IBM SOA Policy Gateway Pattern

Inhaltsverzeichnis

Kapitel 1. SOA Policy - Übersicht

Das Richtlinienmanagement spielt eine entscheidende Rolle bei einer strukturierten und konsistenten Regelung von Richtlinien (Governance). Richtlinien können zur Einrichtung einer besseren Governance in einer beliebigen serviceorientierten Umgebung verwendet werden.

Eine Richtlinie ist ein unabhängiges Element, das auf eine oder mehrere Ressourcen, einschließlich verschiedener Services, angewendet werden kann. Die Zuordnung der Richtlinie und zugehöriger Metadaten kann insbesondere in einer verteilten Umgebung an ganz verschiedenen Durchsetzungspunkten und Entscheidungspunkten stattfinden.

SOA Policy-Architektur

Die SOA Policy-Architektur beschreibt die Interaktionen zwischen dem Richtlinienverwaltungspunkt (PAP), dem Richtliniendurchsetzungspunkt (PEP), dem Richtlinienentscheidungspunkt (PDP), dem Richtlinieninformationspunkt (PIP) und dem Richtlinienüberwachungspunkt (PMP). Im Muster wird der PAP von WSRR, der PEP wird von WebSphere DataPower und der PMP von der DataPower-Überwachungskomponente bereitgestellt.

Die grundlegende Richtlinienarchitektur ist wie folgt aufgebaut:

- **Richtlinienverwaltungspunkt**. Ein Richtlinienverwaltungspunkt (PAP, Policy Administration Point) stellt Richtlinienfunktionen für das Verfassen (Authoring) einer Richtlinie, die Verwaltung und Governance der Richtlinie und die Zuordnung der Richtlinie zu Ressourcen sowie die Verwaltung der Richtlinienergebnisse während der Laufzeit bereit. Der PAP enthält ein Repository zum Speichern von Richtlinien. Der PAP wird von WSRR bereitgestellt.
- **Richtliniendurchsetzungspunkt**. Ein Richtliniendurchsetzungspunkt (PEP, Policy Enforcement Point) ist ein Funktionspunkt, der auf der Middleware ausgeführt wird. Er führt folgende Aufgaben durch:
  - Empfangen von Richtlinien.
  - Empfangen von Aktualisierungen für Durchsetzungsrichtlinien und Vorbereiten bzw. Übersetzen dieser Aktualisierungen für die Verwendung.
  - Bereitstellen von Durchsetzungsmesswerten für den Richtlinienüberwachungspunkt.
  - Bereitstellen von Ergebnis- und Analysedaten von Durchsetzungsrichtlinien für den Richtlinienverwaltungspunkt und die Richtlinienüberwachungspunkte.
  - Ändern der Positionen, an denen Richtlinien angewendet und durchgesetzt werden, abhängig von der Lebenszyklusphase:
    - Während der Entwicklungszeit ist WSRR selbst der Durchsetzungspunkt.
    - Während der Ausführungszeit werden Richtlinien in der Regel vom zugrunde liegenden Vermittlersystem (Middleware) durchgesetzt, das Service-Provider mit Konsumenten verbindet.

  In diesem Muster wird der PEP von WebSphere DataPower bereitgestellt.
- **Richtlinienentscheidungspunkt**. Ein Richtlinienentscheidungspunkt (PDP, Policy Decision Point) wertet teilnehmende Anforderungen anhand der relevanten

Richtlinien oder anhand von Verträgen und Attributen aus. Der PDP gibt eine Autorisierungs-, Berechtigungs- oder Prüfungsentscheidung zurück, um berechnete Ergebnisse bereitzustellen.

- **Richtlinieninformationspunkt**. Ein Richtlinieninformationspunkt (PIP, Policy Information Point) stellt externe Informationen für den Richtlinienentscheidungspunkt bereit, wie zum Beispiel Informationen zu LDAP-Attributen oder die Ergebnisse aus einer Datenbank mit Informationen, die ausgewertet werden müssen, um eine Richtlinienentscheidung zu treffen.
- **Richtlinienüberwachungspunkt**. Ein Richtlinienüberwachungspunkt (PMP, Policy Monitoring Point) ist eine Funktionskomponente, die die detaillierte Richtlinienüberwachungsfunktion für die Gesamtarchitektur bereitstellt, wie zum Beispiel die Übersicht über die Richtlinie in der verteilten Umgebung. Er führt folgende Aufgaben durch:
  - Empfangen von Aktualisierungen für Überwachungsrichtlinien und Vorbereiten bzw. Übersetzen dieser Aktualisierungen für die Verwendung.
  - Erfassen der Echtzeitdaten und statistische Analyse für die Anzeige.
  - Korrelieren, Analysieren und Visualisieren der Daten, die von den verschiedenen Echtzeitkollektoren, einschließlich der Richtliniendurchsetzungspunkte, zugeführt werden.
  - Eine Managementkonsole, die eine Anzeige des Managements des verteilten Netzes von Richtliniendurchsetzungspunkten und des Status dieser Durchsetzungen bereitstellt.
  - Protokollieren, Aggregieren von Messwerten und Hervorheben signifikanter Ereignisse wie in der Überwachungsrichtlinie angegeben.
  - Bereitstellen von Überwachungsrichtlinienanalysen für den Richtlinienverwaltungspunkt (PAP) und die Richtliniendurchsetzungspunkte.

  In diesem Muster wird der PMP von der DataPower-Überwachungskomponente bereitgestellt.

Der Konsument und der Provider interagieren beide mit der Middleware, die wiederum mit dem Repository und der Überwachungssoftware interagiert.

Funktionsweise der SOA-Richtlinienarchitektur

Der SOA Policy-Musterablauf wird in Abb. 1 auf Seite 3 dargestellt.

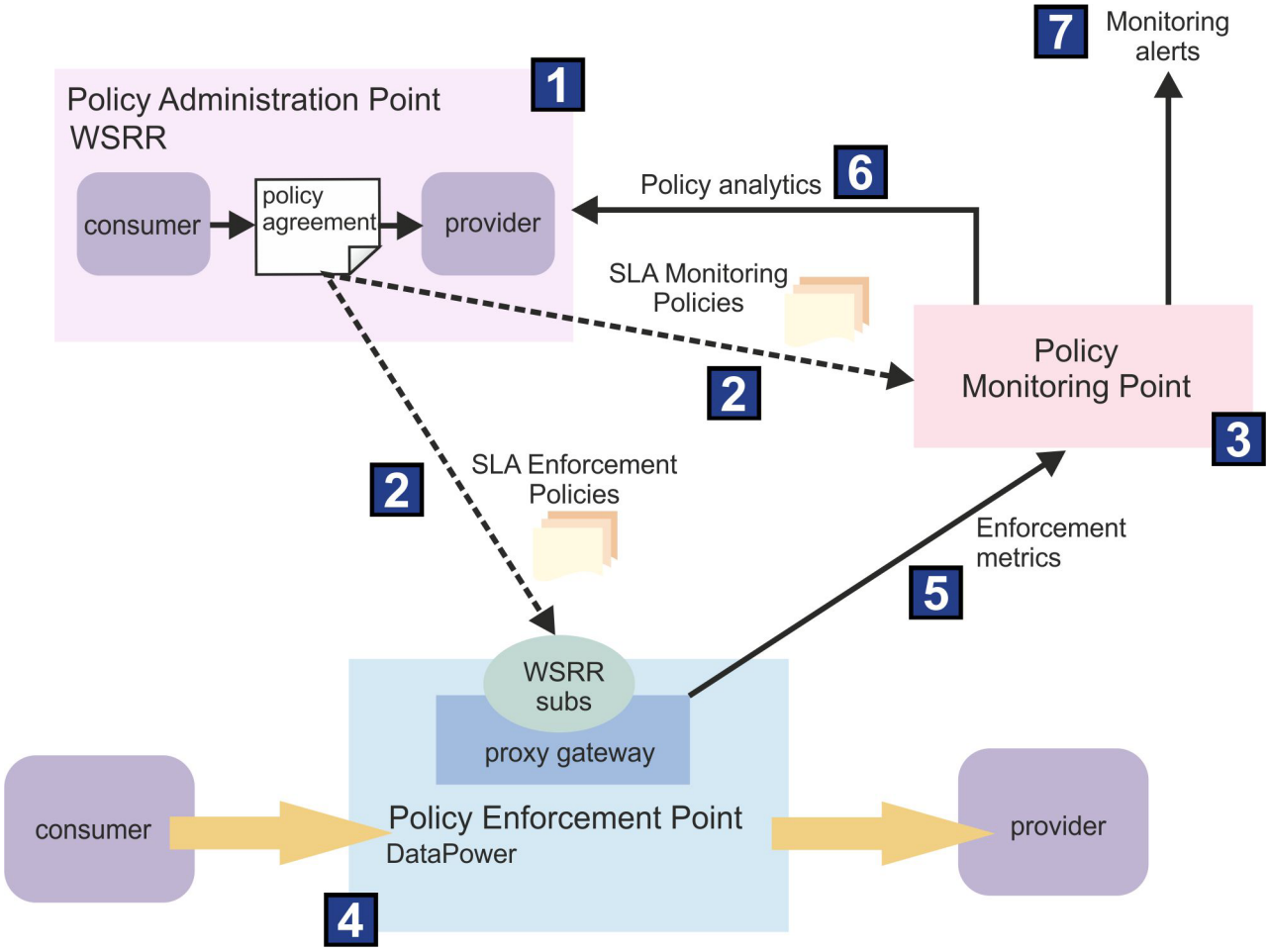


Abbildung 1. Service Level Agreement-Richtlinie (SLA-Richtlinie) - SOA-Implementierungsmodell

1 Richtlinien werden erstellt und anschließend den Services zugeordnet, für die die Richtlinie erforderlich ist. In der Regel geschieht dies in der folgenden Reihenfolge:

1. Die Gruppe von Services wird in das Service-Repository geladen oder dort erstellt. Diese Aktion ist Teil des Richtlinienverwaltungspunkts.
2. Die Gruppe der erforderlichen Richtlinien wird im Richtlinienverwaltungspunkt unter Verwendung des Richtlinienlebenszyklus erstellt:
   - Richtlinien werden den Services zugeordnet, die diese Richtlinien erfordern - je nach Bedarf auf Service-, Operations- oder Endpunktebene.

2 Automatisierte Veröffentlichung/Subskription von Richtlinien vom Richtlinienverwaltungspunkt (PAP) zu den Richtliniendurchsetzungspunkten und dem Richtlinienüberwachungspunkt:

1. Im Rahmen der Konfiguration subskribiert der Monitoring Service die Überwachungsrichtlinie in WSRR. Diese Aktion erfolgt nur einmal.
2. Im Rahmen der Konfiguration werden Proxy-Gateways in jedem WebSphere DataPower-Gerät (oder virtuellem Gerät) erstellt, das Servicetransaktionen mit Richtliniendurchsetzung hat. Diese Aktion erfolgt nur einmal und wird nach Bedarf hinzugefügt oder geändert.

3. Im Rahmen der Konfiguration subskribiert jedes Proxy-Gateway im Gerät Richtlinien in WSRR für Services, für die es zuständig ist. Diese Aktion erfolgt nur einmal und wird nach Bedarf hinzugefügt oder geändert.
4. Im Rahmen der Konfiguration wird WebSphere DataPower so konfiguriert, dass Richtlinien von anderen Geräten in einem Cluster gemeinsam genutzt werden können. Diese Aktion erfolgt nur einmal und wird nach Bedarf hinzugefügt oder geändert.
5. Der Richtlinienüberwachungspunkt lädt die Überwachungsrichtlinien herunter, wenn sie veröffentlicht werden.
6. Der Richtlinienüberwachungspunkt konvertiert die Richtlinien in die interne Darstellung, die als Situationsrichtlinien bezeichnet werden.
7. WebSphere DataPower lädt die WSDLs für Services herunter, für deren Transaktionen es zuständig ist.
8. WebSphere DataPower lädt die Richtlinien für Services herunter, für die es zuständig ist, wenn es von WSRR benachrichtigt wird.
9. WebSphere DataPower konvertiert die Richtlinien in die interne WebSphere DataPower-Darstellung in Form von SLM-Objekten.


Überwachung von SOA-Richtlinien mit Berichten zu Operationen und Benachrichtigungen über Operationen:

1. Überwachungsrichtlinien sind in der Richtlinienüberwachungspunkt-Situationsrichtlinie aktiv.
2. Der Richtlinienüberwachungspunkt empfängt Überwachungsdaten und fügt diese Daten in Arbeitsbereiche ein.


Durchsetzung von SOA-Richtlinien:

1. Durchsetzungsrichtlinien sind in den verschiedenen WebSphere DataPower-Geräten aktiv.
2. WebSphere DataPower empfängt Servicetransaktionen und wendet Richtlinien für den jeweiligen Konsumentenservice und Provider-Service an.


Der Richtliniendurchsetzungspunkt sendet Statistikdaten zur SOA-Richtliniendurchsetzung an den Richtlinienüberwachungspunkt.


Der Richtlinienüberwachungspunkt sendet Überwachungsereignisse an den Richtlinienverwaltungspunkt:

1. Ereignisse werden im Richtlinienverwaltungspunkt konfiguriert, die vom Richtlinienüberwachungspunkt aus überwacht werden müssen. Diese Aktion erfolgt nur einmal und wird nach Bedarf hinzugefügt oder geändert.
2. Wenn Situationsrichtlinien als wahr ausgewertet werden, werden Ereignisse vom Richtlinienüberwachungspunkt an den Richtlinienerstellungspunkt übertragen.


Überwachung von Alerts:

- Situationsrichtlinien werden in regelmäßigen Abständen ausgeführt und führen operative Aktionen durch, wie dies in der Richtlinie angegeben ist. Das Standardintervall beträgt fünf Minuten.

SOA Policy-Lebenszyklus

Richtlinien werden durch den SOA Policy-Lebenszyklus geregelt. Der Lebenszyklus definiert die verschiedenen Phasen, in denen eine Richtlinie zu Anfang erkannt wird, später in einer Produktionsumgebung implementiert wird und schließlich außer Funktion gesetzt wird, wenn sie nicht mehr erforderlich ist.

Weitere Informationen zu den Übergängen und Zuständen im SOA Policy-Lebenszyklus finden Sie im Information Center von IBM® WebSphere Service Registry and Repository Version 8.0 - SOA-Richtlinienlebenszyklus.

Richtlinienstandards

Die technischen Web-Community-Gruppen W3C und OASIS haben Standards entwickelt, um die für Web-Services anwendbaren Richtlinien zu definieren.

- **WS-Policy**: Die Domäne 'Web Services Mediation Policy 1.0' definiert einen Satz von Richtlinienzusicherungen (Assertions) zur Beschreibung der Mediationsanforderungen für einen Service.
- **Web Services Policy 1.5 - Framework**: Definiert ein Framework und ein Modell für die Erstellung von Ausdrücken für Richtlinien, die sich auf domänenspezifische Funktionen, Anforderungen und allgemeine Merkmale von Entitäten in einem Web-Services-basierten System beziehen.

Beispiele von Spezifikationen, die domänenspezifische Richtlinienzusicherungen definieren:

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

Weitere Informationen zu WS-MediationPolicy finden Sie in ftp://public.dhe.ibm.com/software/solutions/soa/pdfs/WSMediationPolicy1.7-20130506.pdf.

Das WS-Policy-Datenmodell enthält folgende Entitäten:

- **Richtlinie (Policy)**: Eine nicht geordnete Sammlung von „Richtlinienalternativen".
- **Richtlinienalternative (Policy Alternative)**: Eine Richtlinienalternative ist eine Sammlung von „Richtlinienzusicherungen".
- **Richtlinienzusicherung (Policy Assertion)**: Stellt eine einzelne Vorgabe dar, zum Beispiel eine Anforderung oder eine Funktion.
- **Richtlinienparameter (Policy Parameters)**: Die nicht transparenten Nutzdaten einer „Richtlinienzusicherung".
- **Richtlinienbetreff (Policy Subject)**: Eine Entität, an die ein Richtlinienausdruck gebunden werden kann. Diese Entität wird in einem WS-PolicyAttachment-Dokument verwendet.

Das folgende Beispiel in Abb. 2 auf Seite 6 zeigt einen Sicherheitsrichtlinienausdruck mit Zusicherungen, die in WS-Security und

WS-SecurityPolicy definiert sind:

```
(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">  <!-- Richtlinienausdruck -->
(02)   <wsp:ExactlyOne>
(03)     <wsp:All>    <!-- Richtlinienalternative Nr. 1 -->
(04)       <sp:SignedParts>;   <!-- Richtlinienzusicherung -->
(05)         <sp:Body>   <!-- Parameter der Richtlinienzusicherung -->
(06)       </sp:SignedParts>
(07)     </wsp:All>
(08)     <wsp:All>    <!-- Richtlinienalternative Nr. 2 -->
(09)       <sp:EncryptedParts> <!-- Richtlinienzusicherung -->
(10)         <sp:Body/>   <!-- Parameter der Richtlinienzusicherung -->
(11)       </sp:EncryptedParts>
(12)     </wsp:All>
(13)   </wsp:ExactlyOne>
(14) </wsp:Policy>
```

Die Zeilen (03-07) stellen eine Richtlinienalternative für das Signieren eines Nachrichtenhauptteils dar.

Die Zeilen (08-12) stellen eine zweite Richtlinienalternative für das Verschlüsseln eines Nachrichtenhauptteils dar.

Die Zeilen (02-13) zeigen den Richtlinienoperator `ExactlyOne`. Richtlinienoperatoren fassen Richtlinienzusicherungen zu Richtlinienalternativen zusammen. Eine gültige Interpretation der Richtlinie ist zum Beispiel, dass ein Aufruf eines Web-Service den Nachrichtenhauptteil entweder signiert oder verschlüsselt, jedoch nicht beides.

Abbildung 2. Verwendung einer Web-Service-Richtlinie mit Sicherheitsrichtlinienzusicherungen

Abb. 3 zeigt eine Richtliniendefinition.

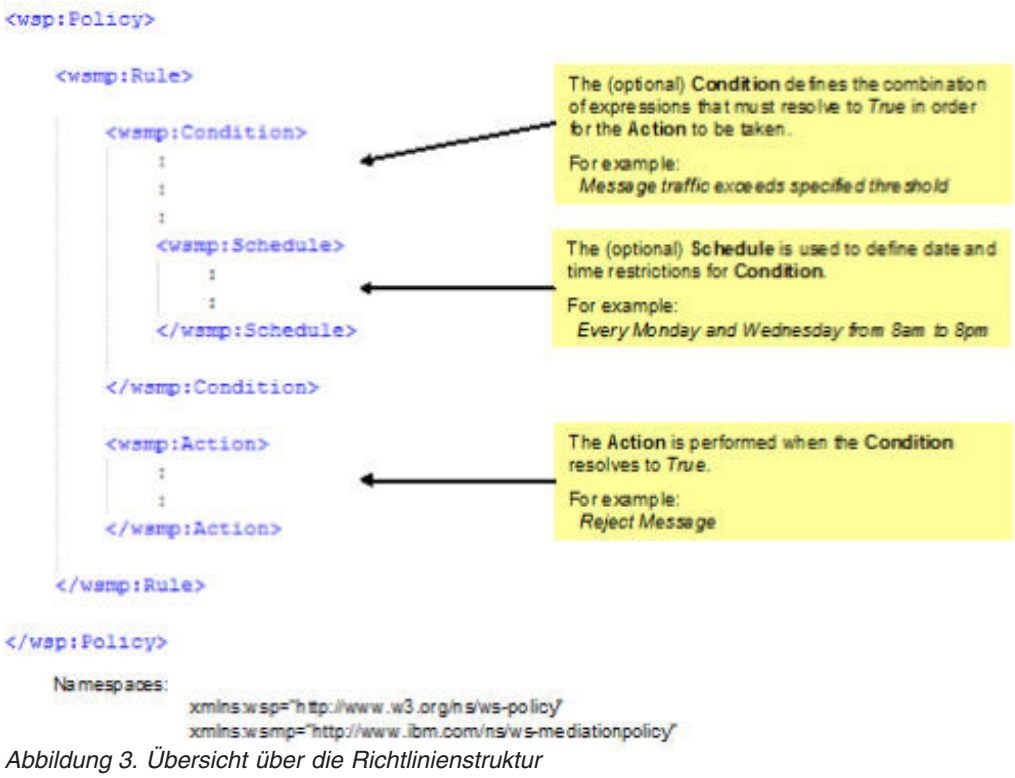


Abbildung 3. Übersicht über die Richtlinienstruktur

Richtlinienzuordnung

Das Richtlinienzuordnungsdokument (Policy Attachment Document) hat die Aufgabe, eine Gruppe von WS-Policy-Richtlinien einem bestimmten Servicezuordnungspunkt für die Durchsetzung, zum Beispiel einem Zuordnungspunkt für Web-Services, zuzuordnen.

Die Web-Services-Plattform kann zum Beispiel Zuordnungspunkte auf der Basis folgender Elemente unterstützen:

- Elemente, die WSDL Element URI 1.1 entsprechen
- WS-Addressing-Elemente

Die Syntax ist in der Spezifikation 'WS-PolicyAttachment' definiert:

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


    </wsp:AppliesTo>
    <wsp:Policy>


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

Abbildung 4. Spezifikation 'WS-PolicyAttachment'

WSRR stellt REST-Schnittstellen bereit, um die entsprechenden Richtlinienzuordnungen in einem SLA-Modell abzurufen. Informationen zu dem Konsumenten/Provider-Paar, für das die Richtlinie gilt, werden an den ESB im WS-PolicyAttachment-Format übergeben. Die Syntax ist in der Spezifikation 'WS-PolicyAttachment: Message Content Filters' definiert.

Die Richtlinie kann für einen Provider-Service allein, für ein bestimmtes Konsumenten/Provider-Paar oder für anonyme Konsumenten angegeben werden. Die Funktionalität für anonyme Konsumenten stellt eine Methode bereit, eine Standardrichtlinie zu definieren, die nur für Konsumenten gilt, für die keine anderen Richtlinien gelten.

In Abb. 4 ist der domänenspezifische Richtlinienbetreff ('subject'), für den die Richtlinie gilt (Provider), im Abschnitt `<wsp:AppliesTo>` enthalten, auf den der Konsumentenkontextfilter folgt, für den die Richtlinie gilt (Konsument). Im Abschnitt `<wsp:Policy>` wird anschließend die Richtlinie (bzw. die Richtlinien) deklariert oder referenziert.

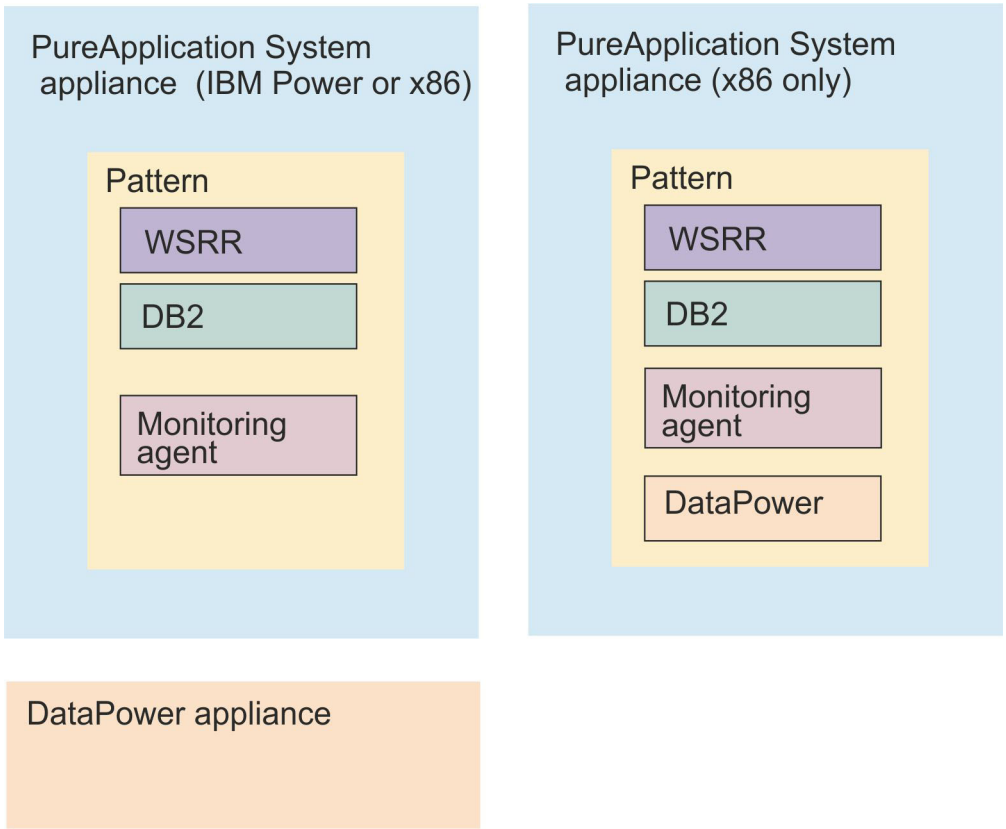
Kapitel 2. Muster - Übersicht

IBM SOA Policy Gateway Pattern besteht aus einem Satz von Mustern für virtuelle Systeme, die einen Richtliniendurchsetzungspunkt und einen Richtlinienverwaltungspunkt bereitstellen.

Sie können IBM SOA Policy Gateway Pattern auf einem IBM PureApplication System-Gerät unter IBM Power- oder x86-Architekturen installieren.

