーを作成できます。モニター・ポリシーを作成する場合、ポリシーの条件とアクションを指定します。

始める前に

WSRR Web UI のアクセスについては、 90 ページの『WSRR への接続 - WSRR Web UI』を参照してください。

手順

1. WSRR Web UI を開きます。
2. 「**ビュー (View)**」 > 「**サービス文書 (Service Documents)**」 > 「**ポリシー文書 (Policy Documents)**」をクリックして、コレクション・ビューで「**新規 (New)**」をクリックします。
3. 使用可能な Policy Framework のリストから、「**モニター (Monitoring)**」を選択します。「**次へ (Next)**」をクリックします。これによってルートのポリシー式を含むポリシー文書が作成されます。
4. 意味のある名前とオプションの説明を入力します。
5. 「ポリシー (Policy)」タブをクリックして、「**ポリシー文書の編集 (Edit policy document)**」をクリックし、必要な条件とアクションを追加します。 条件とアクションの詳細については、関連したリンクを参照してください。
6. 「**公開 (Publish)**」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。 Business Space でポリシーのポリシー文書を表示して、「サービス・レジストリー・ナビゲーター」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:

99 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:

ポリシー・オーサリング・タスク

ポリシー・オーサリング・ツールでの作業

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、 89 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、『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。ポリシーは、DataPower によって適用できるように承認状態になっている必要があります。

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、「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、「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』
ポリシーは SOA Policy ライフサイクルによって制御されます。このライフサイクルとは、ポリシーが最初に識別された時点から、ポリシーが実動環境にデプロイされ、最終的に不要になって非推奨になる時点までです。

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

IBM SOA Policy Gateway Pattern でパターンをデプロイする場合に発生する一般的な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外部 DataPower アプライアンスへの接続失敗

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、Web GUI 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。

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 にログインして、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。

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多くの問題が発生する場合があります。

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 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。

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 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。

モニターに関する問題

デプロイ済みのノードでモニターが使用できない場合、必要な共用サービスが実行されていることを確認する必要があります。「**インスタンス (Instances)**」 > 「**共用サービス (Shared Services)**」とナビゲートします。

システム・モニターおよび WebSphere DataPower のシステム・モニターが、デプロイ済みのインスタンスと同じクラウド・グループ内で実行されていることを確認します。 WSRR モニターの場合、クラウド・グループ内で WebSphere Application Server のシステム・モニターが実行されていることも確認します。

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。
4. モニターの問題の場合は、基本 OS ノードおよび WSRR ノード (WSRR カスタム・ノードは除く) から以下のログを収集します。
   - `/0config/0config.log`
   - `/opt/IBM/maestro/ITCAMSOADP/lx8266/d4/KD4/logs/*` (x86)
   - `/opt/IBM/maestro/ITCAMSOADP/aix523/d4/KD4/logs/*` (Power)

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

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。

注: 緊急フィックスをインストールする前に、すべての WSRR および WAS プロセスをシャットダウンする必要があります。SSH を使用してすべての WSRR ノードにログインして、**stopServer.sh** コマンドと **stopNode.sh** (カスタム・ノードのみ) コマンドを使用して、プロセスをシャットダウンします。

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 (提供される場合) 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 Corporation の商標です。これらおよび他の IBM 商標に、この情報の最初に現れる個所で商標表示 (® または ™) が付されている場合、これらの表示は、この情報が公開された時点で、米国において、IBM が所有する登録商標またはコモン・ロー上の商標であることを示しています。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、www.ibm.com/legal/copytrade.shtml をご覧ください。

ご意見をお寄せください

本書に関してご感想やご要望がありましたら、以下のいずれかの方法で IBM にお送りください。

具体的な誤りや抜けと思われる箇所、あるいは本書の正確性、構成、題材、または完成度について、お気軽にご意見をお寄せください。

ただし、お寄せいただくご意見は、本書の情報とその提供のあり方に関するもののみに限らせていただきます。

IBM の製品またはシステムの機能に関するご意見は、IBM の担当員または IBM に認可された再販業者にご連絡ください。

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。

ご意見は、以下のいずれかの方法で IBM にお送りください。

- 郵送の場合は、以下の住所にお送りください。

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

- FAX の場合:
  - 英国の国外の場合は、国際アクセス・コードの後に 44-1962-816151 とダイヤルしてください。
  - 英国の国内の場合は、01962-816151 とダイヤルしてください。
- 電子送信の場合は、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: IBMMAIL、GBIBM2Q9
  - IBMLink: HURSLEY(IDRCF)
  - インターネット: idrcf@hursley.ibm.com

いずれの方法の場合も、以下を記載してください。

- 資料名と資料番号
- ご意見に関連するトピック
- 氏名および住所/電話番号/FAX 番号/ネットワーク ID