Der Richtlinienverwaltungspunkt wird durch Muster für virtuelle Systeme eingerichtet, die WSRR in einer mehrstufigen Architektur mit einer Produktionsumgebung und einer Bereitstellungsumgebung (Stagingumgebung) zur Verfügung stellen. Der Richtliniendurchsetzungspunkt kann von einem WebSphere DataPower-Gerät bereitgestellt werden. Alternativ kann unter x86PureApplication System ein virtuelles DataPower-Image implementieren. In beiden Fällen wird während der Implementierung des virtuellen Systemmusters eine Domäne erstellt. Der Richtlinienüberwachungspunkt wird durch ein Überwachungs-Add-on zum PureApplication System-Überwachungsservice bereitgestellt.

Im folgenden Diagramm werden die Funktionen dargestellt, die von IBM SOA Policy Gateway Pattern abgeleitet werden.



Es gibt Beispiele für Richtlinien in vielen, wenn nicht sogar in allen, SOA-Umgebungen (SOA - Service Oriented Architecture, serviceorientierte Architektur). Produzenten und Konsumenten von Services stimmen sich über die

Funktionalität, die Leistung und die Merkmale eines Service während der Entwurfsphase ab. Um diese Vereinbarungen zu implementieren, können Sie Service-Level-Definitionen (SLD) und Service-Level-Agreements (SLA) verwenden. Mit der Verwendung dieses Musters definieren Sie die Richtlinien für SLDs und SLAs in einer effizient verwalteten, definierten und geregelten Weise. Zu den Richtlinientypen, die in diesem Muster verwendet werden, gehören die folgenden:

- **Mediationsrichtlinien:**
  - Rejection - Zurückweisen oder Drosseln von Anforderungen, die mit einer höheren als der definierten Rate eintreffen.
  - Logging - Erstellen einer Protokollnachricht für den Richtliniendurchsetzungspunkt, wenn ein Service aufgerufen wird.
  - Transformation.
  - Validation - Validieren (Überprüfen) des Serviceaufrufs anhand der Servicedefinition.
  - Routing - Weiterleiten an einen bestimmten Endpunkt entsprechend den Angaben der Nachricht.
- **Sicherheitsrichtlinien**: Im Beispiel wird die Durchsetzung von Sicherheitsrichtlinien zur XACML-Zugriffssteuerung dargestellt. Diese Richtlinien werden zurzeit im Richtlinienverwaltungspunkt nicht durch Governance-Richtlinien geregelt.
- **Überwachungsrichtlinien**: Sie können für PureApplication System-Implementierungen Überwachungsrichtlinien definieren.

IBM SOA Policy Gateway Pattern enthält die folgenden virtuellen Systemmuster:

- SOA Policy Gateway Basic Runtime Sample (nur x86)
- SOA Policy Gateway Governance Master
- SOA Policy Gateway Basic Runtime
- SOA Policy Gateway Basic Runtime External DataPower
- SOA Policy Gateway Advanced Runtime
- SOA Policy Gateway Advanced Runtime External DataPower
- System Monitoring for SOA Policy Gateway Pattern 2.5 (ein gemeinsam genutzter Service)

Die virtuellen Systemmuster für virtuelle Systeme stellen zusammen eine Governance-Umgebung für Services aus mehreren Ebenen bereit. IBM SOA Policy Gateway Pattern bietet außerdem die Möglichkeit, während der Musterimplementierung mehrere für die Governance-Umgebung konfigurierte DataPower-Domänen bereitzustellen.

Weitere Informationen zu SOA Policy finden Sie in Kapitel 1, „SOA Policy - Übersicht", auf Seite 1.

Zugehörige Konzepte:

Kapitel 1, „SOA Policy - Übersicht", auf Seite 1
Das Richtlinienmanagement spielt eine entscheidende Rolle bei einer strukturierten und konsistenten Regelung von Richtlinien (Governance). Richtlinien können zur Einrichtung einer besseren Governance in einer beliebigen serviceorientierten Umgebung verwendet werden.

„SOA Policy Gateway Basic Runtime External DataPower" auf Seite 24
Das SOA Policy Gateway Basic Runtime External DataPower-Muster entspricht dem Basic Runtime-Muster, erfordert aber, dass externe DataPower-Geräte bei der Implementierung angegeben werden.

„SOA Policy Gateway Basic Runtime Sample (x86)” auf Seite 19
SOA Policy Gateway Basic Runtime Sample stellt ein Basic Runtime-Muster mit einer Beispielschnittstelle und einer Beispielanwendung bereit, die die gegenwärtig in diesem Release unterstützten Richtlinien demonstrieren.

„SOA Policy Gateway Governance Master” auf Seite 21
Das SOA Policy Gateway Governance Master-Muster stellt eine Cluster-Governance-Umgebung für die Erstellung und Verwaltung von Services und Richtlinien bereit. Die Umgebung wird mit dem konfigurierten Standard-Governance-Realisierungsprofil von WSRR bereitgestellt. Das Standard-Governance-Realisierungsprofil unterstützt zwei Umstufungsziele (Promotionsziele): 'Staging' und 'Production'.

„SOA Policy Gateway Advanced Runtime External DataPower” auf Seite 27
SOA Policy Gateway Advanced Runtime External DataPower entspricht dem Advanced Runtime-Muster, erfordert aber, dass externe DataPower-Geräte bei der Implementierung angegeben werden.

„System Monitoring for SOA Policy Gateway” auf Seite 29
Der Shared Service "System Monitoring for SOA Policy Gateway" stellt die Überwachungskomponenten für SOA Policy Gateway bereit.

Kapitel 3. Erste Schritte mit IBM SOA Policy Gateway Pattern

Dieses Muster verwendet WebSphere DataPower zur Steuerung von Nachrichten mithilfe geregelter Richtlinien und Servicedefinitionen in WSRR. Lesen Sie die Informationen in diesem Abschnitt, um sich mit dem Herunterladen und Installieren des Musters, mit der Überprüfung des Musters nach der Installation, mit dem Akzeptieren der Lizenzen und mit den beteiligten Benutzerrollen vertraut zu machen.

Muster herunterladen und installieren

IBM SOA Policy Gateway Pattern für die Verwendung mit IBM PureApplication System wird in einem Paket zum Download von Passport Advantage zur Verfügung gestellt.

Vorbereitende Schritte

Sie laden IBM SOA Policy Gateway Pattern auf ein vorläufiges System herunter, das ein Linux- oder Microsoft Windows-System sein kann. Dann führen Sie das Installationsprogramm auf dem vorläufigen System aus, um die Muster auf IBM PureApplication System zu installieren.

Stellen Sie sicher, dass 16 GB Speicherplatz für die Datei `CIQ1LML.tar.gz` (Power) oder die Datei `CIQ1VML.tar.gz` (x86) sowie weitere 40 GB für die extrahierten Dateien verfügbar sind. Außerdem muss Java™ Runtime Environment (JRE) Version 6 installiert werden, bevor die Musterinstallation gestartet werden kann. Sie können JRE für Linux von der folgenden Adresse herunterladen: http://www.ibm.com/developerworks/java/jdk/linux/download.html.

Informationen zu diesem Vorgang

IBM SOA Policy Gateway Pattern befindet sich im Paket der Datei `CIQ1LML.tar.gz` für das Power-Zielsystem oder der Datei `CIQ1VML.tar.gz` für ein x86-Zielsystem. Dieses Archiv enthält die OVA-Dateien (OVA, Open Virtual Archive), die Scriptpaketdateien und die Musterdefinitionsdateien.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um die IBM SOA Policy Gateway Pattern-Images von Passport Advantage herunterzuladen:

1. Greifen Sie auf die Passport Advantage-Website zu: Passport Advantage.
2. Laden Sie die Archivdatei mit den Images, Scriptpaketen und Mustern herunter, die verwendet werden sollen. Die Datei heißt `CIQ1LML.tar.gz` (Power) oder `CIQ1VML.tar.gz` (x86).
3. Öffnen Sie ein Terminal unter Linux bzw. ein Fenster mit Eingabeaufforderung unter Windows und navigieren Sie in das Verzeichnis, in das die Archivdatei heruntergeladen wurde.
4. Extrahieren Sie den Inhalt der Archivdatei in Ihr lokales Dateisystem. Unter Linux wird der folgende Extraktionsbefehl verwendet:

```
tar xvzf archivdatei
```

Unter Windows verwenden Sie zusätzliche Archivsoftware zum Extrahieren des Inhalts der Archivdatei.

5. Wechseln Sie in das Verzeichnis `installer`:

```
cd installer
```

6. Führen Sie das Installationsprogramm aus, um IBM SOA Policy Gateway Pattern in IBM PureApplication System zu installieren. Der Name des Befehls ist `installer.bat` unter Microsoft Windows bzw. `installer` unter Linux. Geben Sie den folgenden Befehl ein: `installer -h <host> -u <benutzername> -p <kennwort>`. Dabei ist <host> das IBM PureApplication System und 'benutzername' und 'kennwort' sind die Berechtigungsnachweise des Cloudadministrators. Beispiel:

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

7. Wenn Sie dazu aufgefordert werden, akzeptieren Sie die Lizenzvereinbarung für IBM SOA Policy Gateway Pattern.
   a. Unter Microsoft Windows: Wenn das Terminal nach dem Akzeptieren der Lizenzvereinbarung in einer neuen Zeile >>> anzeigt, geben Sie `quit()` ein und drücken die Eingabetaste. Wiederholen Sie Schritt 7.
8. Die Muster werden importiert. Bei der Installation der einzelnen Muster wird jeweils eine Nachricht im Installationsprogramm angezeigt, die angibt, dass es erfolgreich installiert wurde. Beispiel:

```
Importing pattern "SOA Policy Gateway 2.5.0.0 - Governance Master" ...
Import pattern "SOA Policy Gateway 2.5.0.0 - Governance Master" successfully.
```

Ergebnisse

Die Muster und Scripts werden geladen und die Muster für virtuelle Systeme werden erstellt.

Anmerkung: Wenn ein Muster für ein virtuelles System mit der richtigen Version, die in IBM SOA Policy Gateway Pattern verwendet wird, im Katalog vorhanden ist, wird es nicht überschrieben.

Nächste Schritte

Akzeptieren Sie die Lizenzen in IBM PureApplication System, siehe.

Informationen zur Überprüfung der Installation finden Sie in „Das installierte Muster überprüfen”.

Das installierte Muster überprüfen

Sie können überprüfen, ob das Muster erfolgreich installiert wurde.

Vorbereitende Schritte

Stellen Sie sicher, dass alle Schritte in „Muster herunterladen und installieren” auf Seite 13 ausgeführt wurden.

Informationen zu diesem Vorgang

Nach der Installation des Musters können Sie die Musterinstallation überprüfen, um sicherzustellen, ob alle Teile erfolgreich installiert wurden.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um die Installation von IBM SOA Policy Gateway Pattern zu überprüfen:

1. Öffnen Sie die Workload Console auf dem Gerät, auf dem das Muster installiert ist.
2. Überprüfen Sie die virtuellen Images, indem Sie zu **Catalog** > **Virtual Images** navigieren und die folgenden Elemente suchen:
   - DB2 Enterprise 10.1.0.2
   - WebSphere Service Registry and Repository 8.0.0.2
   - WebSphere DataPower X152 Virtual Edition (nur x86-Systeme)
3. Navigieren Sie zu **Catalog** > **Script Packages** und suchen Sie Folgendes:
   - SOA Policy Gateway 2.5.0.0 - DataPower Domain
   - SOA Policy Gateway 2.5.0.0 - DataPower Monitoring (nur x86)
   - 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 (nur x86)
   - 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

   Diese Scriptpakete sind alle in einer erfolgreichen Installation vorhanden.
4. Navigieren Sie zu **Patterns** > **Virtual Systems**. Suchen Sie auf x86-Systemen Folgendes:
   - 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

   Suchen Sie auf Power-Systemen Folgendes:
   - 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

   Diese Muster sind alle in einer erfolgreichen Installation vorhanden.
5. Navigieren Sie zu **Cloud** > **Pattern Types** und suchen Sie das folgende Element:
   - System Monitoring for SOA Policy Gateway Pattern 2.5.0.0

   Dieses Muster ist in einer erfolgreichen Installation vorhanden.

Ergebnisse

Sie haben die Installation von IBM SOA Policy Gateway Pattern überprüft.

Nächste Schritte

Wenn die Installation erfolgreich war, können Sie mit dem Akzeptieren der Lizenzen fortfahren. Siehe „Lizenzen akzeptieren" auf Seite 16. Wenn die Installation nicht erfolgreich war, wiederholen Sie die in „Muster herunterladen

und installieren" auf Seite 13 beschriebene Prozedur ab Schritt 7.

Lizenzen akzeptieren

Sie müssen für neu installierte Teile Lizenzen akzeptieren, bevor Sie mit den Mustern arbeiten können.

Vorbereitende Schritte

Stellen Sie sicher, dass alle Schritte in „Muster herunterladen und installieren" auf Seite 13 ausgeführt wurden.

Informationen zu diesem Vorgang

Bevor ein virtuelles Image verwendet werden kann, müssen Sie die für das Image erforderliche Lizenz akzeptieren.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um Lizenzen zu akzeptieren:

1. Öffnen Sie die Workload Console auf dem Gerät, auf dem das Muster installiert ist.
2. Wählen Sie **Catalog** > **Virtual Images** aus.
3. Suchen Sie in der Liste **Virtual Images** die folgenden Images und bestätigen Sie, dass die Lizenz im Fenster 'Details' akzeptiert wurde. Wenn dies nicht der Fall ist, klicken Sie auf 'Accept', um die Lizenz zu akzeptieren. x86-Systeme:
   - WebSphere DataPower XI52 Virtual Edition, Version 6.0.0.0 - Image-Referenznummer: XI52.6.0.0.0231528 (2013/06/16 14:14:19)
   - WebSphere Service Registry and Repository 8.0.0.2 - Image-Referenznummer: 201309062038
   - DB2 Enterprise 10.1.0.2 - Image-Referenznummer: 39
   - IBM OS Image for Red Hat Linux Systems, Version 2.0.0.3 - Image-Referenznummer: 136

   Power-Systeme:
   - WebSphere Service Registry and Repository 8.0.0.2 - Image-Referenznummer: 201309080001
   - DB2 Enterprise 10.1.0.2 - Image-Referenznummer: 50
   - IBM OS Image for AIX Systems Version 2.0.0.2 - Image-Referenznummer: 126
4. Zum Akzeptieren einer Lizenz klicken Sie auf das Image, um die zugehörigen Details anzuzeigen. Der Status wird angezeigt. Klicken Sie für die Lizenzvereinbarung auf **accept** und anschließend auf eine der Lizenzen, die akzeptiert werden muss, bevor das virtuelle Image verwendet werden kann. Nach dem Abschluss wird für den Status wird **Read-only** und für die Lizenzvereinbarung **Accepted** angezeigt. Wenn eine Lizenz nicht akzeptiert wurde, enthält das Imagesymbol ein rotes Feld mit einem Kreuz.

Ergebnisse

Sie haben die Lizenzen für IBM SOA Policy Gateway Pattern akzeptiert.

Nächste Schritte

Wenn die Installation erfolgreich war und Sie alle Lizenzen akzeptiert haben, können Sie mit den Mustern arbeiten. Siehe Kapitel 5, „Mit IBM SOA Policy Gateway Pattern arbeiten", auf Seite 47. Wenn die Installation nicht erfolgreich war, wiederholen Sie die in „Muster herunterladen und installieren" auf Seite 13 beschriebene Prozedur ab Schritt 7.

Benutzerzugriff konfigurieren

Damit Benutzer auf die Images und Muster auf dem Gerät zugreifen können, muss der Geräteadministrator den Benutzerzugriff zunächst erteilen. Sie können die Benutzer zuerst erstellen und der Gruppe hinzufügen oder Sie können zuerst die Gruppe erstellen und anschließend die Benutzer erstellen und der Gruppe hinzufügen.

Informationen zu diesem Vorgang

Benutzer mit Verwaltungsaufgaben, in der Regel der Geräteadministrator, können der Zugriffsgruppe weitere Benutzer hinzufügen und die Muster verwalten. Dies wird mit der Systemkonsole durchgeführt.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um den Benutzerzugriff zu konfigurieren:

1. Wählen Sie eine der folgenden Optionen zum Konfigurieren von Benutzern und optional von Benutzergruppen aus:
   - Fügen Sie einen Benutzer über das Fenster **Users** der Konsole hinzu und konfigurieren Sie ihn.
     a. Klicken Sie im Menü auf **System** > **Users**.
     b. Klicken Sie auf das Symbol zum Hinzufügen (**Add**).
     c. Geben Sie einen Kurznamen für den Benutzer sowie den tatsächlichen Namen des Benutzers, die E-Mail-Adresse und die Kennwörter an und klicken Sie auf **OK**.
     d. Wählen Sie den hinzugefügten Benutzer in der Anzeige **Users** aus, um den Zugriff zu konfigurieren. Konfigurieren Sie den Zugriff und die Aktionen des ausgewählten Benutzers.
     e. Fügen Sie den Benutzer einer oder mehreren Benutzergruppen im Feld **User groups** hinzu.
   - Erstellen Sie eine Benutzergruppe.
     a. Klicken Sie im Menü auf **System** > **User Groups**.
     b. Klicken Sie auf das Symbol zum Hinzufügen (**Add**). Geben Sie einen Namen und eine Beschreibung für die Gruppe an.
     c. Wählen Sie die hinzugefügte Gruppe in der Anzeige **User Groups** aus, um den Zugriff zu konfigurieren.
     d. Fügen Sie Mitglieder im Feld **Group members** hinzu und geben Sie die Berechtigungen an, die für die Gruppe gelten sollen.
2. Optional: Wenn Sie die virtuellen Images bereits hinzugefügt haben, erteilen Sie den Benutzern bzw. der Gruppe Zugriff auf die virtuellen Images. Wechseln Sie zur Workload Console und klicken Sie auf **Patterns** > **Virtual systems**, um das Fenster "Virtual System Patterns" zu öffnen. Wählen Sie ein virtuellesIBM SOA Policy Gateway Pattern-Image aus, um die Details anzuzeigen. Fügen Sie dem Feld **Access granted to** die Benutzer oder Gruppen hinzu.

Nächste Schritte

Wenn Sie die virtuellen Images noch nicht hinzugefügt haben, fügen Sie diese hinzu und geben den Benutzer- bzw. Gruppenzugriff für sie an.

Zugehörige Informationen:

IBM PureApplication System: Benutzer und Gruppen verwalten

Kapitel 4. Muster, Teile und Scriptpakete

Ein Muster stellt eine Topologiedefinition für eine wiederholbare Implementierung bereit, die gemeinsam genutzt werden kann. Die Teile von IBM SOA Policy Gateway Pattern sind funktionale Komponenten des Musters. Jeder Teil stellt eine einzelne virtuelle Maschine dar.

Muster beschreiben die Funktion, die von jeder virtuellen Maschine in einem virtuellen System bereitgestellt wird. Jede Funktion wird als Teil im Muster angegeben. Muster nehmen die Merkmale der ihnen zugeordneten Teile an. Wenn beispielsweise ein WSRR-Teil in ein Muster eingefügt wird, das anschließend implementiert wird, ist das Ergebnis eine virtuelle Maschine, die eine aktive WSRR-Instanz besitzt.

Muster

Wenn die virtuellen Images in IBM PureApplication System geladen wurden und der Zugriff den Benutzern erteilt wurde, können Benutzer mit der Arbeit mit den Mustern beginnen.

Muster stellen eine wiederholt anwendbare Topologie bereit, die in einer Cloud implementiert werden kann. Implementierte Muster sind virtuelle Systeme, die in der Cloud ausgeführt werden. Muster enthalten Teile, unabhängig davon, ob sie vordefiniert sind oder erstellt wurden. Einige Teile sind für die Funktionsfähigkeit des Musters erforderlich, wenn es in der Cloud als virtuelles System implementiert wird.

SOA Policy Gateway Basic Runtime Sample (x86)

SOA Policy Gateway Basic Runtime Sample stellt ein Basic Runtime-Muster mit einer Beispielschnittstelle und einer Beispielanwendung bereit, die die gegenwärtig in diesem Release unterstützten Richtlinien demonstrieren.

Das SOA Policy Gateway Basic Runtime Sample-Muster ist nur auf x86-Systemen verfügbar.

Das SOA Policy Gateway Basic Runtime Sample-Muster hat die folgenden Teile:

- Eigenständiger WSRR-Server
- DB2 Enterprise
- DataPower

Das SOA Policy Gateway Basic Runtime Sample-Muster installiert eine Beispielanwendung in der implementierten Umgebung. Das Muster installiert eine Beispieldomäne in DataPower, die einen Beispielservice implementiert, installiert eine Beispiel-WSDL und zugeordnete Richtlinien in WSRR für den Service und stellt eine Testanwendung zur Demonstration der durchgesetzten Richtlinien bereit. Weitere Informationen zur Beispielanwendung finden Sie in „Beispielanwendung” auf Seite 60. Die Beispieldomäne wird innerhalb von DataPower installiert und eine Beispiel-WSDL und Beispielrichtlinien werden in WSRR installiert. Die Verwendung mehrerer Richtlinien für einen Service wird demonstriert.

Im folgenden Diagramm wird das Basic Runtime-Beispiel dargestellt.

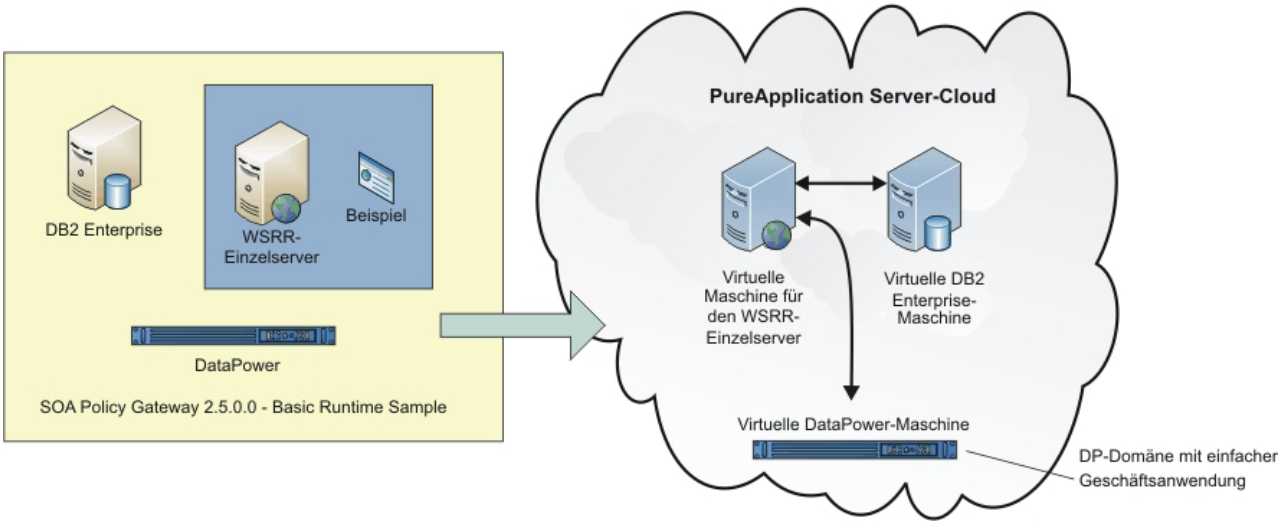


Abbildung 5. PureApplication Server-Konfiguration mit virtueller DataPower-Maschine (nur x86)

Zu den implementierten Richtlinien gehören:

Tabelle 1. Richtlinien, die im Basic Runtime Sample-Muster enthalten sind

Richtlinientyp	**Beschreibung**
Protokollierung (Logging)	Protokolliert auf der Basis einer Anforderungskontext-ID die Anforderung in DataPower.
Routing	Leitet auf der Basis einer Anforderungskontext-ID die Anforderung an einen angegebenen Endpunkt.
Überprüfung	Überprüft (validiert) die Anforderung mithilfe der WSDL-Datei für Serviceimplementierungen.
Zurückweisung (Rejection)	Steuert Anforderungen an einen Service auf der Basis der Nachrichtenzählung mit den Aktionen 'reject' (zurückweisen), 'queue' (in Warteschlange einreihen) und anderen.
Sicherheits-AAA (Security AAA)	Steuert den Zugriff auf den Server mithilfe der XACML-basierten Benutzerberechtigung. Die XACML wird nicht in WSRR gespeichert.
Sicherheitsüberarbeitung (Security Redaction)	Überarbeitet Teile der Antwortnachricht nach XACML-Anweisungen. Die XACML wird nicht in WSRR gespeichert.

Scripts und erweiterte Optionen

Das Muster erfordert die folgenden Teile.

Im Teil für den eigenständigen WSRR-Server:

- SOA Policy Gateway 2.5.0.0 - Sample

Informationen zu den Parametern der Teile und Scripts finden Sie in folgenden Abschnitten:

- „DB2 Enterprise-Teil" auf Seite 30
- „Teil für eigenständigen WSRR-Server" auf Seite 36
- „DataPower-Teil" auf Seite 38

- „Script: SOA Policy Gateway 2.5.0.0 - Sample” auf Seite 42

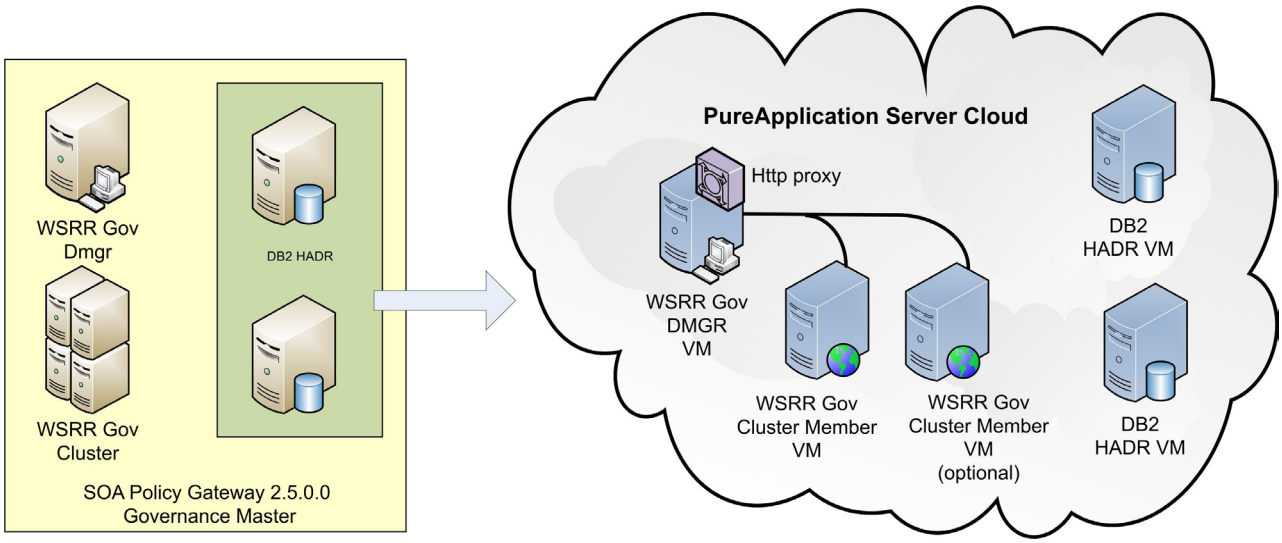
SOA Policy Gateway Governance Master

Das SOA Policy Gateway Governance Master-Muster stellt eine Cluster-Governance-Umgebung für die Erstellung und Verwaltung von Services und Richtlinien bereit. Die Umgebung wird mit dem konfigurierten Standard-Governance-Realisierungsprofil von WSRR bereitgestellt. Das Standard-Governance-Realisierungsprofil unterstützt zwei Umstufungsziele (Promotionsziele): 'Staging' und 'Production'.

Das SOA Policy Gateway Governance Master-Muster erfordert die folgenden Teile:

- DB2-HADR-Primärdatenbank
- DB2-HADR-Bereitschaftsdatenbank
- WSRR-Deployment Manager
- Angepasste WSRR-Knoten

Anmerkung: Das Governance Master-Muster muss vor der Implementierung der Runtime-Muster implementiert werden. Parameter, die zur Konfiguration des Governance Master-Musters verwendet werden, werden von den Runtime-Mustern verwendet, um sich im Governance Master zu konfigurieren.



Parameter der Teile

Informationen zu den Parametern der Teile finden Sie in folgenden Abschnitten:

- „Teil für DB2 Enterprise-HADR-Primärdatenbank” auf Seite 32
- „Teil für DB2 Enterprise-HADR-Bereitschaftsdatenbank” auf Seite 34
- „WSRR-Deployment Manager-Teil” auf Seite 37
- „Teil für angepasste WSRR-Knoten” auf Seite 37
- „Script: SOA Policy Gateway 2.5.0.0 - Security” auf Seite 43
- „Script: SOA Policy Gateway 2.5.0.0 - Promotion” auf Seite 41

Governance-Muster als Governance Master verwenden

Das SOA Policy Gateway Governance Master-Muster wird mit dem WSRR-Standard-Governance-Realisierungsprofil implementiert, das zwei

Promotionsstufen ('Staging' und 'Production') enthält. Weitere Informationen zum Governance-Realisierungsprofil in WSRR finden Sie im Information Center von IBM WebSphere Service Registry and Repository Version 8.0 - Governance-Realisierungsprofil. Das Basic Runtime-Muster und das Advanced Runtime-Muster können in dieser Integration als Umstufungsziele (Promotionsziele) implementiert werden. Weitere Informationen zum Konfigurieren von Umstufungszielen finden Sie in „Eine zusätzliche Laufzeitumgebung hinzufügen” auf Seite 57.

Zugehörige Informationen:

Information Center von IBM WebSphere Service Registry and Repository Version 8.0 - Governance-Realisierungsprofil

SOA Policy Gateway Basic Runtime

Das SOA Policy Gateway Basic Runtime-Muster ist die einfachste Möglichkeit, eine SOA Policy Gateway-Laufzeit bereitzustellen. Sie beinhaltet zwei DataPower-Instanzen (nur x86), eine eigenständige WSRR-Instanz, eine eigenständigeDB2-Instanz und eine Basisbetriebssystem-Instanz (zum Hosten der DataPower-Überwachungsagents).

Anmerkung: In diesem Abschnitt wird das unter x86 verfügbare Muster beschrieben. Informationen zum IBM Power-Muster finden Sie in „SOA Policy Gateway Basic Runtime External DataPower” auf Seite 24.

Das SOA Policy Gateway Basic Runtime-Muster erfordert die folgenden Teile:

- Eigenständiger WSRR-Server
- DB2 Enterprise
- WebSphere DataPower X152 Virtual Edition
- SOA-Überwachung für DataPower (in einem Core OS-Teil)

Im folgenden Diagramm wird die Konfiguration des SOA Policy Gateway Basic Runtime-Musters dargestellt.

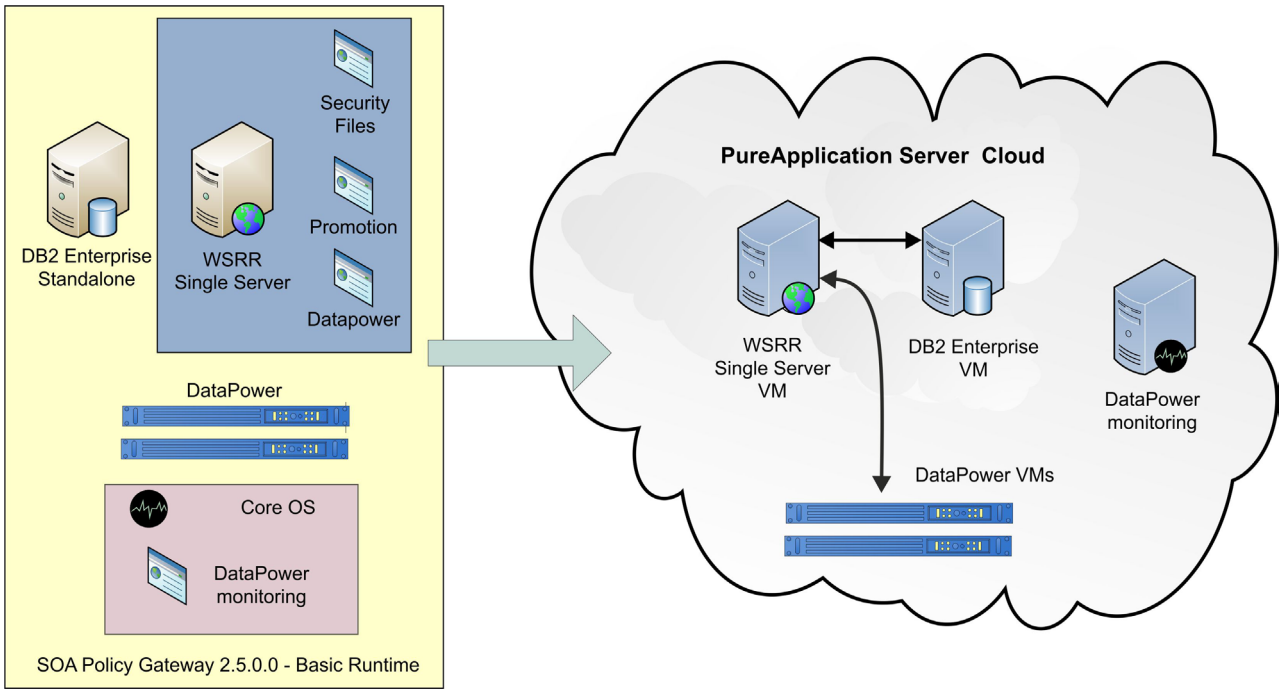


Abbildung 6. PureApplication Server-Konfiguration mit virtueller DataPower-Maschine

Scripts und erweiterte Optionen

Für das Muster wird eine Benutzereingabe in den folgenden Scripts während der Implementierung benötigt.

Im Teil für den eigenständigen WSRR-Server:

- 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

Im Core OS-Teil:

- SOA Policy Gateway 2.5.0.0 - DataPower Monitoring

Informationen zu den Parametern der Teile und Scripts finden Sie in folgenden Abschnitten:

- „Teil für eigenständigen WSRR-Server" auf Seite 36
- „DB2 Enterprise-Teil" auf Seite 30
- „DataPower-Teil" auf Seite 38
- „Script: SOA Policy Gateway 2.5.0.0 - Security" auf Seite 43
- „Script: SOA Policy Gateway 2.5.0.0 - Promotion" auf Seite 41
- „Script: SOA Policy Gateway 2.5.0.0 - DataPower Domain" auf Seite 40
- „Script: SOA Policy Gateway 2.5.0.0 - DataPower Monitoring (nur x86)" auf Seite 44

Basic Runtime mit einem Governance Master konfigurieren

Bei der Konfiguration eines Basic Runtime-Musters mit einem Governance Master-Muster geschieht Folgendes:

- Die zellenübergreifende Sicherheit wird konfiguriert.
- Die Datei `promotion.xml` auf dem Governance Master wird mit den Implementierungsdaten für die Basic Runtime-Implementierung aktualisiert.

Zur Konfiguration der Promotion müssen Sie eine der folgenden Stufenoptionen auswählen:

- Produktion ('production')
- Bereitstellung ('staging')

Diese Optionen entsprechen den Stufen, die durch das Governance-Realisierungsprofil (Governance Enablement Profile) in WSRR bereitgestellt werden. Weitere Informationen zum Governance-Realisierungsprofil in WSRR finden Sie im Information Center von IBM WebSphere Service Registry and Repository Version 8.0 - Governance-Realisierungsprofil.

Anmerkung: Sie können dieses Muster verwenden, um ein eigenständiges System ohne Governance Master bereitzustellen. Geben Sie dazu für die Governance Master-Parameter „Unset" an, wenn Sie das Muster implementieren. Diese Einstellungen führen dazu, dass das Promotion-Script während der Implementierung einen Fehler generiert. Die Implementierung zeigt **failed** an, aber Sie können diesen Fehler ignorieren.

SOA Policy Gateway Basic Runtime External DataPower

Das SOA Policy Gateway Basic Runtime External DataPower-Muster entspricht dem Basic Runtime-Muster, erfordert aber, dass externe DataPower-Geräte bei der Implementierung angegeben werden.

Anmerkung: Diese Beschreibung wird auf das Muster von IBM Power-Systemen angewendet.

Das SOA Policy Gateway Basic Runtime External DataPower-Muster hat die folgenden Teile:

- Eigenständiger WSRR-Server
- DB2 Enterprise
- SOA-Überwachung für DataPower (in einem Core OS-Teil)

Im folgenden Diagramm wird die Konfiguration des SOA Policy Gateway Basic Runtime External DataPower-Musters dargestellt.

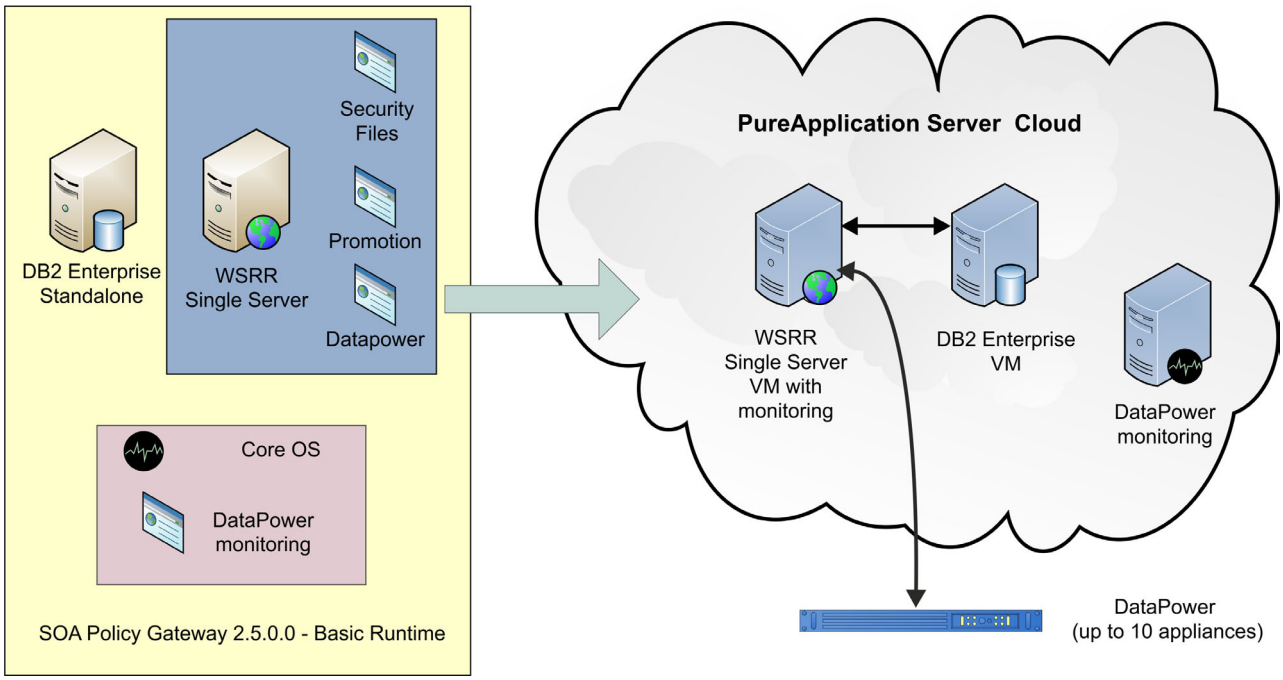


Abbildung 7. PureApplication Server-Konfiguration mit DataPower-Geräten

Scripts und erweiterte Optionen

Für das Muster wird eine Benutzereingabe in den folgenden Scripts während der Implementierung benötigt.

Im Teil für den eigenständigen WSRR-Server:

- 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

Im Core OS-Teil:

- SOA Policy Gateway 2.5.0.0 - DataPower Monitoring

Informationen zu den Parametern der Teile und Scripts finden Sie in folgenden Abschnitten:

- „Teil für eigenständigen WSRR-Server" auf Seite 36
- „DB2 Enterprise-Teil" auf Seite 30
- „Script: SOA Policy Gateway 2.5.0.0 - Security" auf Seite 43
- „Script: SOA Policy Gateway 2.5.0.0 - Promotion" auf Seite 41
- „Script: SOA Policy Gateway 2.5.0.0 - DataPower Domain" auf Seite 40
- „Script: SOA Policy Gateway 2.5.0.0 - DataPower Monitoring (nur x86)" auf Seite 44

Basic Runtime mit einem Governance Master konfigurieren

Bei der Konfiguration eines Basic Runtime-Musters mit einem Governance Master-Muster geschieht Folgendes:

- Die zellenübergreifende Sicherheit wird konfiguriert.

- Die Datei `promotion.xml` auf dem Governance Master wird mit den Implementierungsdaten für die Basic Runtime-Implementierung aktualisiert.

Zur Konfiguration der Promotion müssen Sie eine der folgenden Stufenoptionen auswählen:

- Produktion ('production')
- Bereitstellung ('staging')

Diese Optionen entsprechen den Stufen, die durch das Governance-Realisierungsprofil (Governance Enablement Profile) in WSRR bereitgestellt werden. Wenn das Governance-Profil abweicht, wird „other" ausgewählt, wenn das Governance-Profil für den Governance Master geändert wurde. Weitere Informationen zum Governance-Realisierungsprofil in WSRR finden Sie im Information Center von IBM WebSphere Service Registry and Repository Version 8.0 - Governance-Realisierungsprofil.

Anmerkung: Sie können dieses Muster verwenden, um ein eigenständiges System ohne Governance Master bereitzustellen. Geben Sie dazu für die Governance Master-Parameter „Unset" an, wenn Sie das Muster implementieren. Diese Einstellungen führen dazu, dass das Promotion-Script während der Implementierung einen Fehler generiert. Die Implementierung zeigt **failed** an, aber Sie können diesen Fehler ignorieren.

SOA Policy Gateway Advanced Runtime

Das SOA Policy Gateway Advanced Runtime-Muster beinhaltet zwei DB2-Serverinstanzen in einer HADR-Konfiguration und einen WSRR-Cluster mit einem einzelnen Deployment Manger und zwei angepassten Knoten.

Anmerkung: In diesem Abschnitt wird das unter x86 verfügbare Muster beschrieben. Informationen zum IBM Power-Muster finden Sie in „SOA Policy Gateway Advanced Runtime External DataPower" auf Seite 27.

Das Muster erfordert die folgenden Teile:

- WSRR-Deployment Manager
- Angepasste WSRR-Knoten
- DB2-HADR-Primärdatenbank
- DB2-HADR-Bereitschaftsdatenbank
- WebSphere DataPower X152 Virtual Edition
- SOA-Überwachung für DataPower (in einem Core OS-Teil)

Im folgenden Diagramm wird die Konfiguration eines Advanced Runtime-Systems dargestellt.

Abbildung 8. PureApplication Server-Konfiguration mit virtuellen DataPower-Maschinen

Scripts und erweiterte Optionen

Für das Muster wird eine Benutzereingabe in den folgenden Scripts während der Implementierung benötigt:

Im WSRR-Deployment Manager-Teil:

- 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

Im Core OS-Teil:
- SOA Policy Gateway 2.5.0.0 - DataPower Monitoring

Informationen zu den Parametern der Teile und Scripts finden Sie in folgenden Abschnitten:
- „Teil für DB2 Enterprise-HADR-Primärdatenbank" auf Seite 32
- „Teil für DB2 Enterprise-HADR-Bereitschaftsdatenbank" auf Seite 34
- „WSRR-Deployment Manager-Teil" auf Seite 37
- „Teil für angepasste WSRR-Knoten" auf Seite 37
- „Script: SOA Policy Gateway 2.5.0.0 - Promotion" auf Seite 41
- „Script: SOA Policy Gateway 2.5.0.0 - DataPower Domain" auf Seite 40
- „Script: SOA Policy Gateway 2.5.0.0 - DataPower Monitoring (nur x86)" auf Seite 44

Advanced Runtime mit einem Governance Master konfigurieren

Bei der Konfiguration eines Advanced Runtime-Musters mit einem Governance Master-Muster geschieht Folgendes:
- Die zellenübergreifende Sicherheit wird konfiguriert.
- Die Datei `promotion.xml` auf dem Governance Master wird mit den Daten aus der Advanced Runtime-Implementierung aktualisiert.

Zur Konfiguration der Promotion müssen Sie eine der folgenden Stufenoptionen auswählen:
- Produktion ('production')
- Bereitstellung ('staging')

Diese Optionen entsprechen den Stufen, die durch das Governance-Realisierungsprofil (Governance Enablement Profile) in WSRR bereitgestellt werden. Weitere Informationen zum Governance-Realisierungsprofil in WSRR finden Sie im Information Center von IBM WebSphere Service Registry and Repository Version 8.0 - Governance-Realisierungsprofil.

SOA Policy Gateway Advanced Runtime External DataPower

SOA Policy Gateway Advanced Runtime External DataPower entspricht dem Advanced Runtime-Muster, erfordert aber, dass externe DataPower-Geräte bei der Implementierung angegeben werden.

Anmerkung: Diese Beschreibung wird auf das SOA Policy Gateway Advanced Runtime-Muster auf IBM Power-Systemen angewendet.

Das SOA Policy Gateway Advanced Runtime External DataPower-Muster erfordert die folgenden Teile:
- WSRR-Deployment Manager
- Angepasste WSRR-Knoten
- DB2-HADR-Primärdatenbank
- DB2-HADR-Bereitschaftsdatenbank
- SOA-Überwachung für DataPower (in einem Core OS-Teil)

Im folgenden Diagramm wird die Konfiguration eines Advanced Runtime-Systems dargestellt.

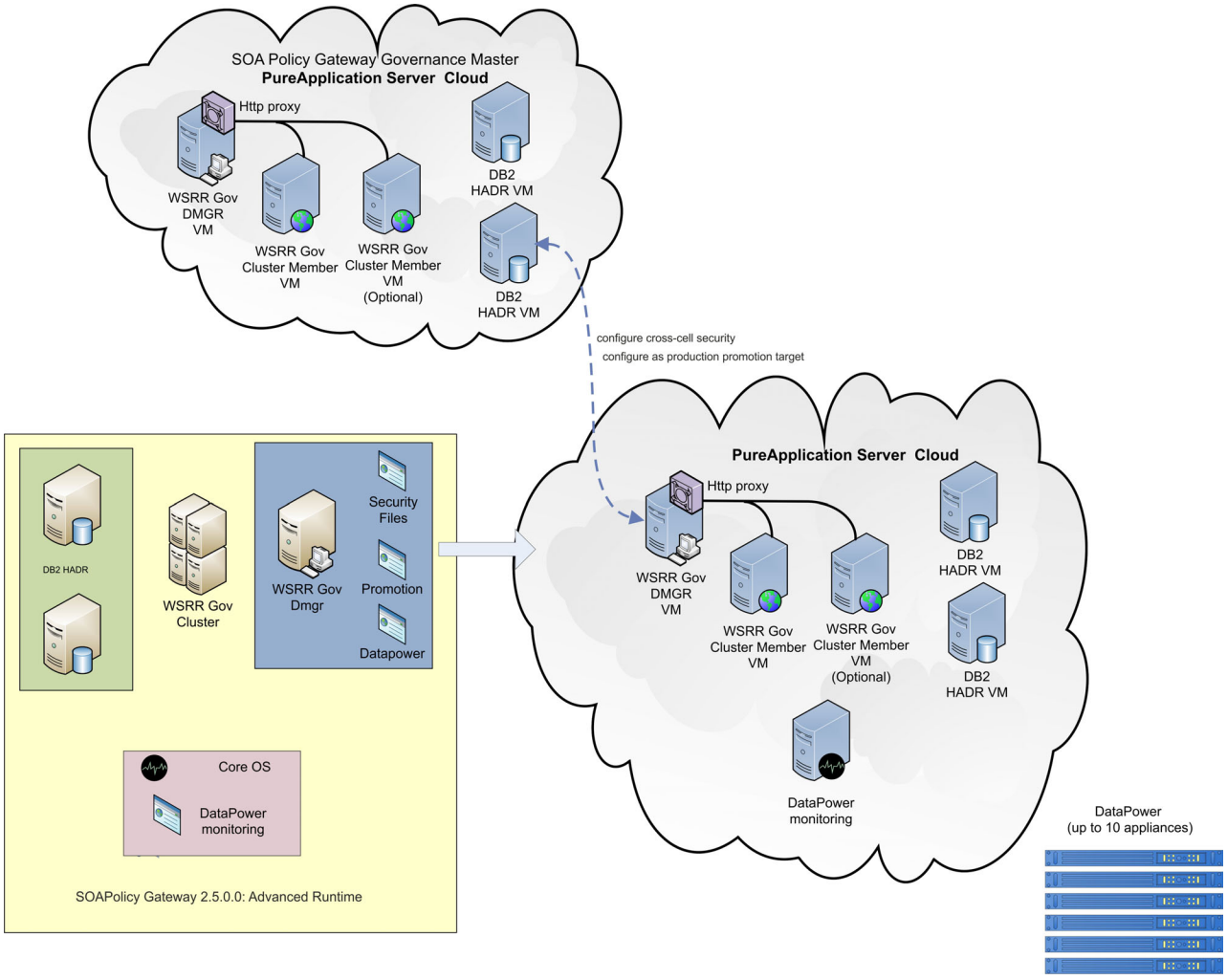


Abbildung 9. PureApplication Server-Konfiguration mit DataPower-Geräten

Scripts und erweiterte Optionen

Für das Muster wird eine Benutzereingabe in den folgenden Scripts während der Implementierung benötigt.

Im WSRR-Deployment Manager-Teil:

- 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

Im Core OS-Teil:

- SOA Policy Gateway 2.5.0.0 - DataPower Monitoring

Informationen zu den Parametern der Teile und Scripts finden Sie in folgenden Abschnitten:

- „Teil für DB2 Enterprise-HADR-Primärdatenbank” auf Seite 32

- „Teil für DB2 Enterprise-HADR-Bereitschaftsdatenbank” auf Seite 34
- „WSRR-Deployment Manager-Teil” auf Seite 37
- „Teil für angepasste WSRR-Knoten” auf Seite 37
- „Script: SOA Policy Gateway 2.5.0.0 - Promotion” auf Seite 41
- „Script: SOA Policy Gateway 2.5.0.0 - DataPower Domain” auf Seite 40
- „Script: SOA Policy Gateway 2.5.0.0 - DataPower Monitoring (nur x86)” auf Seite 44

Advanced Runtime mit einem Governance Master konfigurieren

Bei der Konfiguration eines Advanced Runtime-Musters mit einem Governance Master-Muster geschieht Folgendes:

- Die zellenübergreifende Sicherheit wird konfiguriert.
- Die Datei `promotion.xml` auf dem Governance Master wird mit den Daten aus der Advanced Runtime-Implementierung aktualisiert.

Zur Konfiguration der Umstufung (Promotion) müssen Sie eine der folgenden Stufenoptionen auswählen:

- Produktion ('production')
- Bereitstellung ('staging')

Diese Optionen entsprechen den Stufen, die durch das Governance-Realisierungsprofil (Governance Enablement Profile) in WSRR bereitgestellt werden. Weitere Informationen zum Governance-Realisierungsprofil in WSRR finden Sie im Information Center von IBM WebSphere Service Registry and Repository Version 8.0 - Governance-Realisierungsprofil.

Shared Service

Das Muster enthält einen gemeinsam genutzten Service, der von implementierten Mustern verwendet wird, um eine Überwachung bereitzustellen.

System Monitoring for SOA Policy Gateway

Der Shared Service "System Monitoring for SOA Policy Gateway" stellt die Überwachungskomponenten für SOA Policy Gateway bereit.

Die Überwachung in den Basic Runtime- und Advanced Runtime-Mustern wird durch den DataPower Monitoring Service bereitgestellt, der im Core OS-Teil ausgeführt wird. Der Überwachungsservice selbst verwendet ITCAM for SOA-Komponenten, die im Muster "System Monitoring for SOA Policy Gateway" enthalten sind. Für die Überwachung der WSRR-Instanzen muss außerdem der Shared Service "System Monitoring for WebSphere Application Server" ausgeführt werden.

Folgen Sie dem zugehörigen Link, um eine vollständige ITCAM for SOA-Dokumentation zu erhalten.

Zugehörige Informationen:

ITCAM for SOA 7.2.1 - Dokumentation (von Fix Central)

Teile

IBM SOA Policy Gateway Pattern umfasst die folgenden Teile.

DB2 Enterprise-Teil

Der DB2 Enterprise-Teil stellt einige Konfigurationsoptionen bereit.

Die konfigurierbaren Parameter des Teils für das virtuelle Systemimage von DB2 Enterprise 10.1.0.2 werden in der folgenden Tabelle beschrieben:

Tabelle 2. Konfigurierbare Parameter

Parametername	Standardwert	Beschreibung
Virtuelle CPUs (Virtual CPUs)	1	Die Anzahl der virtuellen Prozessoren, die für die durch diesen Teil dargestellte virtuelle Maschine zugeordnet werden.
Speicherkapazität (Memory size, MB)	2048	Die Speicherkapazität in MB, die dieser virtuellen Maschine zugeordnet wird.
Instanzeignergruppe (Instance owner group)	db2iadm1	Die Gruppe, zu der der DB2-Instanzeigner gehört.
Instanzeigner (Instance owner)	db2inst1	Die ID des DB2-Instanzeigners. Diese Benutzer-ID wird als Installationseigner der DB2-Instanz und als Eigner der Datenbankschemas verwendet.
Kennwort (Instanzeigner) (Password (Instance owner))	password	Das Kennwort für die Benutzer-ID 'db2inst1' des Betriebssystems.
Kennwort überprüfen (Verify password)	password	Überprüft das Kennwort des Instanzeigners.
Abgeschirmte Benutzergruppe (Fenced user group)	db2fadm1	Die Gruppe, zu der der abgeschirmte DB2-Eigner gehört.
Abgeschirmter Benutzer (Fenced user)	db2fenc1	Die ID des abgeschirmten DB2-Benutzers. Die abgeschirmte Benutzer-ID, die zur Ausführung benutzerdefinierter Funktionen (UDFs) und gespeicherter Prozeduren außerhalb des von der DB2-Datenbank verwendeten Adressraums verwendet wird. Ein abgeschirmter Benutzer ist ein Benutzer, unter dem "abgeschirmte" gespeicherte Prozeduren mit eingeschränkten Betriebssystemberechtigungen ausgeführt werden können.
Kennwort (Password) - db2fenc1		Das Kennwort für die abgeschirmte Benutzer-ID
Kennwort überprüfen (Verify password)		Überprüft das Kennwort des abgeschirmten Benutzers.
DAS-Benutzergruppe (DAS user group)	dasadm1	Die Gruppe, zu der der DB2-DAS-Eigner gehört.

Tabelle 2. Konfigurierbare Parameter (Forts.)

Parametername	Standardwert	Beschreibung
DAS-Benutzer (DAS user)	dasusr1	Die Benutzer-ID, die für den DB2-Verwaltungsserver verwendet wird, der zur Ausführung des DB2-Verwaltungsservers auf Ihrem System verwendet wird. Diese Benutzer-ID wird außerdem von den DB2-GUI-Tools zur Ausführung von Verwaltungstasks für die lokalen Datenbankinstanzen und Datenbanken des Servers verwendet.
Kennwort (DAS-Benutzer (Password (DAS user))	password	Das Kennwort für den DAS-Benutzer.
Kennwort überprüfen (Verify password)	password	Überprüft das Kennwort für 'dasusr1'.
DB2-Service-Port (DB2 Service port)	50000	Dieser Port ist gesperrt und kann nicht geändert werden.
Datenbankerstellung (Database creation)	Create-new-database	Dieser Wert ist gesperrt und kann nicht geändert werden.
Name für die neue Datenbank (Name for the new database)	WSRR	Dieser Wert ist gesperrt und kann nicht geändert werden.
Codeset für die neue Datenbank (Codeset for the new database)	UTF-8	
Gebiet für die neue Datenbank (Territory for the new database)	US	
Sammlung für die neue Datenbank (Codeset for the new database)	SYSTEM	
Seitengröße für die neue Datenbank (Pagesize for the new database)	32768	Dieser Wert ist gesperrt und kann nicht geändert werden.
DB2-Kompatibilitätsmodus (DB2 compatibility mode)	Default	Dieser Wert ist gesperrt und kann nicht geändert werden.
Alle Datenträger für DB2 konfigurieren (Configure all raw disks for use by DB2)	NO	
Kennwort (Password) - Root		Das Kennwort für die Rootbenutzer-ID. Dies ist das Kennwort für das Betriebssystem der virtuellen Maschine, die durch diesen Teil im Muster dargestellt wird.
Kennwort überprüfen (Verify password)		Überprüft das Kennwort für 'root'.
Kennwort (Password) - virtuser		Das Kennwort für die Benutzer-ID 'virtuser' des Betriebssystems. Diese Benutzer-ID wird als Benutzer-ID ohne Rootberechtigung für die virtuelle Maschine verwendet.
Kennwort überprüfen (Verify password)		Überprüft das Kennwort für 'virtuser'.
Enable VNC	True	Dieser Wert ist gesperrt und kann nicht geändert werden.

Teil für DB2 Enterprise-HADR-Primärdatenbank

Der Teil für die DB2 Enterprise-HADR-Primärdatenbank stellt einige Konfigurationsoptionen bereit.

Die konfigurierbaren Parameter des Teils für die DB2 Enterprise-HADR-Primärdatenbank werden in der folgenden Tabelle beschrieben:

Tabelle 3. Konfigurierbare Parameter

Parametername	Standardwert	Beschreibung
Virtuelle CPUs (Virtual CPUs)	1	Die Anzahl der virtuellen Prozessoren, die für die durch diesen Teil dargestellte virtuelle Maschine zugeordnet werden.
Speicherkapazität (Memory size, MB)	2048	Die Speicherkapazität in MB, die dieser virtuellen Maschine zugeordnet wird.
Instanzeignergruppe (Instance owner group)	db2iadm1	Die Gruppe, zu der der DB2-Instanzeigner gehört.
Instanzeigner (Instance owner)	db2inst1	Die ID des DB2-Instanzeigners. Diese Benutzer-ID wird als Installationseigner der DB2-Instanz und als Eigner der Datenbankschemas verwendet.
Kennwort (Instanzeigner) (Password (Instance owner))	password	Das Kennwort für die Benutzer-ID 'db2inst1' des Betriebssystems.
Kennwort überprüfen (Verify password)	password	Überprüft das Kennwort des Instanzeigners.
Abgeschirmte Benutzergruppe (Fenced user group)	db2fadm1	Die Gruppe, zu der der abgeschirmte DB2-Eigner gehört.
Abgeschirmter Benutzer (Fenced user)	db2fenc1	Die ID des abgeschirmten DB2-Benutzers. Die abgeschirmte Benutzer-ID, die zur Ausführung benutzerdefinierter Funktionen (UDFs) und gespeicherter Prozeduren außerhalb des von der DB2-Datenbank verwendeten Adressraums verwendet wird. Ein abgeschirmter Benutzer ist ein Benutzer, unter dem 'abgeschirmte' gespeicherte Prozeduren mit eingeschränkten Betriebssystemberechtigungen ausgeführt werden können.
Kennwort (Password) - db2fenc1		Das Kennwort für die abgeschirmte Benutzer-ID
Kennwort überprüfen (Verify password)		Überprüft das Kennwort des abgeschirmten Benutzers.
DAS-Benutzergruppe (DAS user group)	dasadm1	Die Gruppe, zu der der DB2-DAS-Eigner gehört.

Tabelle 3. Konfigurierbare Parameter (Forts.)

Parametername	Standardwert	Beschreibung
DAS-Benutzer (DAS user)	dasusr1	Die Benutzer-ID, die für den DB2-Verwaltungsserver verwendet wird, der zur Ausführung des DB2-Verwaltungsservers auf Ihrem System verwendet wird. Diese Benutzer-ID wird außerdem von den DB2-GUI-Tools zur Ausführung von Verwaltungstasks für die lokalen Datenbankinstanzen und Datenbanken des Servers verwendet.
Kennwort (DAS-Benutzer (Password (DAS user))	password	Das Kennwort für den DAS-Benutzer.
Kennwort überprüfen (Verify password)	password	Überprüft das Kennwort für 'dasusr1'.
DB2-Service-Port (DB2 Service port)	50000	Dieser Port ist gesperrt und kann nicht geändert werden.
Datenbankerstellung (Database creation)	Create-new-database	Dieser Wert ist gesperrt und kann nicht geändert werden.
Name für die neue Datenbank (Name for the new database)	WSRR	Dieser Wert ist gesperrt und kann nicht geändert werden.
Codeset für die neue Datenbank (Codeset for the new database)	UTF-8	
Gebiet für die neue Datenbank (Territory for the new database)	US	
Sammlung für die neue Datenbank (Codeset for the new database)	SYSTEM	
Seitengröße für die neue Datenbank (Pagesize for the new database)	32768	Dieser Wert ist gesperrt und kann nicht geändert werden.
DB2-Kompatibilitätsmodus (DB2 compatibility mode)	Default	Dieser Wert ist gesperrt und kann nicht geändert werden.
Alle Datenträger für DB2 konfigurieren (Configure all raw disks for use by DB2)	NO	
Kennwort (Password) - Root		Das Kennwort für die Rootbenutzer-ID. Dies ist das Kennwort für das Betriebssystem der virtuellen Maschine, die durch diesen Teil im Muster dargestellt wird.
Kennwort überprüfen (Verify password)		Überprüft das Kennwort für 'root'.
Kennwort (Password) - virtuser		Das Kennwort für die Benutzer-ID 'virtuser' des Betriebssystems. Diese Benutzer-ID wird als Benutzer-ID ohne Rootberechtigung für die virtuelle Maschine verwendet.
Kennwort überprüfen (Verify password)		Überprüft das Kennwort für 'virtuser'.
Enable VNC	True	Dieser Wert ist gesperrt und kann nicht geändert werden.

Sonstige Parameter werden aus dem Basismuster für virtuelle Systeme übernommen und sind gesperrt.

Teil für DB2 Enterprise-HADR-Bereitschaftsdatenbank

Der Teil für die DB2 Enterprise-HADR-Bereitschaftsdatenbank stellt einige Konfigurationsoptionen bereit.

Tabelle 4. Konfigurierbare Parameter

Parametername	Standardwert	Beschreibung
Virtuelle CPUs (Virtual CPUs)	1	Die Anzahl der virtuellen Prozessoren, die für die durch diesen Teil dargestellte virtuelle Maschine zugeordnet werden.
Speicherkapazität (Memory size, MB)	2048	Die Speicherkapazität in MB, die dieser virtuellen Maschine zugeordnet wird.
Instanzeignergruppe (Instance owner group)	db2iadm1	Die Gruppe, zu der der DB2-Instanzeigner gehört.
Instanzeigner (Instance owner)	db2inst1	Die ID des DB2-Instanzeigners. Diese Benutzer-ID wird als Installationseigner der DB2-Instanz und als Eigner der Datenbankschemas verwendet.
Kennwort (Instanzeigner) (Password (Instance owner))	password	Das Kennwort für die Benutzer-ID 'db2inst1' des Betriebssystems.
Kennwort überprüfen (Verify password)	password	Überprüft das Kennwort des Instanzeigners.
Abgeschirmte Benutzergruppe (Fenced user group)	db2fadm1	Die Gruppe, zu der der abgeschirmte DB2-Eigner gehört.
Abgeschirmter Benutzer (Fenced user)	db2fenc1	Die ID des abgeschirmten DB2-Benutzers. Die abgeschirmte Benutzer-ID, die zur Ausführung benutzerdefinierter Funktionen (UDFs) und gespeicherter Prozeduren außerhalb des von der DB2-Datenbank verwendeten Adressraums verwendet wird. Ein abgeschirmter Benutzer ist ein Benutzer, unter dem 'abgeschirmte' gespeicherte Prozeduren mit eingeschränkten Betriebssystemberechtigungen ausgeführt werden können.
Kennwort (Password) - db2fenc1		Das Kennwort für die abgeschirmte Benutzer-ID
Kennwort überprüfen (Verify password)		Überprüft das Kennwort des abgeschirmten Benutzers.
DAS-Benutzergruppe (DAS user group)	dasadm1	Die Gruppe, zu der der DB2-DAS-Eigner gehört.

Tabelle 4. Konfigurierbare Parameter (Forts.)

Parametername	Standardwert	Beschreibung
DAS-Benutzer (DAS user)	dasusr1	Die Benutzer-ID, die für den DB2-Verwaltungsserver verwendet wird, der zur Ausführung des DB2-Verwaltungsservers auf Ihrem System verwendet wird. Diese Benutzer-ID wird außerdem von den DB2-GUI-Tools zur Ausführung von Verwaltungstasks für die lokalen Datenbankinstanzen und Datenbanken des Servers verwendet.
Kennwort (DAS-Benutzer (Password (DAS user))	password	Das Kennwort für den DAS-Benutzer.
Kennwort überprüfen (Verify password)	password	Überprüft das Kennwort für 'dasusr1'.
DB2-Service-Port (DB2 Service port)	50000	Dieser Port ist gesperrt und kann nicht geändert werden.
Datenbankerstellung (Database creation)	Create-new-database	Dieser Wert ist gesperrt und kann nicht geändert werden.
Name für die neue Datenbank (Name for the new database)	WSRR	Dieser Wert ist gesperrt und kann nicht geändert werden.
Codeset für die neue Datenbank (Codeset for the new database)	UTF-8	
Gebiet für die neue Datenbank (Territory for the new database)	US	
Sammlung für die neue Datenbank (Codeset for the new database)	SYSTEM	
Seitengröße für die neue Datenbank (Pagesize for the new database)	32768	Dieser Wert ist gesperrt und kann nicht geändert werden.
DB2-Kompatibilitätsmodus (DB2 compatibility mode)	Default	Dieser Wert ist gesperrt und kann nicht geändert werden.
Alle Datenträger für DB2 konfigurieren (Configure all raw disks for use by DB2)	NO	
Kennwort (Password) - Root		Das Kennwort für die Rootbenutzer-ID. Dies ist das Kennwort für das Betriebssystem der virtuellen Maschine, die durch diesen Teil im Muster dargestellt wird.
Kennwort überprüfen (Verify password)		Überprüft das Kennwort für 'root'.
Kennwort (Password) - virtuser		Das Kennwort für die Benutzer-ID 'virtuser' des Betriebssystems. Diese Benutzer-ID wird als Benutzer-ID ohne Rootberechtigung für die virtuelle Maschine verwendet.
Kennwort überprüfen (Verify password)		Überprüft das Kennwort für 'virtuser'.
Enable VNC	True	Dieser Wert ist gesperrt und kann nicht geändert werden.

Sonstige Parameter werden aus dem Basismuster für virtuelle Systeme übernommen und sind gesperrt.

Teil für eigenständigen WSRR-Server

Der Teil für eigenständigen WSRR-Server stellt einige Konfigurationsoptionen bereit.

Die konfigurierbaren Parameter des Teils für eigenständigen WSRR-Server werden in der folgenden Tabelle beschrieben:

Tabelle 5. Konfigurierte Parameter

Parametername	Standardwert	Beschreibung
Virtuelle CPUs (Virtual CPUs)	1	Die Anzahl der virtuellen Prozessoren, die für die durch diesen Teil dargestellte virtuelle Maschine zugeordnet werden.
Speicherkapazität (Memory size, MB)	4096	Die Speicherkapazität in MB, die dieser virtuellen Maschine zugeordnet wird.
Zellenname (Cell name)	Legen Sie einen der folgenden Werte fest: • SOAPolicySampleCell (Basic Runtime Sample-Muster) • SOAPolicyBasicCell (Basic Runtime-Muster) • SOAPolicyBasicCell (externes DataPower-Muster von Basic Runtime)	
Knotenname (Node name)	Legen Sie einen der folgenden Werte fest: • SOAPolicySampleNode (Basic Runtime Sample-Muster) • SOAPolicyBasicNode (Basic Runtime-Muster) • SOAPolicyBasicNode (externes DataPower-Muster von Basic Runtime)	
Kennwort (Password) - Root		Das Kennwort für die Rootbenutzer-ID. Dies ist das Kennwort für das Betriebssystem der virtuellen Maschine, die durch diesen Teil im Muster dargestellt wird.
Kennwort überprüfen (Verify password)		Überprüft die Benutzereingabe für das Kennwort (root).
Name des WebSphere-Benutzers mit Verwaltungsaufgaben (Administrator)	virtuser	Der Name des Benutzers mit Administratorberechtigung für WebSphere Application Server. Dieser Wert darf nicht geändert werden.
Kennwort (Password) für den WebSphere-Administrator		Das Kennwort des Benutzers mit Administratorberechtigung für WebSphere Application Server.

Tabelle 5. Konfigurierte Parameter (Forts.)

Parametername	Standardwert	Beschreibung
Kennwort überprüfen (Verify password)		Überprüft die Benutzereingabe für das Kennwort des WebSphere Application Server-Administrators.
Enable VNC	True	Dieser Wert ist gesperrt und kann nicht geändert werden.

WSRR-Deployment Manager-Teil

Der WSRR-Deployment Manager-Teil stellt einige Konfigurationsoptionen bereit.

Die konfigurierbaren Parameter des WSRR-Deployment Manager-Teils werden in der folgenden Tabelle beschrieben:

Tabelle 6. Konfigurierbare Parameter

Parametername	Standardwert	Beschreibung
Virtuelle CPUs (Virtual CPUs)	1	Die Anzahl der virtuellen Prozessoren, die für die durch diesen Teil dargestellte virtuelle Maschine zugeordnet werden.
Speicherkapazität (Memory size, MB)	2048	Die Speicherkapazität in MB, die dieser virtuellen Maschine zugeordnet wird.
Zellenname (Cell name)	SOAPolicyAdvancedCell	Der Zellenname für das Advanced Runtime-Muster.
Knotenname (Node name)	SOAPolicyAdvancedNode	Der Knotenname für den Knoten, der sich auf der virtuellen Maschine des Deployment Managers im Advanced Runtime-Muster befindet.
Kennwort (Password) - Root		Das Kennwort für die Rootbenutzer-ID. Dies ist das Kennwort für das Betriebssystem der virtuellen Maschine, die durch diesen Teil im Muster dargestellt wird.
Kennwort überprüfen (Verify password)		Überprüft die Benutzereingabe für das Kennwort (root).
Name des WebSphere-Benutzers mit Verwaltungsaufgaben (Administrator)	virtuser	Der Name des Benutzers mit Administratorberechtigung für WebSphere Application Server. Dieser Wert darf nicht geändert werden.
Kennwort (Password) für den WebSphere-Administrator		Dar Kennwort des Benutzers mit Administratorberechtigung für WebSphere Application Server.
Kennwort überprüfen (Verify password)		Überprüft die Benutzereingabe für das Kennwort des WebSphere Application Server-Administrators.
Enable VNC	True	Dieser Wert ist gesperrt und kann nicht geändert werden.

Teil für angepasste WSRR-Knoten

Das Teil für angepasste WSRR-Knoten stellt einige Konfigurationsoptionen bereit.

Die konfigurierbaren Parameter des Teils für angepasste WSRR-Knoten werden in der folgenden Tabelle beschrieben:

Tabelle 7. Konfigurierbare Parameter

Parametername		**Beschreibung**
Virtuelle CPUs (Virtual CPUs)	2	Die Anzahl der virtuellen Prozessoren, die für die durch diesen Teil dargestellte virtuelle Maschine zugeordnet werden.
Speicherkapazität (Memory size, MB)	4096	Die Speicherkapazität in MB, die dieser virtuellen Maschine zugeordnet wird.
Zellenname (Cell name)	CloudBurstCell	Der Wert für den Zellennamen in der Konfiguration des Teils für angepasste Knoten wird ignoriert.
Knotenname (Node name)	SOAPolicyAdvancedNode	Der Knotenname für den Knoten, der sich auf der virtuellen Maschine des angepassten Knotens im Advanced Runtime-Muster befindet.
Kennwort (Password) - Root		Das Kennwort für die Rootbenutzer-ID. Dies ist das Kennwort für das Betriebssystem der virtuellen Maschine, die durch diesen Teil im Muster dargestellt wird.
Kennwort überprüfen (Verify password)		Überprüft die Benutzereingabe für das Kennwort (root).
Name des WebSphere-Benutzers mit Verwaltungsaufgaben (Administrator)	virtuser	Der Name des Benutzers mit Administratorberechtigung für die WebSphere Application Server-Umgebung. Dieser Wert darf nicht geändert werden.
Kennwort (Password) für den WebSphere-Administrator		Das Kennwort des Benutzers mit Administratorberechtigung für die WebSphere Application Server-Umgebung.
Kennwort überprüfen (Verify password)		Überprüft die Benutzereingabe für das Kennwort des WebSphere Application Server-Administrators.
Enable VNC	True	Dieser Wert ist gesperrt und kann nicht geändert werden.

DataPower-Teil

Das DataPower-Teil hat einige Konfigurationsoptionen.

Die konfigurierbaren Parameter des virtuellen Systemimages von DataPower werden in der folgenden Tabelle beschrieben:

Tabelle 8. Konfigurierte Parameter

Parametername	**Standardwert**	**Beschreibung**
Virtuelle CPUs (Virtual CPUs)	4	Die Anzahl der virtuellen Prozessoren, die für die durch diesen Teil dargestellte virtuelle Maschine zugeordnet werden.

Tabelle 8. Konfigurierte Parameter (Forts.)

Parametername	Standardwert	Beschreibung
Speicherkapazität (Memory size, MB)	4096	Die Speicherkapazität in MB, die dieser virtuellen Maschine zugeordnet wird.
Administratorkennwort (admin password)		Das Kennwort für den DataPower-Administrator.
Kennwort überprüfen (Verify password)		Überprüft die Benutzereingabe für das Administratorkennwort.
SSH aktivieren (Enable SSH)	True	Aktiviert SSH (zur Verwendung der DataPower-Befehlszeilenschnittstelle).
SSH-Port (SSH port)	22	Der Port für SSH.
XML-Managementschnittstelle aktivieren (Enable XML Management interface)	True	Aktiviert die XML-Managementschnittstelle. Wenn diese Option aktiviert ist, können Administratoren mit dieser Schnittstelle Status- und Konfigurationsanforderungen an das DataPower-Gerät über eine Standard-SOAP-Schnittstelle senden.
Port der XML Managementschnittstelle (XML Management Interface port)	5550	Der Port für die XML Managementschnittstelle.
Web-Management-Service aktivieren (Enable Web Management Service)	True	Aktiviert die Web-GUI für die Interaktion mit dem DataPower-Gerät.
Web-Service-Port (Web Service port)	9090	Der Port für die Web-GUI.
RAID-Verzeichnis (RAID directory)	raid0	Das Verzeichnis, in dem Sie auf Dateien im externen DataPower-Datenspeicher zugreifen können.

Scriptpakete

Im Lieferumfang von IBM SOA Policy Gateway Pattern sind sieben Scriptpakete enthalten.

In diesem Muster sind die folgenden Scriptpakete enthalten:

- 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

Die Scripts "Add Named Queries" und "Tear Down" enthalten keine vom Benutzer konfigurierbaren Parameter.

Script: SOA Policy Gateway 2.5.0.0 - DataPower Domain

Das DataPower Domain-Script stellt die DataPower-Domäne während der Implementierung bereit. Das Script konfiguriert die Verbindung zwischen der WSRR-Laufzeit und bis zu 10 (virtuellen) DataPower-Geräten.

Parameter

Tabelle 9. Konfigurierbare Parameter

Parametername	Standardwert	Beschreibung
DataPower_hostname	*Dieser Wert ist gesperrt und kann nicht geändert werden.*	Der Hostname für die DataPower-Instanz oder das DataPower-Gerät, die bzw. das überwacht werden soll.
DataPower_admin_id	*Dieser Wert ist gesperrt und kann nicht geändert werden.*	Die Administrator-ID für diese Instanz oder dieses Gerät.
DataPower_XML_mgmt_port	*Dieser Wert ist gesperrt und kann nicht geändert werden.*	Der Port für die Kommunikation mit der XML Management-Schnittstelle in der DataPower-Instanz oder im DataPower-Gerät.
DataPower_admin_password	*Dieser Wert ist gesperrt und kann nicht geändert werden.*	Das Kennwort für die Administrator-ID.
Kennwort überprüfen (Verify password)	*Dieser Wert ist gesperrt und kann nicht geändert werden.*	Geben Sie das Kennwort des Administrators erneut ein.
DataPower2_hostname	*Dieser Wert ist gesperrt und kann nicht geändert werden.*	
DataPower2_admin_id	*Dieser Wert ist gesperrt und kann nicht geändert werden.*	
DataPower2_XML_mgmt_port	*Dieser Wert ist gesperrt und kann nicht geändert werden.*	
DataPower2_admin_password	*Dieser Wert ist gesperrt und kann nicht geändert werden.*	
Kennwort überprüfen (Verify password)	*Dieser Wert ist gesperrt und kann nicht geändert werden.*	
...		...
DataPower10_hostname	*Dieser Wert ist gesperrt und kann nicht geändert werden.*	
DataPower10_admin_id	*Dieser Wert ist gesperrt und kann nicht geändert werden.*	
DataPower10_XML_mgmt_port	*Dieser Wert ist gesperrt und kann nicht geändert werden.*	
DataPower10_admin_password	*Dieser Wert ist gesperrt und kann nicht geändert werden.*	
Kennwort überprüfen (Verify password)	*Dieser Wert ist gesperrt und kann nicht geändert werden.*	

Tabelle 9. Konfigurierbare Parameter (Forts.)

Parametername	Standardwert	Beschreibung
New_DataPower_domain	Der Standardwert hängt vom Mustertyp ab: • SOAPolicyAdvancedRuntime • SOAPolicyBasicRuntime	Der neue Domänenname, der auf jedem DataPower-Gerät oder auf jeder DataPower-Instanz zu erstellen ist. Dieser Name darf mit keiner vorhandenen Domäne übereinstimmen. Andernfalls schlägt die Ausführung des Scriptpakets fehl oder es wird vorzeitig beendet. Der Wert darf keine Leerzeichen enthalten.
Remove_security_files	True	Zur Unterstützung der Verwendung können Sie diese Einstellung ignorieren.

Script: SOA Policy Gateway 2.5.0.0 - Promotion

Durch das Umstufungsscript 'Promotion' kann ein Basic Runtime-Muster oder Advanced Runtime-Muster in ein vorimplementiertes SOA Policy Gateway Governance Master-Muster integriert werden. Es richtet eine zellenübergreifende Sicherheit zwischen dem Laufzeitmuster (Runtime) und dem Governance-Muster ein. Optional kann es die WSRR-Umstufung in den Governance Master konfigurieren.

Parameter

Tabelle 10. Konfigurierbare Parameter

Parametername	Standardwert	Beschreibung
WSRR_GOV_DMGR_hostname		Der Hostname des Deployment Managers (Dmgr) für den WSRR-Cluster.
WSRR_GOV_DMGR_cellname	SOAPolicyGMCell	Der Zellenname für den WSRR-Cluster.
WSRR_GOV_admin_user	virtuser	Die Administrator-ID für die WSRR-Governance-Zelle
WSRR_GOV_admin_password		Das Kennwort für die Administrator-ID für die WSRR-Governance-Zelle.
Kennwort überprüfen (Verify password)		Überprüft die Benutzereingabe für "WSRR_GOV_admin_password".
Promotion_environment		Muss den Wert "staging", "production" oder "Unset" haben. Bei diesen Werten muss die Groß-/Kleinschreibung beachtet werden und sie müssen exakt übereinstimmen.

Tabelle 10. Konfigurierbare Parameter (Forts.)

Parametername	Standardwert	Beschreibung
LTPA_key_password		Ein LTPA-Schlüssel wird exportiert und während der Ausführung des Scriptpakets verwendet, das vom Governance Master stammt und in der Umstufungsumgebung über alle Zellen hinweg verwendet wird verwendet wird. Dies ist das Kennwort, das beim Exportieren dieses LTPA-Schlüssels verwendet wird.
Kennwort überprüfen (Verify password)		Überprüft die Benutzereingabe für "LTPA_key_password".

Script: SOA Policy Gateway 2.5.0.0 - Sample

Das Beispielscript 'Sample' konfiguriert die Beispielanwendungsparameter für die Verwendung mit dem SOA Policy Gateway Basic Runtime Sample-Muster.

Parameter

Keiner dieser Parameter kann vom Benutzer festgelegt werden.

Tabelle 11. Konfigurierbare Parameter

Parametername		Beschreibung
SCP_host	*Dieser Wert ist gesperrt und kann nicht geändert werden.*	
SCP_user	*Dieser Wert ist gesperrt und kann nicht geändert werden.*	
SCP_password	*Dieser Wert ist gesperrt und kann nicht geändert werden.*	
Kennwort überprüfen (Verify password)	*Dieser Wert ist gesperrt und kann nicht geändert werden.*	
SCP_zip_location	*Dieser Wert ist gesperrt und kann nicht geändert werden.*	
CLIENT_PUBLIC_KEY_file	*Dieser Wert ist gesperrt und kann nicht geändert werden.*	
CLIENT_PUBLIC _KEY_password	*Dieser Wert ist gesperrt und kann nicht geändert werden.*	
Kennwort überprüfen (Verify password)		
CLIENT_PRIVATE_KEY_file	*Dieser Wert ist gesperrt und kann nicht geändert werden.*	
CLIENT_PRIVATE_KEY_password	*Dieser Wert ist gesperrt und kann nicht geändert werden.*	
Kennwort überprüfen (Verify password)		
CLI_FILE_file	*Dieser Wert ist gesperrt und kann nicht geändert werden.*	
Kennwort überprüfen (Verify password)	*Dieser Wert ist gesperrt und kann nicht geändert werden.*	

Tabelle 11. Konfigurierbare Parameter (Forts.)

Parametername		**Beschreibung**
DataPower_hostname	*Dieser Wert ist gesperrt und kann nicht geändert werden.*	Der Hostname der DataPower-Instanz.
DataPower_XML_mgmt_port	*Dieser Wert ist gesperrt und kann nicht geändert werden.*	Der Port, der für DataPower XML Management Interface verwendet wird.
DataPower_admin_id	*Dieser Wert ist gesperrt und kann nicht geändert werden.*	Die Administrator-ID mit den entsprechenden Berechtigungen zur Verwendung von XML Management Interface.
DataPower_admin_password	*Dieser Wert ist gesperrt und kann nicht geändert werden.*	Das Kennwort für 'DataPower_admin_id'.
Kennwort überprüfen (Verify password)	*Dieser Wert ist gesperrt und kann nicht geändert werden.*	Überprüft die Benutzereingabe für 'DataPower_admin_password'.
SOAPolicySample_DataPower_domain	*Dieser Wert ist gesperrt und kann nicht geändert werden.*	Der Name der Beispieldomäne. Dieser Name darf mit keiner vorhandenen Domäne in der DataPower-Instanz übereinstimmen.
SamplePolicySample_starting_port	*Dieser Wert ist gesperrt und kann nicht geändert werden.*	Die Anwendung erfordert fünf freie Ports, die nacheinander beginnend mit der in diesem Wert angegebenen Portnummer verwendet werden. Beispiel: Wenn der Wert 62000 angegeben wird, werden die Ports 62000-62004 verwendet. Das Script überprüft nicht, ob die Ports frei sind.
LDAP_hostname	*Dieser Wert ist gesperrt und kann nicht geändert werden.*	Der Hostname des eigenständigen WSRR-Teils, wobei der LDAP-Server ebenfalls gehostet wird.
LDAP_port	*Dieser Wert ist gesperrt und kann nicht geändert werden.*	Der Port für den LDAP-Server.
LDAP_password	*Dieser Wert ist gesperrt und kann nicht geändert werden.*	Das Kennwort, das beim Binden mit dem LDAP_DN verwendet wird.
Kennwort überprüfen (Verify password)	*Dieser Wert ist gesperrt und kann nicht geändert werden.*	Überprüft die Benutzereingabe für 'LDAP_password'.
LDAP_DN	*Dieser Wert ist gesperrt und kann nicht geändert werden.*	Der definierte Name, der zum Binden an das LDAP verwendet wird.

Script: SOA Policy Gateway 2.5.0.0 - Security

Das Security-Script kopiert Sicherheitsinformationen (Zertifikate usw.) zwischen DataPower- und WSRR-Systemen im Muster.

Die Konfigurationsparameter für die Security-Script-Dateien dienen der Unterstützungsverwendung. Sie sollten die Standardwerte beibehalten.

Script: SOA Policy Gateway 2.5.0.0 - DataPower Monitoring (nur x86)

Das DataPower Monitoring-Script gibt die Verbindungsparameter für den DataPower Monitoring Shared Service an. Die ITCAM DataPower-Datenkollektoren und der Agent werden im Core OS-Teil ausgeführt.

Parameter

Der Überwachungsservice kann bis zu 10 virtuelle DataPower-Geräte überwachen.

Tabelle 12. Konfigurierbare Parameter

Parametername	Standardwert	Beschreibung
DataPower1_hostname		Der Hostname für das virtuelle DataPower-Gerät, das überwacht werden soll.
DataPower1_admin_id	admin	Die Administrator-ID für dieses virtuelle Gerät.
DataPower1_XML_mgmt_port	5550	Der Port für die Kommunikation mit der XML Management-Schnittstelle im virtuellen DataPower-Gerät.
DataPower1_admin_password		Das Kennwort für die Administrator-ID.
Kennwort überprüfen (Verify password)		Geben Sie das Kennwort des Administrators erneut ein.
DataPower2_hostname		
DataPower2_admin_id	admin	
DataPower2_XML_mgmt_port	5550	
DataPower2_admin_password		
Kennwort überprüfen (Verify password)		
...		...
DataPower10_hostname		
DataPower10_admin_id	admin	
DataPower10_XML_mgmt_port	5550	
DataPower10_admin_password		
Kennwort überprüfen (Verify password)		

Script: SOA Policy Gateway 2.5.0.0 - External DataPower Monitoring

Das DataPower Monitoring-Script gibt die Verbindungsparameter für den DataPower Monitoring Shared Service an. Die ITCAM DataPower-Datenkollektoren und der Agent werden im Core OS-Teil ausgeführt.

Parameter

Der Überwachungsservice kann bis zu 10 DataPower-Geräte überwachen.

Tabelle 13. Konfigurierbare Parameter

Parametername	**Standardwert**	**Beschreibung**
DataPower1_hostname		Der Hostname für das DataPower-Gerät, das überwacht werden soll.
DataPower1_admin_id	admin	Die Administrator-ID für dieses Gerät.
DataPower1_XML_mgmt_port	5550	Der Port für die Kommunikation mit der XML Management-Schnittstelle im DataPower-Gerät.
DataPower1_admin_password		Das Kennwort für die Administrator-ID.
Kennwort überprüfen (Verify password)		Geben Sie das Kennwort des Administrators erneut ein.
DataPower2_hostname		
DataPower2_admin_id	admin	
DataPower2_XML_mgmt_port	5550	
DataPower2_admin_password		
Kennwort überprüfen (Verify password)		
...		...
DataPower10_hostname		
DataPower10_admin_id	admin	
DataPower10_XML_mgmt_port	5550	
DataPower10_admin_password		
Kennwort überprüfen (Verify password)		

Kapitel 5. Mit IBM SOA Policy Gateway Pattern arbeiten

IBM SOA Policy Gateway Pattern stellt die Musterdefinitionen für eine wiederholbare Implementierung bereit. Diese Themen beschreiben, wie Muster implementiert werden.

Im Rahmen des Implementierungsprozesses konfigurieren Sie die Parameter der Teile. Weitere Informationen finden Sie in „Muster implementieren" auf Seite 49. Die Muster werden in Kapitel 4, „Muster, Teile und Scriptpakete", auf Seite 19 beschrieben.

Zugehörige Tasks:

Kapitel 3, „Erste Schritte mit IBM SOA Policy Gateway Pattern", auf Seite 13
Dieses Muster verwendet WebSphere DataPower zur Steuerung von Nachrichten mithilfe geregelter Richtlinien und Servicedefinitionen in WSRR. Lesen Sie die Informationen in diesem Abschnitt, um sich mit dem Herunterladen und Installieren des Musters, mit der Überprüfung des Musters nach der Installation, mit dem Akzeptieren der Lizenzen und mit den beteiligten Benutzerrollen vertraut zu machen.

Musterkonfiguration und Mustervoraussetzungen planen

IBM SOA Policy Gateway Pattern stellt eine Möglichkeit zur Verfügung, schnell und zuverlässig eine Umgebung für die Governance von Servicedefinitionen und -richtlinien sowie zur Durchsetzung dieser Richtlinien bereitzustellen. Die Implementierung des Musters beginnt mit dem Governance Master. Anschließend erfolgt die Implementierung der Runtime-Muster.

IBM SOA Policy Gateway Pattern vorbereiten und implementieren

- Wenn Sie ein externes DataPower-Gerät verwenden, bereiten Sie das Gerät für eine Fernverwaltung vor. Weitere Informationen finden Sie in „Ein DataPower-Gerät für IBM SOA Policy Gateway Pattern konfigurieren" auf Seite 48.

Implementieren Sie das Governance Master-Muster wie folgt:

1. Implementieren Sie ein SOA Policy Gateway Governance Master-Muster. Warten Sie ab, bis die Implementierung abgeschlossen ist, bevor Sie Laufzeitmuster implementieren. Weitere Informationen finden Sie in „Das Governance Master-Muster implementieren" auf Seite 52.

Implementieren Sie die Laufzeitmuster:

1. Entscheiden Sie, ob ein Basic Runtime-Muster mit einer eigenständigen Umgebung oder ein Advanced Runtime-Muster mit einer Clusterumgebung benötigt wird.
2. Bestimmen Sie, wie viele DataPower-Instanzen oder -Geräte Ihre Laufzeitmuster benötigen.

   Muster, die DataPower-Geräte beinhalten, haben standardmäßig zwei DataPower-Instanzen. Sie können bis zu 10 DataPower-Instanzen konfigurieren. Weitere Informationen finden Sie in „Einem Muster DataPower-Instanzen hinzufügen" auf Seite 58.

Muster mit externen DataPower-Geräten können für die Arbeit mit bis zu 10 DataPower-Geräten konfiguriert werden. Siehe „Die Basic und Advanced External DataPower-Muster implementieren" auf Seite 59.

Anmerkung: Es können keine zusätzlichen DataPower-Instanzen und -Geräte nach Abschluss dieser Konfiguration hinzugefügt werden.

3. Konfigurieren Sie das Laufzeitmuster mit den Informationen des Governance Master-Musters. Weitere Informationen finden Sie in „Implementierungsinformationen zum SOA Policy Gateway Governance Master" auf Seite 53. Sie können Governance Master-Musterinformationen ausschließen, um bei Bedarf ein eigenständiges System zu implementieren. (Es wird ein Implementierungsfehler angezeigt, der ignoriert werden kann.)
4. Geben Sie an, ob das Laufzeitsystem eine Stagingumgebung oder Produktionsumgebung ist.
5. Implementieren Sie Ihr Muster. Weitere Informationen finden Sie in „Ein Advanced Runtime-Muster implementieren" auf Seite 55 bzw. „Ein Basic Runtime-Muster implementieren" auf Seite 54.
6. Warten Sie ab, bis die Implementierung vollständig abgeschlossen ist, bevor Sie eine weitere Laufzeit implementieren.

Nach Abschluss der Implementierung der Laufzeitmuster gilt für die Umgebung Folgendes:

1. WSRR und die WebSphere-Sicherheit können über die Standardsicherheitskonfiguration aktualisiert werden. Weitere Informationen finden Sie in „Sicherheit für die IBM SOA Policy Gateway Pattern-Muster" auf Seite 49.
2. Die DataPower-Domäne ist für die Gateway-Konfiguration bereit. Sie müssen bei der Verwendung eines virtuellen DataPower-Geräts zunächst das aktuelle Fixpack anwenden. Siehe „DataPower in einer implementierten Instanz aktualisieren" auf Seite 57.

Ein DataPower-Gerät für IBM SOA Policy Gateway Pattern konfigurieren

Führen Sie die folgenden Schritte zur Konfiguration von DataPower aus, bevor Sie die SOA Policy-Scripts ausführen.

Vorgehensweise

1. Melden Sie sich als Administrator an der DataPower-Geräte-Web-GUI an.
2. Suchen Sie nach `XML Management Interface`.
3. Stellen Sie sicher, dass es aktiviert ('enabled') ist.
4. Stellen Sie sicher, dass die folgenden Elemente aktiv und ordnungsgemäß geschützt sind:
   - SOAP-Management-URI
   - SOAP-Konfigurationsmanagement
   - SOAP-Konfigurationsmanagement (v2004)
   - AMP-Endpunkt
   - SLM-Endpunkt
   - WS-Management-Endpunkt
   - WSDM-Endpunkt
   - UDDI-Subskription

- WSRR-Subskription

Sicherheit für die IBM SOA Policy Gateway Pattern-Muster

Eine gegenseitige Authentifizierung tritt zwischen den DataPower-Anwendungen und den Scripts in den Basic- und Advanced-Mustern auf. Die Scripts führen den notwendigen Austausch der Zertifikate durch. Beachten Sie, dass die Standard-SSL-Zertifikate, die im Lieferumfang des Musters enthalten sind, zu dem Host hinzugefügt werden, der für die Erstellung des Musters verwendet wurde.

Höhere Sicherheit

Für die WSRR-Images und die WebSphere Application Server-Images, die in den Mustern verwendet werden, werden nur die Standardsicherheitseinstellungen konfiguriert. Um eine sicherere Umgebung herzustellen, können Sie diese mit den Standardverfahren der WebSphere Application Server-Sicherheit schützen.

Informationen dazu finden Sie im Information Center von WebSphere Network Deployment Version 8.0 unter den folgenden Links:

- WebSphere Application Server, Network Deployment (verteilte Plattformen und Windows), Version 8.0: Information Center von IBM WebSphere Application Server, Network Deployment (verteilte Plattformen und Windows), Version 8.0
- Anwendungssicherheit: Information Center von IBM WebSphere Application Server, Network Deployment (verteilte Plattformen und Windows), Version 8.0 - Anwendungen und ihre Umgebung schützen
- Durchgängige Pfade für die Sicherheit: Information Center von IBM WebSphere Application Server, Network Deployment (verteilte Plattformen und Windows), Version 8.0 - Anwendungen und ihre Umgebung schützen

Muster implementieren

Durch die Implementierung von Mustern mit IBM PureApplication System in der Cloud wird eine aktive SOA Policy Gateway-Umgebung bereitgestellt. Sie können die vordefinierten Muster implementieren, die mit den IBM SOA Policy Gateway Pattern-Images bereitgestellt werden, oder Muster implementieren, die Sie selbst erstellt haben.

Vorbereitende Schritte

Zur Implementierung eines Musters müssen Sie zunächst ein vordefiniertes Muster oder ein neues Muster haben, das vollständig mit allen erforderlichen Teilen konfiguriert ist. Sie benötigen Informationen zur Umgebung, zur Cloudgruppe und zur IP-Gruppe, die von Ihrem PureAS-Systemadministrator implementiert werden.

Informationen zu diesem Vorgang

Sie implementieren das Muster mithilfe der Workload Console.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um die Muster von IBM SOA Policy Gateway Pattern zur Ausführung in Ihrer privaten Cloud zu implementieren:

1. Wählen Sie in der Liste der Muster im Fenster **Virtual System Patterns** das zu implementierende Muster aus.
2. Klicken Sie auf das Symbol zum Implementieren (**Deploy**).

3. Füllen Sie die erforderlichen Felder aus, um das Muster zu implementieren. Geben Sie im Fenster einen Namen für das virtuelle System sowie alle weiteren erforderlichen Informationen ein. Ein Häkchen neben einem Element weist darauf hin, dass es keine weitere Konfiguration erfordert. Sie können die Parameter für konfigurierte Teile vor der Implementierung des Musters ändern, indem Sie auf den Namen eines Teils klicken, um den Editor für den Teil zu öffnen. Virtuelle Maschinen werden in der erforderlichen Reihenfolge erstellt und anschließend gestartet.

Ergebnisse

Der Implementierungsprozess erstellt und startet virtuelle Maschinen für die definierten Teile und stellt Links zu den erforderlichen Konsolen bereit. Der Zeitaufwand für die Implementierung hängt von der Komplexität des Musters ab, das implementiert wird. Ein implementiertes Muster ist ein virtuelles System bzw. eine neu bereitgestellte IBM SOA Policy Gateway Pattern-Laufzeitumgebung.

Nächste Schritte

Über das Fenster **Virtual System Instances** können Sie den Status für Ihre Instanz anzeigen, um festzustellen, wann die Implementierung abgeschlossen ist, und mit der Verwaltung der Instanz beginnen.

Zugehörige Informationen:

IBM PureApplication System: Virtuelle Systemmuster verwalten

Den System Monitoring Shared Service implementieren

Mit der Implementierung des Shared Service 'System Monitoring for SOA Policy Gateway' werden die Überwachungskomponenten für Ihr virtuelles System bereitgestellt.

Vorbereitende Schritte

Der PureAS-Systemadministrator muss den System Monitoring Shared Service starten und Sie über die Cloudgruppe und Umgebung, in denen er gestartet wird, informieren. Sie müssen dieselbe Cloudgruppe und Umgebung verwenden, um den SOA Policy Gateway System Monitoring Shared Service und Ihre Laufzeit und Governance-Muster zu implementieren.

Für das Überwachen der WSRR-Instanzen ist es außerdem erforderlich, dass der Shared Service 'System Monitoring for WebSphere Application Server' gestartet wird. Stellen Sie also sicher, dass er auf Ihrem PureAS-System vorhanden ist.

Vorgehensweise

Führen Sie die folgenden Schritte in der Workload Console aus:

1. Klicken Sie auf **Instances** > **Shared Services**.
2. Überprüfen Sie, dass der Monitoring Shared Service in der Cloudgruppe ausgeführt wird, in der Ihre Muster implementiert werden. Wenn er nicht ausgeführt wird, wenden Sie sich diesbezüglich an Ihren PureAS-Administrator.
3. Gehen Sie wie folgt vor, um den DataPower Monitoring Shared Service zu aktivieren:
   a. Klicken Sie auf **Cloud** > **Pattern Types**.

b. Wählen Sie den Eintrag **System Monitoring for SOA Policy Gateway Pattern 2.5.0.0** im Fenster **Pattern Types** aus.
c. Klicken Sie auf **Enable** im Feld **Status** und warten Sie, bis sich das Statusfeld zu **Disable** ändert.

4. Gehen Sie wie folgt vor, um den WebSphere Application Server Monitoring Shared Service zu starten:
   a. Klicken Sie auf **Instances** > **Shared Services**.
   b. Klicken Sie auf das Pluszeichen im Fenster **Shared Service Instances**, um das Fenster **Deploy Shared Service** zu öffnen.
   c. Wählen Sie **System Monitoring for WebSphere Application Server** aus und klicken Sie auf **OK**.
   d. Geben Sie im Fenster **Configure and Deploy a Shared Service** ein, ob der Service auf zuvor implementierten Mustern gestartet werden soll, indem Sie die unteren zwei Kontrollkästchen aktivieren. Klicken Sie auf **OK**.
   e. Geben Sie im Fenster **Deploy Virtual Application** die Option **Target cloud group**, **IP group** und **Profile** an, wie von Ihrem PureAS-Administrator vorgegeben. Diese Optionen müssen mit denen Ihrer virtuellen Systeme übereinstimmen.
5. Gehen Sie wie folgt vor, um den WebSphere DataPower Monitoring Shared Service zu starten:
   a. Klicken Sie in der Menüleiste auf **Instances** > **Shared Services**.
   b. Klicken Sie auf das Pluszeichen im Fenster **Shared Service Instances**, um das Fenster **Deploy Shared Service** zu öffnen.
   c. Wählen Sie aus der Liste **System Monitoring for WebSphere DataPower** aus und klicken Sie auf **OK**.
   d. Geben Sie im Fenster **Configure and deploy a shared service** ein, ob die Überwachung auf zuvor implementierten Mustern gestartet werden soll, indem Sie die unteren zwei Kontrollkästchen aktivieren. Klicken Sie auf **OK**.
   e. Geben Sie im Fenster **Deploy Virtual Application** die Option **Target cloud group**, **IP group** und **Profile** an, wie von Ihrem PureAS-Administrator vorgegeben. Diese Optionen müssen mit denen Ihrer virtuellen Systeme übereinstimmen.
   f. Generieren und speichern Sie einen SSH-Schlüssel, wenn Sie Debugzugriff auf den Monitoring Shared Service benötigen.
   g. Klicken Sie auf **OK**.

Ergebnisse

Der System Monitoring for WebSphere DataPower Shared Service wird als ausgeführt angezeigt. Der Shared Service 'System Monitoring for WebSphere Application Server' wird als ausgeführt angezeigt.

Nächste Schritte

Informationen zur Überprüfung der Implementierung finden Sie in „Implementierung überprüfen" auf Seite 57.

Das Basic Runtime Sample-Muster implementieren

Durch die Implementierung des SOA Policy Gateway Basic Runtime Sample-Musters wird eine aktive virtuelle Systeminstanz des Musters erstellt. Dieses Muster ist nur auf x86-Systemen verfügbar.

Informationen zu diesem Vorgang

Durch die Implementierung eines Musters wird eine virtuelle Systeminstanz erstellt, die in der Cloud ausgeführt wird.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um das SOA Policy Gateway Basic Runtime Sample-Muster zu implementieren:

1. Klicken Sie in der Workload Console auf **Patterns** > **Virtual Systems**.
2. Wählen Sie in der Liste 'Virtual System Patterns' den Eintrag **SOA Policy Gateway 2.5.0.0 - Basic Runtime Sample** aus.
3. Klicken Sie auf das Symbol zum Implementieren (**Deploy**).
4. Füllen Sie die erforderlichen Felder aus, um das Muster zu implementieren. Ein Häkchen neben einem Element weist darauf hin, dass es keine weitere Konfiguration erfordert.
   a. Geben Sie im Feld **Virtual system name** einen eindeutigen Namen für die Instanz ein.
   b. Erweitern Sie den Abschnitt **Choose Environment** und geben Sie das Profil (**Profile**) an, wie von Ihrem PureAS-Systemadministrator vorgegeben.
   c. Konfigurieren Sie die virtuellen Muster. Klicken Sie auf **Configure virtual parts** und anschließend auf den Namen des Teils, um den Editor für Teile und Scripts zu öffnen. Geben Sie die Cloudgruppe (**Cloud group**) und die IP-Gruppe (**IP group**) an, wie von Ihrem PureAS-Systemadministrator vorgegeben. Details zu den musterspezifischen und scriptspezifischen Konfigurationsparametern finden Sie in den folgenden Themen.

      Anmerkung: Für alle Kennwörter in diesem Muster wird der Standardwert `password` verwendet.

      - „DataPower-Teil" auf Seite 38
      - „DB2 Enterprise-Teil" auf Seite 30.
      - „Teil für eigenständigen WSRR-Server" auf Seite 36
      - „Script: SOA Policy Gateway 2.5.0.0 - Sample" auf Seite 42
5. Klicken Sie auf **OK**, um das Muster zu implementieren.

Nächste Schritte

Informationen zur Überprüfung der Implementierung finden Sie in „Implementierung überprüfen" auf Seite 57.

Das Governance Master-Muster implementieren

Durch die Implementierung des SOA Policy Gateway Governance Master-Musters wird eine aktive virtuelle Systeminstanz des Musters erstellt.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um das SOA Policy Gateway Governance Master-Muster zu implementieren:

1. Klicken Sie in der Workload Console auf **Patterns** > **Virtual Systems**.
2. Wählen Sie in der Liste "Virtual System Patterns" die Option **SOA Policy Gateway 2.5.0.0 - Governance Master** aus.
3. Klicken Sie auf das Symbol zum Implementieren (**Deploy**).

4. Füllen Sie die Felder aus, um das Muster zu implementieren. Ein Häkchen neben einem Element weist darauf hin, dass es keine weitere Konfiguration erfordert.
   a. Geben Sie im Feld **Virtual system name** einen eindeutigen Namen für die Instanz ein.
   b. Erweitern Sie den Abschnitt **Choose Environment** und geben Sie das Profil (**Profile**) an, wie von Ihrem PureAS-Systemadministrator vorgegeben.
   c. Konfigurieren Sie die virtuellen Muster. Klicken Sie auf **Configure virtual parts** und anschließend auf den Namen des Teils, um den Editor für Teile und Scripts zu öffnen. Geben Sie die Cloudgruppe (**Cloud group**) und die IP-Gruppe (**IP group**) an, wie von Ihrem PureAS-Systemadministrator vorgegeben. Details zu den musterspezifischen und scriptspezifischen Konfigurationsparametern finden Sie in den folgenden Themen.
      - „Teil für DB2 Enterprise-HADR-Primärdatenbank" auf Seite 32
      - „WSRR-Deployment Manager-Teil" auf Seite 37
      - „Teil für angepasste WSRR-Knoten" auf Seite 37
      - „Teil für DB2 Enterprise-HADR-Bereitschaftsdatenbank" auf Seite 34
5. Klicken Sie auf **OK**, um das Muster zu implementieren.

Nächste Schritte

Informationen zur Überprüfung der Implementierung finden Sie in „Implementierung überprüfen" auf Seite 57.

Implementierungsinformationen zum SOA Policy Gateway Governance Master

Governance Master muss vor der Implementierung der Runtime-Muster implementiert werden.

Informationen zu diesem Vorgang

Implementierungsinformationen aus der Governance Master-Instanz sind als Eingabe für Implementierungswerte für die Runtime-Muster erforderlich.

Vorgehensweise

Gehen Sie wie folgt vor, um die erforderlichen Werte aus der Governance Master-Instanz zu ermitteln:

1. Navigieren Sie zu **Instances** > **Virtual Systems**.
2. Wählen Sie die Governance Master-Instanz der Implementierung aus.
3. Erweitern Sie **Virtual machines**.
4. Erweitern Sie die virtuelle Maschine mit dem Namen ***WSRRDMGR***.
5. Beachten Sie die folgenden Punkte:
   - Notieren Sie den Hostnamen und die IP-Adresse im Abschnitt **Hardware and network**. Der Hostname ist der Wert in **Network interface 0**.
   - Notieren Sie den Zellennamen im Abschnitt **WebSphere configuration**.

   Der Hostname bzw. die IP-Adresse, der Zellenname und der Name des WebSphere-Administrators mit zugehörigem Kennwort, die bei der Implementierung der Governance Master-Instanz verwendet wurden, sind erforderliche Eingaben für die folgenden Parameter im Runtime-Muster:
   - WSRR_GOV_DMGR_hostname
   - WSRR_GOV_DMGR_cellname

- WSRR_GOV_admin_user
- WSRR_GOV_admin_password

Wenn Sie ein Runtime-Muster als Standalone-System implementieren möchten, können Sie diese Parameter auf „Unset" festlegen. Mit dieser Einstellung wird die Implementierung als **fehlgeschlagen** in **Virtual System** > **Instances** angezeigt, da das Promotion-Scriptpaket fehlschlägt. Die Implementierung kann jedoch weiterhin verwendet werden.

Ein Basic Runtime-Muster implementieren

Durch die Implementierung des Basic Runtime-Musters wird eine aktive virtuelle Systeminstanz des Musters erstellt.

Vorbereitende Schritte

Führen Sie die folgenden Tasks aus, bevor Sie das Basic Runtime-Muster implementieren:

- Wenn Sie ein Basic Runtime-Muster mit einem externen DataPower-Gerät implementieren, konfigurieren Sie Ihre DataPower-Geräte für IBM SOA Policy Gateway Pattern; siehe „Ein DataPower-Gerät für IBM SOA Policy Gateway Pattern konfigurieren" auf Seite 48. Auf Power-Systemen wird nur ein externes DataPower-Gerät implementiert.
- Stellen Sie die Implementierungsinformationen zum Governance Master zusammen (siehe „Implementierungsinformationen zum SOA Policy Gateway Governance Master" auf Seite 53).

Informationen zu diesem Vorgang

Durch die Implementierung eines Musters wird eine virtuelle Systeminstanz erstellt, die in der Cloud ausgeführt wird.

Anmerkung: Wenn Sie das Governance-Realisierungsprofil (GEP, Governance Enablement Profile) verwenden, können Sie nicht gleichzeitig eine Bereitstellungsumgebung und eine Produktionsumgebung in den Runtime-Mustern implementieren. Diese Einschränkung ist darauf zurückzuführen, dass während des Konfigurationsprozesses für die Umstufungseigenschaften (Promotion) ein Konflikt verursacht werden kann. Implementieren Sie die Bereitstellungsumgebung ('Staging') zuerst und anschließend die Produktionsumgebung.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um ein Basic Runtime-Muster zu implementieren:

1. Klicken Sie auf **Patterns** > **Virtual Systems**.
2. Wählen Sie in der Liste 'Virtual System Patterns' den Eintrag **SOA Policy Gateway 2.5.0.0 - Basic Runtime External DataPower** oder **SOA Policy Gateway 2.5.0.0 - Basic Runtime** aus.
3. Klicken Sie auf das Symbol zum Implementieren (**Deploy**).
4. Füllen Sie die erforderlichen Felder aus, um das Muster zu implementieren. Ein Häkchen neben einem Element weist darauf hin, dass es keine weitere Konfiguration erfordert.
   a. Geben Sie im Feld **Virtual system name** einen eindeutigen Namen für die Instanz ein.

b. Erweitern Sie den Abschnitt **Choose Environment** und geben Sie das Profil (**Profile**) an, wie von Ihrem PureAS-Systemadministrator vorgegeben.
c. Konfigurieren Sie die virtuellen Muster. Klicken Sie auf **Configure virtual parts** und anschließend auf den Namen des Teils, um den Editor für Teile und Scripts zu öffnen. Geben Sie die Cloudgruppe (**Cloud group**) und die IP-Gruppe (**IP group**) an, wie von Ihrem PureAS-Systemadministrator vorgegeben. Details zu den musterspezifischen und scriptspezifischen Konfigurationsparametern finden Sie in den folgenden Themen.

   Anmerkung: Wenn Sie das Muster ohne Governance Master implementieren möchten, geben Sie "Unset" als Parameter des Governance Master-Hostnamens ein. Beachten Sie, dass dies dazu führt, dass im Promotion-Scriptpaket die Implementierung als fehlgeschlagen gemeldet wird, aber keine weiteren Konsequenzen hat.

   - „DataPower-Teil" auf Seite 38
   - „DB2 Enterprise-Teil" auf Seite 30
   - „Teil für eigenständigen WSRR-Server" auf Seite 36
   - „Script: SOA Policy Gateway 2.5.0.0 - Security" auf Seite 43
   - „Script: SOA Policy Gateway 2.5.0.0 - Promotion" auf Seite 41
   - „Script: SOA Policy Gateway 2.5.0.0 - DataPower Domain" auf Seite 40
   - „Script: SOA Policy Gateway 2.5.0.0 - DataPower Monitoring (nur x86)" auf Seite 44

5. Klicken Sie auf **OK**, um das Muster zu implementieren.

Nächste Schritte

Informationen zur Überprüfung der Implementierung finden Sie in „Implementierung überprüfen" auf Seite 57.

Ein Advanced Runtime-Muster implementieren

Durch die Implementierung des Advanced Runtime-Musters wird eine aktive virtuelle Systeminstanz des Musters erstellt.

Vorbereitende Schritte

Führen Sie die folgenden Tasks aus, bevor Sie das Advanced Runtime-Muster implementieren:

- Wenn Sie ein Advanced Runtime-Muster mit einem externen DataPower-Gerät implementieren, konfigurieren Sie Ihre DataPower-Geräte für eine Verbindung mit dem Muster. Siehe „Ein DataPower-Gerät für IBM SOA Policy Gateway Pattern konfigurieren" auf Seite 48. Auf Power-Systemen wird nur ein externes DataPower-Gerät implementiert.
- Stellen Sie die Implementierungsinformationen zum Governance Master zusammen (siehe „Implementierungsinformationen zum SOA Policy Gateway Governance Master" auf Seite 53).

Informationen zu diesem Vorgang

Durch die Implementierung eines Musters wird eine virtuelle Systeminstanz erstellt, die in der Cloud ausgeführt wird.

Anmerkung: Wenn Sie das Governance-Realisierungsprofil (GEP, Governance Enablement Profile) verwenden, können Sie nicht gleichzeitig eine

Bereitstellungsumgebung und eine Produktionsumgebung in den Runtime-Mustern implementieren. Diese Einschränkung ist darauf zurückzuführen, dass während des Konfigurationsprozesses für die Umstufungseigenschaften (Promotion) ein Konflikt verursacht werden kann. Implementieren Sie die Bereitstellungsumgebung ('Staging') zuerst und anschließend die Produktionsumgebung.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um ein Advanced Runtime-Muster zu implementieren:

1. Klicken Sie auf **Patterns** > **Virtual Systems**.
2. Wählen Sie in der Liste 'Virtual System Patterns' den Eintrag **SOA Policy Gateway 2.5.0.0 - Advanced Runtime External DataPower** oder **SOA Policy Gateway 2.5.0.0 - Advanced Runtime** aus.
3. Klicken Sie auf das Symbol zum Implementieren (**Deploy**).
4. Füllen Sie die erforderlichen Felder aus, um das Muster zu implementieren. Ein Häkchen neben einem Element weist darauf hin, dass es keine weitere Konfiguration erfordert.
   a. Geben Sie im Feld **Virtual system name** einen eindeutigen Namen für die Instanz ein.
   b. Erweitern Sie den Abschnitt **Choose Environment** und geben Sie das Profil (**Profile**) an, wie von Ihrem PureAS-Systemadministrator vorgegeben.
   c. Konfigurieren Sie die virtuellen Muster. Klicken Sie auf **Configure virtual parts** und anschließend auf den Namen des Teils, um den Editor für Teile und Scripts zu öffnen. Geben Sie die Cloudgruppe (**Cloud group**) und die IP-Gruppe (**IP group**) an, wie von Ihrem PureAS-Systemadministrator vorgegeben. Details zu den musterspezifischen und scriptspezifischen Konfigurationsparametern finden Sie in den folgenden Themen.

      Anmerkung: Wenn Sie das Muster ohne Governance Master implementieren möchten, geben Sie "Unset" als Parameter des Governance Master-Hostnamens ein. Beachten Sie, dass dies dazu führt, dass im Promotion-Scriptpaket die Implementierung als fehlgeschlagen gemeldet wird, aber keine weiteren Konsequenzen hat.
      - „DataPower-Teil” auf Seite 38
      - „Teil für DB2 Enterprise-HADR-Primärdatenbank” auf Seite 32
      - „WSRR-Deployment Manager-Teil” auf Seite 37
      - „Script: SOA Policy Gateway 2.5.0.0 - Promotion” auf Seite 41
      - „Script: SOA Policy Gateway 2.5.0.0 - DataPower Domain” auf Seite 40
      - „Teil für angepasste WSRR-Knoten” auf Seite 37
      - „Teil für DB2 Enterprise-HADR-Bereitschaftsdatenbank” auf Seite 34
      - „Script: SOA Policy Gateway 2.5.0.0 - DataPower Monitoring (nur x86)” auf Seite 44
5. Klicken Sie auf **OK**, um die Implementierung auszuführen.

Nächste Schritte

Informationen zur Überprüfung der Implementierung finden Sie in „Implementierung überprüfen” auf Seite 57.

DataPower in einer implementierten Instanz aktualisieren

Nach der Implementierung eines Musters, das eine WebSphere DataPower-Komponente enthält, müssen Sie DataPower auf das aktuelle Fixpack aktualisieren.

Informationen zu diesem Vorgang

Sie aktualisieren DataPower, indem Sie das Fixpack von Fix Central herunterladen und es auf die DataPower-Web-GUI anwenden.

Vorgehensweise

1. Laden Sie das Aktualisierungspaket von Fix Central herunter:
   a. Suchen Sie in Fix Central nach den WebSphere DataPower-SOA-Geräten.
   b. Wählen Sie das Paket "XI52-virtual-6.0.0.1-Firmware" aus und laden Sie es herunter.
2. Stellen Sie eine Verbindung zur Web-GUI für die virtuelle DataPower-Maschine in Ihrem implementierten Muster her. Siehe „Verbindung zur Konsole einer virtuellen DataPower-Maschine herstellen" auf Seite 90.
3. Wählen Sie in der Systemsteuerung die Option **System Control** aus.
4. Suchen Sie den Abschnitt **Boot Image**.
5. Laden Sie auf das DataPower-Gerät die Datei `xi6001.scrypt4` aus dem heruntergeladenen Fixpack hoch. Verwenden Sie den File Managerin der DataPower-Web-GUI.
6. Wählen Sie das hochgeladene Script aus der Liste **Firmware File** aus.
7. Akzeptieren Sie die Lizenzbedingungen und klicken Sie auf **Boot Image**.
8. Folgen Sie den Eingabeaufforderungen, um das Fixpack zu installieren.

Implementierung überprüfen

Wenn Sie das Muster implementiert haben, überprüfen Sie, ob die Implementierung erfolgreich war.

Vorgehensweise

1. Überprüfen Sie die Implementierungsprotokolle auf Fehler im Verlauf der Implementierung der virtuellen Systeme. Weitere Informationen finden Sie in „Fehlerbehebung bei Problemen mit der Implementierung" auf Seite 109.
2. Optional: Wenn Sie SOA Policy Gateway Basic Runtime Sample implementiert haben, testen Sie die implementierte Instanz, indem Sie nach den Anweisungen des Lernprogramms einige Beispielnachrichten unter Verwendung der bereitgestellten Beispielanwendung senden. Siehe „Beispieltestfälle ausführen" auf Seite 64.

Eine zusätzliche Laufzeitumgebung hinzufügen

Das Governance-Realisierungsprofil (GEP, Governance Enablement Profile) wird mit einem vordefinierten Umgebungsklassifikationssystem geliefert, das vier unterschiedliche Umgebungen enthält: Entwicklung (Development), Test, Bereitstellung (Staging) und Produktion.

Informationen zu diesem Vorgang

Die Bereitstellungs- und Produktionsumgebung sind auch im SOA-Lebenszyklus codifiziert, der den Lebenszyklus von Funktionalitätsversionen, wie zum Beispiel

Serviceversionen, definiert. Es sind Zustände (Status) und Übergänge vorhanden, die für die Bereitstellungs- und die Produktionsumgebung spezifisch sind, sodass eine kontrollierte Umstufung (Promotion) in diese Laufzeitumgebungen durch Definieren der Zielsysteme in der Promotionskonfigurationsdatei ermöglicht wird. Diese Prozedur ist ein geeignetes Verfahren, wenn Ihr Unternehmen Umgebungen in derselben Weise definiert, wobei Bereitstellung (Staging) als eine Vor-Produktionsumgebung aufzufassen ist, in der Tests durchgeführt werden können, bevor die Funktionalitätsversion zur allgemeinen Verwendung geöffnet wird. Viele Unternehmen benötigen allerdings weitere Umgebungen, sodass Modifikationen im Profil erforderlich sind, um diesen Unterschieden Rechnung zu tragen. In diesem Abschnitt wird eine Möglichkeit beschrieben, eine neue Laufzeitumgebung in einem WSRR-Governance-Realisierungsprofil hinzuzufügen.

Weitere Informationen zur Planung einer Implementierungsumgebung finden Sie in „Musterkonfiguration und Mustervoraussetzungen planen" auf Seite 47.

Vorgehensweise

1. Implementieren Sie den SOA Policy Gateway Governance Master. Weitere Informationen finden Sie in „Das Governance Master-Muster implementieren" auf Seite 52.
2. Optional: Ändern Sie das WSRR-Governance-Realisierungsprofil. Weitere Informationen finden Sie im Information Center von IBM WebSphere Service Registry and Repository Version 8.0 - Lernprogramm: Laufzeitumgebungen anpassen.
3. Konfigurieren Sie die Basic Runtime-Muster oder Advanced Runtime-Muster mit den Governance Master-Details. Weitere Informationen finden Sie in „Implementierungsinformationen zum SOA Policy Gateway Governance Master" auf Seite 53.

   Anmerkung: Der Wert für die Umstufungsumgebung (Promotionsumgebung) muss auf „Unset" gesetzt werden.
4. Implementieren Sie die vordefinierten Basic Runtime-Muster oder Advanced Runtime-Muster. Weitere Informationen finden Sie in „Ein Basic Runtime-Muster implementieren" auf Seite 54 und „Ein Advanced Runtime-Muster implementieren" auf Seite 55.

Einem Muster DataPower-Instanzen hinzufügen

Basic- und Advanced-Muster mit internen DataPower-Instanzen haben standardmäßig zwei Instanzen. Jedes Muster kann insgesamt bis zu 10 DataPower-Instanzen haben.

Informationen zu diesem Vorgang

Die Muster selbst können nicht bearbeitet werden. Sie können dem Basic Runtime- oder Advanced Runtime-Mustern weitere DataPower-Instanzen hinzufügen, indem Sie eine Kopie des Musters erstellen und bearbeiten.

Vorgehensweise

1. Öffnen Sie das Muster in der Workload Console.
2. Klicken Sie auf **Clone** und geben Sie einen Namen für die Kopie des Muster an.
3. Klicken Sie auf **Edit**.

4. Ziehen Sie weitere DataPower-Teile aus der Teileliste, um sie dem Muster hinzuzufügen.
5. Klicken Sie auf **Done editing**.

DataPower-Instanzen aus einem Muster löschen

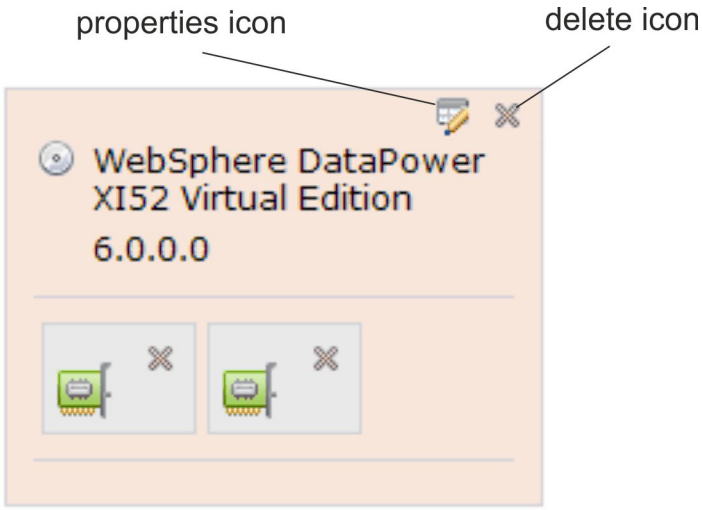
Sie können bei Bedarf aus einem Muster interne DataPower-Instanzen löschen.

Informationen zu diesem Vorgang

Die Muster selbst können nicht bearbeitet werden. Sie können aus den Basic Runtime- oder Advanced Runtime-Mustern DataPower-Instanzen löschen, indem Sie eine Kopie des Musters erstellen und bearbeiten.

Vorgehensweise

1. Öffnen Sie das Muster in der Workload Console.
2. Klicken Sie auf **Clone** und geben Sie einen Namen für die Kopie des Muster an.
3. Klicken Sie auf **Edit**.
4. Löschen Sie eine DataPower-Instanz, indem Sie auf das Löschsymbol klicken.



Anmerkung: Die DataPower-Instanzen müssen in umgekehrter numerischer Reihenfolge gelöscht werden. Jede DataPower-Instanz im Erstellungsbereich besitzt eine Zahl im Namensfeld, die angezeigt wird, wenn Sie auf das Eigenschaftensymbol klicken. Der Name hat das folgende Format: 'DataPower_XI52*x*', wobei *x* die Zahl ist. (Die erste DataPower-Instanz besitzt keine Zahl, sie hat den Namen 'DataPower_XI52'.) Die DataPower-Instanzen mit den höchsten Zahlen befinden sich in der Regel links oben im Erstellungsbereich.

5. Klicken Sie auf **Done editing**.

Die Basic und Advanced External DataPower-Muster implementieren

Die SOA Policy Gateway Basic Runtime External DataPower- und SOA Policy Gateway Advanced Runtime External DataPower-Muster können mit bis zu 10 DataPower-Geräten implementiert werden.

Informationen zu diesem Vorgang

Weitere Informationen zum Implementieren von Mustern finden Sie in „Ein Basic Runtime-Muster implementieren" auf Seite 54 oder „Ein Advanced Runtime-Muster implementieren" auf Seite 55. Weitere Informationen zu den Konfigurationsparametern, für die Sie Werte festlegen müssen, finden Sie in „Teil für eigenständigen WSRR-Server" auf Seite 36, „WSRR-Deployment Manager-Teil" auf Seite 37 und „Script: SOA Policy Gateway 2.5.0.0 - DataPower Monitoring (nur x86)" auf Seite 44.

Vorgehensweise

1. Implementieren Sie das Muster und klicken Sie auf **Configure virtual parts**.
2. Geben Sie für das eigenständige WSRR-Teil oder WSRR-Deployment Manager-Teil folgende Informationen für jedes Gerät ein:
   - DataPower_hostname
   - DataPower_XML_mgmt_port
   - DataPower_admin_id
   - DataPower_admin_password
   - Kennwort überprüfen (Verify password)
   - New_DataPower_domain

Beispielanwendung

Die Beispielanwendung besteht aus einem Web-Service und einer REST-konformer API, die beide in WSRR beschrieben und geregelt werden. Eine DataPower-Domäne wird mit WSRR als Gateway konfiguriert und ein Beispiel-Web-Client wird bereitgestellt, um die Services auszuführen.

Das Grundszenario in der Beispielanwendung ist eine Anwendung zur Warenbestandsführung für ein Geschäft ('Warehouse') und ein REST-konformer Service, der eine der Operationen für mobile Geräte dupliziert. Der Web-Service 'Store' besitzt drei Operationen:

- purchase (einkaufen)
- findInventory (Bestand ermitteln)
- returnProduct (Produkt zurückgeben)

Die letzte Operation 'findInventory' ist auch als REST-konformer Service verfügbar.

Der Beispiel-Web-Service

Die Basis-Service-Level-Definition (SLD) enthält zwei angehängte Mediationsrichtlinien:

- Überprüfung anhand der Datei 'Store.wsdl'. Dieses Beispiel basiert auf der Annahme, dass die DataPower-Validierung inaktiviert ist.
- Zurückweisung, wenn mehr als fünf Nachrichten in 90 Sekunden eingehen. Dieser Schwellenwert ist zu Demonstrationszwecken niedrig.

Der Konsument des Service 'Store' ist die Anwendung 'StoreConsumer', die die Konsumenten-ID „CEO" hat. Dieser Konsument hat zwei Service-Level-Agreements (SLAs): Gold und Silver. Wenn eine Anforderung bei DataPower mit der Konsumenten-ID „CEO" und der Kontext-ID „Silver" eingeht, ist das Durchlaufen der Anforderung zulässig, da die SLA 'Silver' vorhanden ist. Wenn die Konsumenten-ID „CEO" und die Kontext-ID „Gold" lautet, wird die SLA 'Gold'

abgeglichen. Dieser SLA ist eine Weiterleitungsrichtlinie angehängt, sodass die Anforderung an den alternativen Endpunkt weitergeleitet wird, der in der Richtlinie angegeben ist.

Wenn eine Anforderung mit einer anderen Konsumenten-ID als „CEO" eingeht, gibt es keine Anwendungsversion mit dieser Konsumenten-ID. Es gibt deshalb auch keine SLAs, die abgeglichen werden können. Dies ist daher eine Anforderung von einem anonymen Konsumenten. Es werden alle Richtlinien angewendet, die der anonymen SLA angehängt sind. In diesem Fall wird eine Benachrichtigung in den Protokollen angezeigt. Beachten Sie, dass das Beispiel keine Möglichkeit beinhaltet, eine Anforderung mit einer anderen Konsumenten-ID als „CEO" zu senden.

Das Szenario führt außerdem eine Autorisierung für die Operation 'findInventory' auf der Basis der Gruppenzugehörigkeit aus. Es wird ein LDAP-Server mit einem Beispiel für die Zuordnung von Benutzerberechtigungen zur richtigen Gruppe bereitgestellt.

Die Beispielanwendung zeigt den Ablauf der Anwendung, wobei jedes Feld ein anderes DataPower-Gateway darstellt.

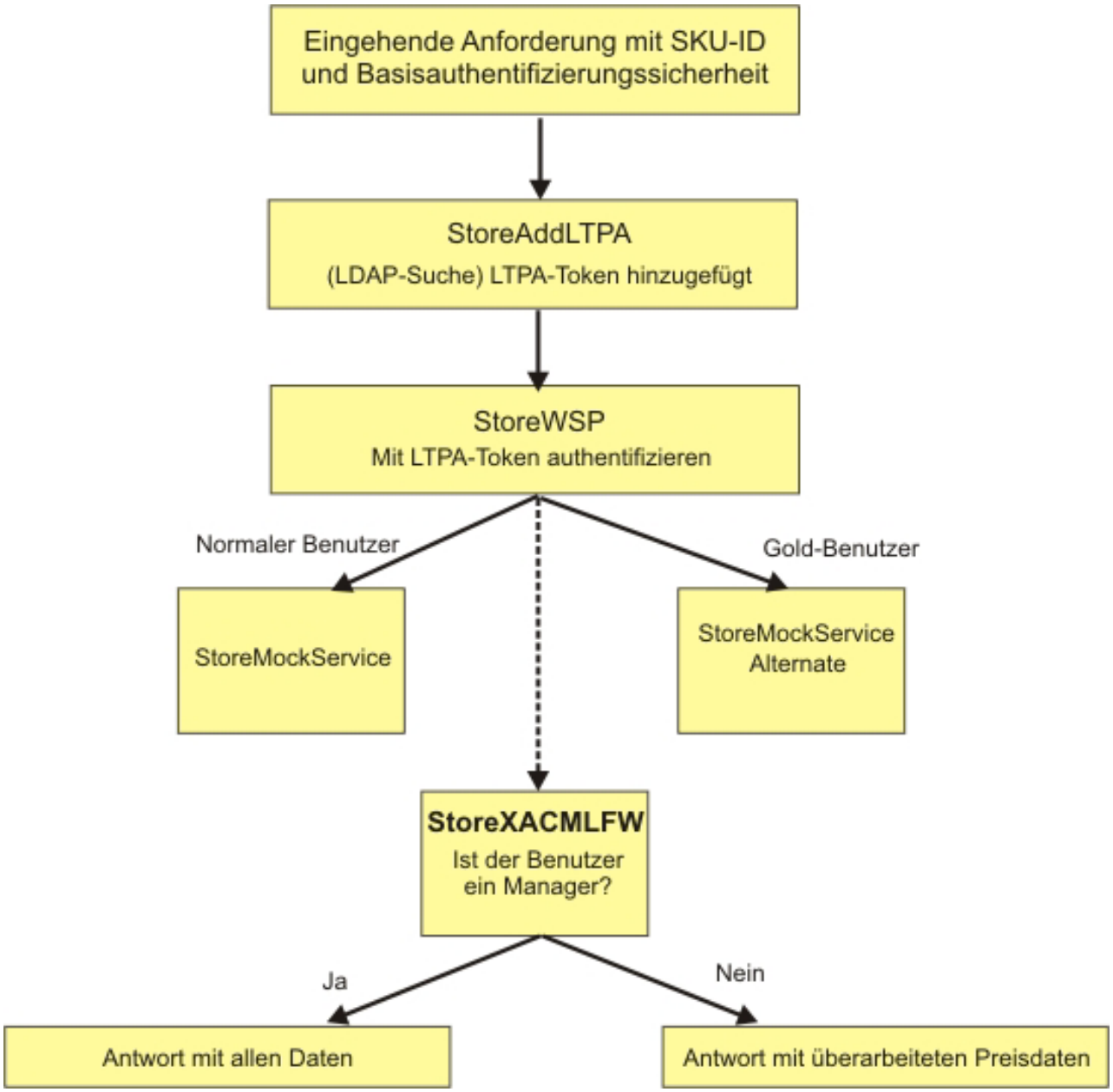


Abbildung 10. Ablaufdiagramm der Beispielanwendung

Der REST-konforme Beispiel-Service

Der REST-konforme Service wird auf ähnliche Weise geregelt wie der Web-Service, unterscheidet sich aber von ihm in der Art und Weise, wie Richtlinien verwendet werden. Wie beim Web-Service gibt es zwei SLAs: eine SLA für 'Silver'-Kunden und eine SLA für 'Gold'-Kunden. Beim REST-konformen Service gibt es jedoch keine Richtlinien, die auf SLD-Ebene (werden auf alle Anforderungen angewendet) angehängt sind. Stattdessen ist jeder SLA eine Richtlinie angehängt. Die SLA 'Gold' besitzt eine Richtlinie, die Nachrichten nach mehr als 5 Anforderungen in 90 Sekunden abweist, und die SLA 'Silver' lässt 2 Anforderungen in 90 Sekunden vor dem Abweisen zu.

Übersicht über die WSRR-Artefakte im Beispiel

Die WSRR-Artefakte, die den Service 'Store' beschreiben, werden hier beschrieben. Die Artefakte für den REST-Service folgen einem ähnlichen Muster.

Der Organisation 'Bob's Warehouse' gehören sowohl der bereitstellende Service 'Store' als auch die konsumierende Anwendung 'StoreConsumer'.

Der Geschäftsservice 'Warehouse' ist das Objekt, unter dem alle Versionen des Service 'Store' gehören. Die Version des Service 'Store' stellt eine besondere Version des Service 'Store' dar. Diese Version ist der Service, der für eine Wiederverwendung bereitgestellt wird. Die Service-Level-Definition 'Store SLD' sind zwei weitere Richtlinien zugeordnet: Die erste Richtlinie weist Nachrichten zurück, nachdem fünf Nachrichten innerhalb von 90 Sekunden eingegangen sind, und die zweite Richtlinie führt eine Prüfung anhand des in 'Store.wsdl' angegebenen Schemas aus. Diese Richtlinien bedeutet Folgendes: Anforderungen an den Service 'Store' werden überprüft und es werden in einem Zeitraum von 90 Sekunden maximal 5 Anforderungen an den Service weitergeleitet, unabhängig davon, von wem die Anforderung stammt. Die SLD besitzt außerdem eine anonyme Service-Level-Agreement (SLA). Alle Richtlinien, die dieser SLA angehängt sind, werden angewendet, wenn Anforderungen eintreffen, für die es keine übereinstimmenden SLAs gibt. Eine SLA stimmt überein, wenn folgende Bedingungen erfüllt sind:

- Es gibt eine konsumierende Anwendungsversion, die der Konsumenten-ID in der Anforderung entspricht.
- Es gibt eine SLA zwischen dieser konsumierenden Anwendungsversion und der SLD für den Service, der konsumiert wird und der der Kontext-ID in der Anforderung entspricht.

Die Geschäftsanwendung 'StoreConsumer' stellt die Anwendung 'StoreConsumer' dar, während die Anwendungsversion 'StoreConsumer' eine besondere Version dieser Anwendung ist. Diese Anwendung ist der Konsument: Sie verwendet den Service 'Store' wieder. Die Konsumenten-ID lautet „CEO”. Es gibt zwei SLAs für diese Anwendung, die eine Vereinbarung darstellt, sodass diese Anwendung den Service 'Store' konsumieren darf. Eine SLA hat die Kontext-ID „Gold”, das heißt, es stimmen Anforderungen der Anwendung 'StoreConsumer' überein, die die Kontext-ID „Gold” in der Anforderung haben. Die andere SLA stimmt mit 'Silver' überein. Die SLA 'Gold' besitzt eine angehängte Richtlinie zum Weiterleiten von Anforderungen, daher werden alle Anforderungen der Anwendung 'StoreConsumer' mit der Kontext-ID 'Gold' an den Endpunkt weitergeleitet, der in der Richtlinie angegeben ist. Der SLA 'Silver' sind keine Richtlinien angehängt, das heißt, Anforderungen der Anwendung 'StoreConsumer' mit der Kontext-ID 'Silver' werden weitergeleitet, obwohl keine Richtlinie angewendet wird.

In diesem Beispiel ist die Benachrichtigungsrichtlinie der anonymen SLA zugeordnet.

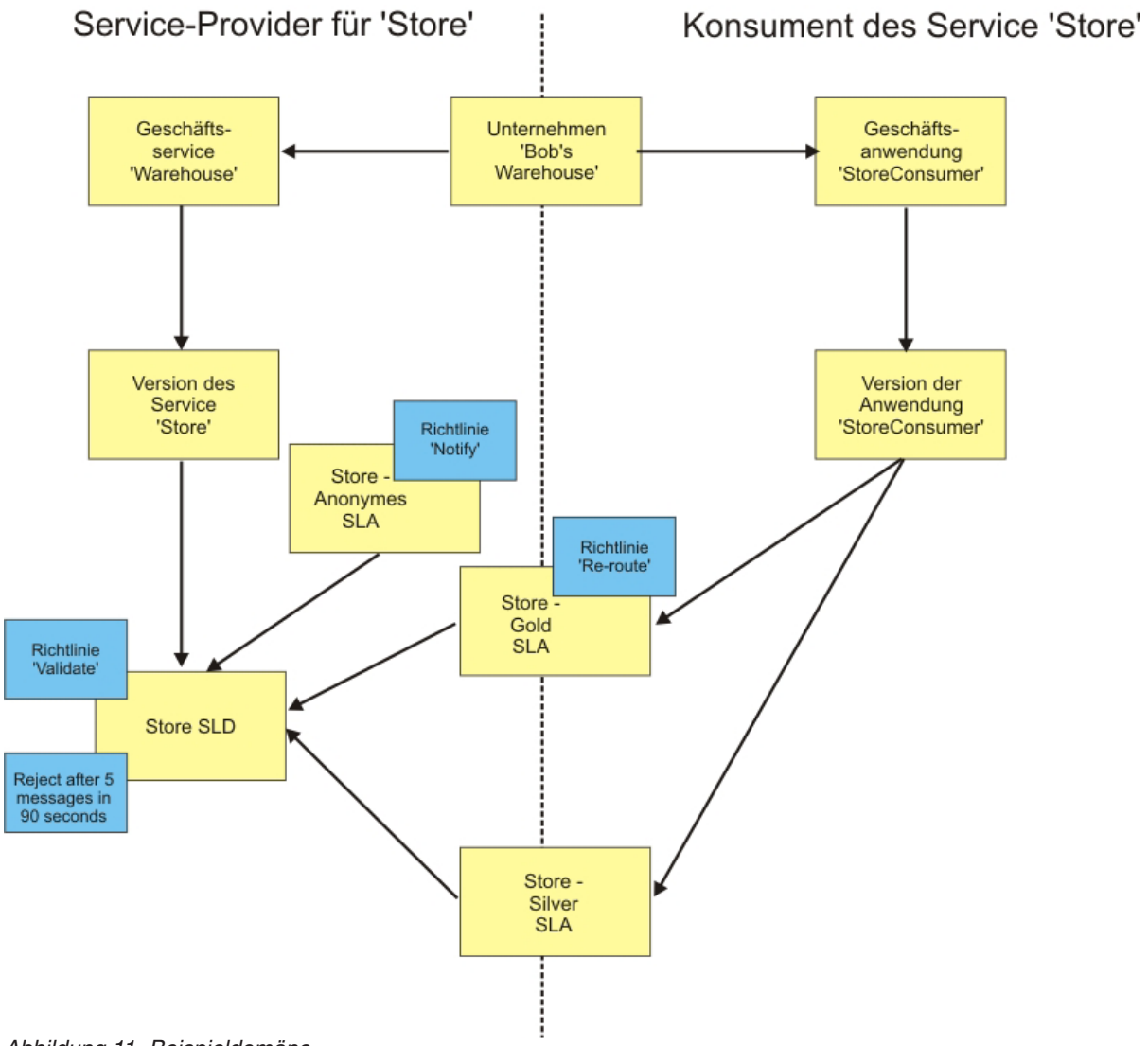


Abbildung 11. Beispieldomäne

Beispieltestfälle ausführen

Sie können die Anwendung 'Sample' im implementierten Muster von SOA Policy Gateway Basic Runtime Sample mithilfe einer Beispielwebanwendung oder über die Befehlszeile testen. Es stehen sechs Testvarianten für die Befehlszeile zur Verfügung, die für die Beispielanwendung ausgeführt werden können.

Informationen zur Implementierung von Basic Sample Runtime finden Sie in „Das Basic Runtime Sample-Muster implementieren" auf Seite 51.

Testfall für die Beispielwebanwendung ausführen

Gehen Sie wie folgt vor, um den Testfall für die Webanwendung ausführen:

1. Ermitteln Sie den Hostnamen der implementierten WSRR-Umgebung, indem Sie die implementierte virtuelle Systeminstanz öffnen. Um den Hostnahmen zu suchen, erweitern Sie den Abschnitt **Virtual machines** und wählen Sie die virtuelle Maschine für den eigenständigen WSRR-Server (WSRR Standalone

Server) aus, um die Details zur virtuellen Maschine anzuzeigen. Im Abschnitt **Hardware and network** ist der Hostname der Wert in **Network interface 0**.

2. Öffnen Sie die URL-Adresse in einem Web-Browser: `http://<wssrHostName>:9080/SoaPolicyTester`
3. Folgende Optionen sind verfügbar:
   - **Standard Request** - Sendet eine Anforderung 'findInventory' an den Service 'Store'. Die Kontext-ID ist 'Silver'. Die Konsumenten-ID ist 'CEO'. Ein erfolgreiches Ergebnis zeigt den Text „Part: SKU10 Price: 401.73" an.
   - **Routing Policy Test** - Wie bei 'Standard Request', jedoch lautet die Kontext-ID 'Gold'. Die Anforderung wird an einen alternativen Endpunkt weitergeleitet, der den Service ausführt. Ein erfolgreiches Ergebnis gibt „Part: GOLDSKU10 Price: 401.73" zurück.
   - **Validation Policy Test** - Sendet eine Anforderung mit ungültigen Nutzdaten. Die Prüfrichtlinie erfordert, dass DataPower die Anforderung überprüft und die ungültigen Nachrichten ablehnt. Ein erfolgreiches Ergebnis ist eine Antwortnachricht von DataPower `"Internal Error (from client)"`.
   - **REST Gold** - Sendet eine Anforderung an den REST-konformen Service mit der Konsumenten-ID "CEO" und der Kontext-ID "Gold". Gold-Anforderungen unterliegen einer Richtlinie, die nur 5 Nachrichten in 90 Sekunden zulässt. Eine erfolgreiche Anforderung zeigt „Part: SKU33 Price: 136.43" an.
   - **REST Silver** - Wie "Rest GOLD", aber mit der Kontext-ID "Silver". Silver-Anforderungen lassen 3 separate Anforderungen in 90 Sekunden zu. Eine erfolgreiche Anforderung zeigt „Part: SKU33 Price: 136.43" an.
   - **User ID** - Die Option "User ID" hat zwei mögliche Werte: "Full Content" oder "Redacted Content". Jede Option ergibt Anforderungen, die von verschiedenen Benutzern stammen. Das Beispiel verwendet eine XACML-Richtlinie, mit der nur Manager den Preis sehen können. Der Wert von 'Price' in der Antwortnachricht wird überarbeitet es sei denn, "Full Content" wurde ausgewählt. Ein erfolgreiches Ergebnis für Anforderungen, wenn "Redacted Content" ausgewählt wurde, ist „Price: 0.0". Der REST-konforme Service unterstützt die Überarbeitung nicht. Der ausgewählte Benutzer hat keine Auswirkungen.
4. Öffnen Sie die WSRR-Konsole und untersuchen Sie den Service und die Richtlinien. Weitere Informationen finden Sie in „Verbindung zu WSRR herstellen - Business Space" auf Seite 86.

Das Beispiel kann auch über die Befehlszeile ausgeführt werden. Dies ist die einzige Möglichkeit, Datenverkehr zu senden, der eine anonyme SLA verwendet.

XACML-Permit/Deny-Richtlinien mit dem Überarbeitungsszenario über die Befehlszeile demonstrieren

Die das folgende Anforderungs-XML kann an den DataPower-Service 'StoreAddLTPA' gesendet werden:

```
<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>
```

Unter der Annahme, dass das Beispiel für das Anforderungs-XML in einer Datei mit dem Namen `silver.xml` enthalten ist, geben Sie den folgenden curl-Befehl ein:

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

In diesem Beispiel ist ConsumerX ein Manager, sodass die vollständigen Preisinformationen in der Antwort angezeigt werden:

```
<?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>
```

Überarbeitungsszenario über die Befehlszeile ausführen

Der Benutzer 'ConsumerA' ist kein Manager, sodass ihm eine andere Antwort zurückgegeben wird. Geben Sie den curl-Befehl ein:

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

Beachten Sie, dass in der Antwort der Preis überarbeitet wurde und nun mit 0.0 angegeben wird:

```
<?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>
```

Routing-Richtlinie über die Befehlszeile testen

Bei der Routing-Richtlinie, die der durchzusetzenden "Gold SLA" zugeordnet ist, müssen die Kontext-ID und die Konsumenten-ID übereinstimmen. In diesem Fall hat das SLA für Gold-Kunden die Kontext-ID "Gold" und die verwendete Serviceversion hat die Kosumenten-ID "CEO". Der Inhalt einer Beispielanforderung sieht wie folgt aus (Kontext-ID und Konsumenten-ID sind erforderlich):

```
<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>
```

Unter der Annahme, dass das Beispiel für das Anforderungs-XML in einer Datei mit dem Namen `gold.xml` enthalten ist, geben Sie den folgenden curl-Befehl ein:

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

Die Antwort sieht wie folgt aus:

```
<?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>
```

Beachten Sie, dass die zurückgegebene Antwort den Wert `GOLDSKU` als SKU-Wert enthält, was darauf hinweist, dass der Endpunkt für "Gold" verwendet wurde.

Prüfung des Schemas über die Befehlszeile testen

Die Prüfrichtlinie überprüft das Schema der Anforderung anhand der Datei 'Store.wsdl' und der zugeordneten Datei 'Company.xsd'.

Das folgende XML-Beispiel `badvalid.xml` zeigt eine Anforderung, die ungültig ist, weil der Hauptteil ein Element mit dem Namen `<skubad>` anstelle des geforderten Elements `<sku>` enthält:

```
<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>
```

Wenn Sie die folgende curl-Anforderung eingeben:

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

Der folgende Fehler wird angezeigt:

```
<?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>
```

Zurückweisung in der Mediationsrichtlinie über die Befehlszeile testen

Eine der Mediationsrichtlinien, die im Beispiel enthalten sind, testet die Zurückweisung, nachdem die Nachrichtenzählung 5-mal in 90 Sekunden ausgeführt wurde. Führen Sie den folgenden Befehl 6-mal aus:

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

Die Beispielanforderung sieht wie folgt aus:

```
<?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>
```

In diesem Fall ist ConsumerX ein Manager. Daher werden die vollständigen Preisinformationen für die ersten fünf Ausführungen zurückgegeben:

```
<?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>
```

Bei der sechsten Ausführung wird der folgende Fehler zurückgegeben:

```
<?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>
```

Anmerkung: Dieser Fehler wird möglicherweise früher angezeigt, wenn Sie andere Tests innerhalb des 90-Sekunden-Intervalls ausgeführt haben.

Benachrichtigung in der Mediationsrichtlinie über die Befehlszeile testen

Die Benachrichtigungsrichtlinie ist der anonymen SLA zugeordnet. Sie wird durchgesetzt, wenn eine Anforderung von einem Konsumenten eingeht, der keine SLA besitzt. In diesem Beispiel ist der einzige Konsument, der SLAs besitzt, ein "CEO", daher wird durch die Anforderung, die eine Konsumenten-ID hat, die auf etwas anderes festgelegt ist, die Richtlinie zur anonymen SLA durchgesetzt. In diesem Fall ist ConsumerX ein Manager, sodass die vollständigen Preisinformationen angezeigt werden:

Um diese Funktion über die Befehlszeile zu testen, erstellen Sie eine Datei mit dem Namen `anon.xml` , die das folgende XML enthält:

```
<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>
```

Geben Sie dann den folgenden Befehl ein:

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

Die folgende Nachricht wird im Standardprotokoll der Domäne ausgegeben:

```
Notify action triggered ('operation_38_2_sla1-1-filter_1-notify') from source policy ('LogEveryTime_287d0790-83d9-11e1-a2
```

Anmerkung: Die Protokollierung muss auf „notice" eingestellt sein, damit diese Nachricht angezeigt wird. Wenn dies nicht der Fall ist, klicken Sie auf das Symbol für Fehlerbehebung in der DataPower-Webkonsole. Ändern Sie im Abschnitt für

die Protokollierung ('Logging') den Wert für 'Log level' (Protokollierungsstufe) in „notice“ und klicken Sie auf **Set Log Level** (Protokollierungsstufe festlegen). Um das Protokoll zu suchen, kehren Sie zur Systemsteuerung zurück und klicken Sie auf das Symbol **View Logs**.

REST-konformen Service über die Befehlszeile testen

Sie können auf die REST-konforme Schnittstelle über die Befehlszeile mit dem curl-Befehl zugreifen. Mit dem Web-Client lässt die Kontext-ID "Gold" nur 5 Nachrichten pro 90 Sekunden und "Silver" nur 2 Nachrichten zu.

Um diese Funktion über die Befehlszeile zu testen, erstellen Sie eine Datei mit dem Namen "restRequest.xml", die das folgende XML enthält:

```
<?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>
```

Geben Sie dann den folgenden Befehl ein, um einen Test mit der Kontext-ID „Gold“ durchzuführen:

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

Um die Kontext-ID 'Silver' zu testen, verwenden Sie denselben Befehl, aber ersetzen Sie 'Gold' durch 'Silver'.

Die erfolgreiche Antwort ist:

```
<?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>
```

Wenn der Schwellenwert überschritten wurde, wird folgende Nachricht angezeigt:

```
<?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><
```

Um die anonyme SLA für den REST-konformen Service auszuführen, dem einfach eine Benachrichtigungsrichtlinie zugeordnet wurde, verwenden Sie eine andere Kontext-ID und Konsumenten-ID als die registrierten IDs. Die Benachrichtigung wird im DataPower-Protokoll angezeigt, wie im Web-Services-Beispiel bereits beschrieben wurde.

Zugehörige Tasks:

„Das Basic Runtime Sample-Muster implementieren“ auf Seite 51
Durch die Implementierung des SOA Policy Gateway Basic Runtime Sample-Musters wird eine aktive virtuelle Systeminstanz des Musters erstellt.

Dieses Muster ist nur auf x86-Systemen verfügbar.

Beispielanwendung erweitern

Die Beispielanwendung kann durch Modifikation des Style-Sheets für Bindungen und der XSL-Style-Sheets geändert werden.

Modifikationen am Style-Sheet für Bindungen

Die Variable 'xacml-subjects' wurde dem Style-Sheet `apil-xacml-binding-new.xsl` hinzugefügt. Sie beinhaltet die Erstellung des Betreffabschnitts ('Subjects') der Anforderung. Auf diese Variable wird später in der Datei `sendToPDP.xsl` zugegriffen.

```
<xsl:variable name="xacml-subjects">
  <xacml-context:Subject
  SubjectCategory="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject">
<!--
***********************************************
Ab hier: Verwenden Sie das MC-Ergebnis als Betreff.
***********************************************
```

sendToPDP.xsl

Dieses Style-Sheet ruft 'StoreXACMLFW' mithilfe von 'url-open' auf. Der Aufruf erfolgt in einer Box mit einer anderen XML-Firewall, sodass kein SSL-Proxy-Profil verwendet wird. Um den Richtlinienentscheidungspunkt (PDP) in eine andere DataPower-Box zu versetzen, kann ein SSL-Proxy-Profil erstellt und mit dem url-open-Aufruf verwendet werden.

```
<xsl:param name="resource" />
<!--
<xsl:variable name="incoming_resource">
<xsl:value-of select="$resource" />
</xsl:variable>
<xsl:message dp:priority="debug">
*********** AUFRUF VON PDP ERFOLGT für RESSOURCE 'equal' *************
<xsl:value-of select="$incoming_resource" />
</xsl:message>
-->
- <!--
Erstellung der XACML-Anforderung für Maskierung
-->
<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/enve
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">
- <!--
Kopieren in Subjects, die aus der AAA-Anforderungsverarbeitung gespeichert wurden
-->
<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>
- <!--
Verwenden von 'set-variable', sodass sie im Testmonitor (Probe) sichtbar ist, was nützlich ist.
-->
<dp:set-variable name="'var://context/snip/xacml/BacksideXacmlRequest'" value="$customized-request" />
- <!--
Aufzeichnen von XACML-REQUEST im Debugprotokoll
-->
<xsl:message dp:priority="debug">
<XACML-REQUEST>
<xsl:copy-of select="$customized-request" />
</XACML-REQUEST>
</xsl:message>
<xsl:variable name="headers">
<header name="SOAPAction">xacml:authorization</header>
</xsl:variable>
- <!--
Aufruf von XACML-PDP für Entscheidung
-->
<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>
- <!--
Verwenden von 'set-variable', sodass sie im Testmonitor (Probe) sichtbar ist, was nützlich ist.
-->
<dp:set-variable name="'var://context/snip/xacml/BacksideXacmlResponse'" value="$rtss-response" />
- <!--
Aufzeichnen von XACML-RESPONSE im Debugprotokoll
-->
<xsl:message dp:priority="debug">
<XACML-RESPONSE>
<xsl:value-of select="$rtss-response" />
</XACML-RESPONSE>
</xsl:message>
</xsl:template>
</xsl:stylesheet>
```

Beachten Sie die folgenden Punkte bei der Datei `sendToPDP.xsl`:

1. Das Style-Sheet ruft den Port für XACMLFW aus der Datei `soavars.xsl` ab.
2. Es wird erwartet, dass die Variable 'rtssResponse' genau das Format hat, das Runtime Security Services verwenden würden und somit auch das Format, das der PDP in der DataPower-Box verarbeiten kann.
3. Das Style-Sheet setzt eine SOAP-Anforderung zusammen. Die Betreffinformationen werden durch das vorherige Style-Sheet `apil-binding.xsl` konstruiert und durch die folgende copy-of-select-Anforderung abgerufen:

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

4. Die Aktion besteht einfach in der Anzeige der Aktion: <xacml-context:AttributeValue>View</xacml-context:AttributeValue>
5. Die Umgebung sind die Geschäftspreisdaten 'StorePriceData', die in der Terminologie von IBM Tivoli Security Policy Manager oder Runtime Security Services als Anwendungsobjekt (Application object) bezeichnet werden.

StorePrivateDataXACML.xml

Im folgenden Code wird das Richtlinien-Style-Sheet für die Überarbeitung (Redaktion) angezeigt.

```
<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>
```

Beachten Sie die folgenden Punkte:

- Die Rolle muss 'Manager' sein:

```
<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>
```

- Die Ressource muss 'PriceInfo' sein:

```
<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>
```

- Die Aktion muss 'View' sein:

```
<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>
```

Beispiel-XSL-Style-Sheets ändern

Sie können das Überarbeitungs-Style-Sheet (Redaktion) `noPriceInfo.xsl` ändern.

Vorgehensweise

Ändern Sie das Überarbeitungs-Style-Sheet (Redaktion).
Das Style-Sheet `noPriceInfo.xsl` enthält den folgenden Code, durch den alle Werte für den Preis durch Nullen ersetzt werden. Sie können der Überarbeitungslogik weitere Felder oder komplexere Transformationen hinzufügen, die mit Berechnungen zur Ermittlung von Feldwerten verbunden sind.

```
<!-- Felder nur für privaten Zugriff -->
<xsl:template match="price">
<price>0.0</price>
</xsl:template>
<xsl:template match="Price">
<Price>0.0</Price>
</xsl:template>
```

Später führt das Style-Sheet eine Identitätstransformation für alle anderen Elemente aus.

Weitere Erkundung des Beispiels

Wenn Sie mehr über das Beispiel erfahren möchten, können Sie den XACML-Richtlinienentscheidungspunkt (PDP) in DataPower konfigurieren und Richtliniendokumente bearbeiten.

XACML-PDP in DataPower ändern

Sie können versuchsweise die XACML-Informationen ändern, die für den Sicherheits-PDP (Richtlinienentscheidungspunkt) in DataPower verwendet werden, um sich eingehender mit der Zugriffssteuerung mithilfe von XACML vertraut zu machen.

Vorgehensweise

Gehen Sie wie folgt vor, um einen Richtlinienentscheidungspunkt (PDP) zu ändern oder hinzuzufügen:

1. Suchen Sie im Fenster 'DataPower Control Panel' nach `XACML PDP`.
2. Klicken Sie auf einen vorhandenen PDP oder klicken Sie auf **Add**.
3. Geben Sie eine URL ein. Beispiel: `local:///storePrivateDataXACML.xml`.
4. Fügen Sie abhängige Dateien oder Verzeichnisdateien hinzu, die zur Unterstützung der Richtlinie erforderlich sind.

Anmerkung: Wenn Sie eine XACML-Richtliniendatei direkt im Dateisystem bearbeiten, müssen Sie zu der PDP-Definition zurückkehren und die URL bzw. den geänderten Wert dafür erneut eingeben oder die Domäne erneut starten, damit die Änderung wirksam wird.

Neue Richtliniendokumente hinzufügen oder vorhandene bearbeiten

Verwenden Sie die Business Space-Benutzerschnittstelle, um neue Richtliniendokumente hinzuzufügen oder vorhandene zu bearbeiten.

Vorbereitende Schritte

Konfigurieren Sie den SOA-Governance-Space. Weitere Informationen finden Sie in „Business Space für die Erstverwendung konfigurieren" auf Seite 87.

Vorgehensweise

1. Erstellen Sie eine Mediationsrichtlinie mit den Bedingungen und Aktionen, die Sie benötigen. Beispiel: Eine Bedingung könnte 'Nachrichtenanzahl > 5 Nachrichten in 5 Minuten' sein, die zugehörige Aktion 'Zurückweisen' (reject). Weitere Informationen zur Erstellung einer Mediationsrichtlinie finden Sie in „Neue Mediationsrichtlinien erstellen" auf Seite 103.
2. Legen Sie Governance-Regeln für die Richtlinie fest. Weitere Informationen zur Governance eines Richtliniendokuments finden Sie in „Lebenszyklus der Richtlinie verwalten" auf Seite 106.
   a. Klicken Sie auf das Richtliniendokument im Service-Registry-Navigator oder suchen Sie das Dokument über das Suchwidget. Die Aktionen werden im Richtliniendokumenteditor angezeigt.
   b. Klicken Sie auf **Propose Specification** (Spezifikation vorschlagen).
   c. Klicken Sie auf **Approve Specification** (Spezifikation genehmigen).

   Die Richtlinie wurde genehmigt. Sie können die Richtlinie neu definieren, ersetzen oder aussetzen, um den Lebenszyklus zu verwalten, oder eine vorhandene Definition bearbeiten.
3. Ordnen Sie die Richtlinie zu. Suchen Sie in Business Space die SLD oder SLA, die Sie der Richtlinie zuordnen möchten. In diesem Beispiel können Sie das an vier Stellen tun:
   - Store SLD - Ordnen Sie Ihre Richtlinie hier zu, wenn Sie sie auf jede Store-Verwendung anwenden möchten.
   - Gold SLA - Ordnen Sie Ihre Richtlinie hier zu, wenn Sie sie nur auf Gold-Anforderungen vom Konsumenten "CEO" anwenden möchten.
   - Silver SLA - Ordnen Sie Ihre Richtlinie hier zu, wenn Sie sie nur auf Silver-Anforderungen vom Konsumenten "CEO" anwenden möchten.
   - Anonymous SLA - Ordnen Sie Ihre Richtlinie hier zu, wenn Sie sie auf alle Anforderungen von anderen Konsumenten als "CEO" anwenden möchten.

Zugehörige Tasks:

„Neue Mediationsrichtlinien erstellen" auf Seite 103
Sie können mit der Business Space-Benutzerschnittstelle neue Mediationsrichtlinien erstellen. Wenn Sie Mediationsrichtlinien verfassen, legen Sie die Bedingungen und Aktionen für die Richtlinie fest.

„Lebenszyklus der Richtlinie verwalten" auf Seite 106
Richtlinien können in der Business Space-Benutzerschnittstelle durch Übergänge von einem Governance-Zustand in einen anderen versetzt werden. Die Richtlinien müssen sich im Zustand 'Approved' befinden, damit sie von DataPower

durchgesetzt werden können.

Zugehörige Informationen:

Information Center von IBM WebSphere Service Registry and Repository Version 8.0 - Business Space-Benutzerschnittstelle verwenden

DataPower-Beispieldomäne

Das Muster stellt ein Beispiel für eine DataPower-Domäne bereit, mit dem Sie die Verwendung des Musters beginnen können. Als DataPower-Entwickler können Sie die vorhandenen Gateways als Schablonen für eigene Anwendungen verwenden. Die Beispielumgebung enthält fünf Gateways. Ein primäres Gateway ist für den Service 'Store' vorgesehen. Vier unterstützende Gateways stellen Beispiel-Back-Ends, die das Store-Gateway aufrufen kann, die XACML-Unterstützung für ein Überarbeitungsszenario (Redaktion) sowie ein Front-End bereit, um höhere Sicherheitsfunktionalität hinzuzufügen.

Web-Service-Proxy 'Store'

Der Web-Service-Proxy (WSP) 'Store' ist das primäre Gateway der Anwendungsdomäne. Er empfängt eine Anforderung mit einem angehängten LTPA-Token.

Bei Anforderung führt die Verarbeitungsregel für die Anforderung die folgenden Aktionen aus:

1. Sie prüft die Anforderung, wie dies durch die Prüfrichtlinie (Validation) angefordert wird. Weitere Informationen finden Sie in „Übersicht über die WSRR-Artefakte im Beispiel" auf Seite 63.
2. Sie leitet die Anforderung an den alternativen Endpunkt weiter, wenn das Service-Level-Agreement (SLA) die Benutzerkategorie „Gold" angibt.
3. Sie führt die Authentifizierung, die Autorisierung und die Abrechnung (AAA) für die Anforderung aus. Die Authentifizierung umfasst die folgenden Aktionen:
   a. Authentifizieren des Benutzers mit einem LTPA-Token.
   b. Zuordnen der Berechtigungsnachweise mithilfe des LDAP-Servers, der Informationen dazu bereitstellt, zu welcher Gruppe der Kunde gehört. Diese Gruppen sind 'Manager', 'Clerk' (Sachbearbeiter) und 'Customer' (Kunde).
   c. Umwandeln der angegebenen Eingaben in ein Anforderungsobjekt, das der XACML-Richtlinienentscheidungspunkt (PDP) verarbeiten kann.
   d. Ausführen der Autorisierung mithilfe eines XACML-PDP in der DataPower-Box mit einem XACML-Richtliniendokument, das in IBM Tivoli Security Policy Manager erstellt werden kann. Die Kriterien der Richtlinie legen fest, dass der Benutzer ein Manager, ein Kunde (Customer) oder ein Sachbearbeiter (Clerk) sein muss. Für die Operation 'findInventory' erfordern die Rückgaben entweder einen Manager oder einen Sachbearbeiter, während die Operation 'purchase' von Kunden ausgeführt werden kann.
4. Sie legt den Wert für ConsumerID mithilfe eines XSL-Scripts fest.
5. Sie entfernt den gesamten HTTP-Sicherheitsheader aus der Anforderung.
6. Sie ruft das Back-End für den Service 'Store' auf.

Wenn die Anforderung verarbeitet ist, führt die Antwortverarbeitungsregel die folgenden Aktionen aus:

1. Sie ruft das Gateway 'StoreXACMLFW' auf, das als PDP im Szenario dient.

2. Abhängig von der Antwort wird das Feld für die Preisinformation überarbeitet (mit Nullen überschrieben), je nach dem, ob der Benutzer die Managerrolle hat oder nicht.

Im Beispiel enthaltene XML-Firewalls

Die folgenden XML-Firewalls sind im Beispiel definiert.

XML-Firewall StoreAddLTPA

Die Funktion der XML-Firewall StoreAddLTPA besteht darin, ein Front-End mit einem Port auszustatten, den Benutzer nur mit der Basisauthentifizierung (zum Beispiel ohne LTPA (Lightweight Third Party Authentication)) aufrufen können. Die Regel zur Anforderungsverarbeitung führt folgende Aktionen aus:

1. Sie identifiziert durch Basisauthentifizierung.
2. Sie authentifiziert durch eine einfache LDAP-Suche (Lookup).
3. Sie fügt ein LTPA-Token im Rahmen der Nachverarbeitung hinzu.
4. Sie leitet die Anforderung an die StoreWSP-Sicherheitsrichtlinie mit der jetzt angehängten LTPA-Information weiter.

XML-Firewall StoreMockService

Der Service 'StoreMockService' ist ein Beispielservice, der eine XML-Firewall als Implementierung verwendet. Die Operationen 'findInventory', 'purchase' und 'return' werden alle unterstützt. Die Antwortwerte sind statisch. Dieser Beispielservice wird erstellt, wenn es nicht möglich ist, einen WebSphere Application Server in das Muster einzubeziehen. Die drei Anforderungsregeln der Richtlinie ermitteln die Anforderungsoperation durch eine Abgleichsaktion und abhängig von einer gefundenen Übereinstimmung und antworten mit einer statischen SOAP-Antwort. Statische SOAP-Antworten werden auf der Basis der Anforderungsoperation und nicht durch eine vollständige Serviceimplementierung bereitgestellt.

XML-Firewall StoreMockServiceAlternate

Der Service 'StoreMockServiceAlternate' ist ein Beispielservice, der eine XML-Firewall als Implementierung verwendet. Die Operationen 'findInventory', 'purchase' und 'return' werden alle unterstützt. Der Service dient zur Demonstration, wie die Routing-Richtlinie durchgesetzt wird.

Firewall StoreXACMLFW

In diesem Szenario wird eine Überarbeitung (Redaktion) auf der Basis des Ergebnisses eines XACML-basierten Zulassungs-/Verweigerungsmechanismus (Permit/Deny) ausgeführt. In DataPower gibt es keine Möglichkeit, eine einzelne AAA-Aktion im Antwortablauf aufzurufen. Ein separates Gateway wird für den XACML-Richtlinienentscheidungspunkt (PDP) erstellt. Dieser PDP wurde in der Anforderungsregel der Firewall 'StoreXACMLFW' in eine AAA-Aktion eingebunden.

StoreXACMLFW ist ein XML-Firewall-Gateway in DataPower. Diese Implementierung wird verwendet, weil sie eine einfache Methode ist, die Funktionalität bereitzustellen. Die Firewall 'StoreXML' verwendet dieselbe WSDL-Schnittstelle wie der Tivoli Runtime Security Services-Server. Das StoreWSP-Gateway erstellt das Anforderungsobjekt und sendet es, durch SSL geschützt, an das StoreXMLFW-Gateway.

Die Anforderungsregel der StoreXML-Firewall führt die folgenden Aufgaben aus:

1. Führt AAA mit den SSL-Informationen für die Authentifizierung aus.
2. Führt die Autorisierung mit einem boxinternen XACML-PDP aus. Die Richtlinie, die vom PDP verwendet wird, wurde ursprünglich in IBM Tivoli Security Policy Manager verfasst, kann jedoch mit einem Standardeditor erneut erstellt werden. Das Schema ist in der XACML-Spezifikation definiert.
3. Es ist keine Transformation der Anforderung für diese Autorisierungsverarbeitung erforderlich.
4. Wenn die XACML-Anforderung gültig ist, führt die Anforderungsverarbeitungsregel einen Abruf einer Zulassungsantwort ('Permit') aus und gibt diese an den Client zurück. Andernfalls wird eine Ausnahmebedingung ausgelöst, die von der Ausnahmebehandlungsregel verarbeitet wird, und es wird eine Verweigerungsantwort (Deny) an den Client zurückgegeben.

Anmerkung: Die Verarbeitung mit der Antwort Zulassung/Verweigerung/Unbestimmt ist lediglich ein Beispiel. In einen kundenorientierten Ablauf könnten zusätzliche Fehlerinformationen einbezogen werden.

XACML-Sicherheitsrichtlinie

In diesem Abschnitt wird beschrieben, wie XACML-Dokumente erstellt werden.

Die im Beispiel verwendeten XACML-Dokumente wurden mithilfe des Richtlinieneditors von IBM Tivoli Security Policy Manager erstellt. Sie können jedoch einen beliebigen Text- oder XML-Editor zur Erstellung solcher Dokumente verwenden. Informationen zum Zusammenstellen oder Ändern vorhandener XACML-Richtlinien finden Sie in den OASIS-Spezifikationen: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml.

Die im Beispiel verwendete XACML-Sicherheitsrichtlinie ist in den Dateien `storeSWPXACML.xml` und `storePrivateDataXACML.xml` enthalten. Diese Richtlinien werden zur Auswertung von Anforderungen verwendet, die beim Richtlinienentscheidungspunkt (PDP) eingehen. Eine Anforderung besteht aus vier Schlüsselelementen:

1. Abschnitt 'Subjects' - Enthält die Details des definierten Namens (Distinguished Name, DN) des Aufrufers der Anforderung sowie die Gruppen, zu denen der Aufrufer gehört.
2. Abschnitt 'resource' - Enthält die Dokumente, auf die der Aufrufer Zugriff anfordert. Im Beispiel werden zwei Typen von Ressourcen verwendet. Der erste Typ ist die Operation im Web-Service und der zweite Typ die Autorisierung für die Daten in der Antwort, in diesem Fall die Ressource 'priceInfo'.
3. Abschnitt 'Environment' - Enthält Informationen zur Umgebung der Anforderung.
4. Abschnitt 'action' - Die Aktion, die der Benutzer mit dem autorisierten Material ausführen möchte. Im Überarbeitungsszenario besteht die Aktion einfach darin, die Preisinformationen (priceInfo) anzuzeigen.

Sicherheitsrichtlinie für 'StoreWSP'

Die Sicherheitsrichtlinie in der Datei `storeSWPXACML.xml` ordnet Gruppen Web-Service-Operationen zu.

Das folgende Beispiel zeigt eine Sicherheitsrichtlinie:

```
<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>
```

Anmerkung: Im Abschnitt 'subjects' tritt eine Übereinstimmung beim x500-Namen oder bei dem Wert 'Manager' im Feld 'subject:role' auf. Wenn Sie die gesamte `.xml`-Datei der Richtlinie untersuchen, können Sie feststellen, dass ähnliche Zuordnungen für Customer und Clerk vorhanden sind. Sie können feststellen, dass die Operation 'findInventory' für die Verwendung aller drei Gruppen autorisiert ist, während die Operationen 'returnProduce' und 'purchase' auf bestimmte Gruppen begrenzt sind.

Überarbeitungsgateway

Nachfolgend werden Details zum Style-Sheet 'storeCallPDP.xsl' beschrieben.

Wenn Sie das Style-Sheet 'storeCallPDP.xsl' untersuchen, werden Sie die folgenden Punkte bemerken:

1. Den Einschluss des Style-Sheets 'storeSendToPDP.xsl'. Dieses Style-Sheet enthält die Logik zum Aufrufen von 'storeXAMLFW'.
2. Den Aufruf der Schablone 'call_PDP' in 'storeSendToPDP'.
3. Die Extraktion der Entscheidung aus der Antwort des Aufrufs (z. B. „Permit").
4. Die Einstellung des Werts der Variablen `var:/context/response/displayfilter` entweder auf das Style-Sheet 'allData.xsl' oder auf das Style-Sheet 'noPriceInfo.xsl'.
5. Die Struktur des XACML-Dokuments für die Überarbeitung (Redaktion) mit dem Namen 'storePrivateDataXACML.xml' ist annähernd identisch mit der Struktur im StoreWSP-Szenario. Der Unterschied besteht darin, dass nur die Managerrolle Zugriff hat.

storeCallPDP.xsl

```
<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:dp="http://www.datapower.com/extension
extension-element-prefixes="dp" exclude-result-prefixes="dp">
  <xsl:include href="storeSendToPDP.xsl" />
    <xsl:template match="/">
      <xsl:call-template name="call_PDP">
        <xsl:with-param name="resource" select="'StorePrivateData'" />
      </xsl:call-template>
      <xsl:variable name="decision">
        <xsl:copy-of select="dp:variable('var://context/snip/xacml/BacksideXacmlResponse')/
    *[local-name()='url-open']/*[localname()='response']/*[local-name()='Envelope']/*[local-name()='Body']/
    *[local-name()='Response']/*[local-name()='Result']/*[localname()='Decision']" />
      </xsl:variable>
      <xsl:message dp:priority="debug">
        <DECISION-FROM-RTSS>
          <xsl:value-of select="$decision" />
        </DECISION-FROM-RTSS>
      </xsl:message>
      <xsl:choose>
      <xsl:when test="$decision = 'Permit'">
        <xsl:message dp:priority="debug">****** EINSTELLEN DES PRIVATEN FILTERS ********</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>
```

In SOA Policy Gateway Basic Runtime Sample erstellte WSRR-Artefakte

Nachfolgend werden die WSRR-Artefakte, die im SOA Policy Gateway Basic Runtime Sample-Muster erstellt werden, und ihre Verwendungsweise durch das Beispiel beschrieben.

Tabelle 14. Für das SOA Policy Gateway Basic Runtime Sample-Muster erstellte WSRR-Artefakte

Objekt	Beschreibung
Organisation	Bob's Warehouse. Dies ist der Geschäftsbereich des Service "Store".

Tabelle 14. Für das SOA Policy Gateway Basic Runtime Sample-Muster erstellte WSRR-Artefakte (Forts.)

Objekt	Beschreibung
Geschäftsfunktion (Business Capability)	Warehouse. Stellt alle Versionen des Service "Store" dar und gehört dem Unternehmen "Bob's Warehouse".
Serviceversion	Store. Stellt die Version 1.0 des Service "Store" dar.
WSDL	Store.wsdl.
XSD	Company.xsd.
Richtlinie	• Validate.xml • RouteForGold.xml • LogEveryTime.xml • RejectAfter5MsgIn90Seconds.xml
SLD	Store SLD. Alle hier angehängten Richtlinien werden auf alle Anforderungen für diesen Service angewendet.
Gold SLA	Gold SLA. Diese SLA bedeutet, dass Gold-Anforderungen vom Konsumenten "CEO" nicht als anonym gezählt werden. Alle hier angehängten Richtlinien werden bei Gold-Anforderungen vom Konsumenten "CEO" durchgesetzt.
Silver SLA	Silver SLA. Diese SLA bedeutet, dass Silver-Anforderungen vom Konsumenten "CEO" nicht als anonym gezählt werden. Wenn keine Richtlinien angehängt sind, wird die Anforderung zugelassen.
Anonymes SLA	Anonymous Users. Die hier angehängten Richtlinien werden bei allen Anforderungen durchgesetzt, die keine übereinstimmende SLA haben. In diesem Beispiel werden bei allen Anforderungen von anderen Konsumenten als "CEO" bzw. alle Anforderungen von "CEO", der nicht "Gold" oder "Silver" ist, die Richtlinien "Anonymous SLA" durchgesetzt.

In SOA Policy Gateway Basic Runtime Sample erstellte DataPower-Artefakte

Nachfolgend werden die DataPower-Artefakte beschrieben, die im SOA Policy Gateway Basic Runtime Sample-Muster erstellt werden.

Tabelle 15. DataPower-Artefakte, die für das SOA Policy Gateway Basic Runtime Sample-Muster erstellt werden

Typ	Name	Zweck
WebService-Proxy	StoreWSP	Der Hauptservice.
XML-Firewalls	StoreAddLTPA StoreMockService StoreAlternateMockService StoreXACMLFW	Authentifiziert das LTPA-Token und fügt es hinzu. Der Service-Provider für Nicht-Gold-Kunden. Der Service-Provider für Gold-Kunden. Überprüft den Zugriff auf die Preisinformationen ('PriceInfo').
WSRR-Server	WSRRSVR	Die Verbindung zu WSRR.

Tabelle 15. DataPower-Artefakte, die für das SOA Policy Gateway Basic Runtime Sample-Muster erstellt werden (Forts.)

Typ	Name	Zweck
WSRR-Subskription	StoreSub	Stellt Suchinformationen zu WSRR-Namensbereich, WSRR-Objekt usw. bereit.
AAA-Richtlinie	StoreAddLTPA	Basisauthentifizierung und Identifikation für LDAP. Führt die Authentifizierung durch eine Suche aus. Fügt der Anforderung das LTPA-Token hinzu.
AAA-Richtlinie	StoreWSDLAAA	LTPA-Identifikation und -Authentifizierung. Gruppenzuordnung für die Autorisierung. XACML-Autorisierung.
AAA-Richtlinie	StoreXACMLFWAZ	XACML-Autorisierung für Preisinformationen ('PriceInfo').
SSL-Proxy-Profil	WSRRPP	SSL-Proxy-Profil für den WSRR-Server.
Kryptoprofil	WSRRCP	Kryptoprofil für den WSRR-Server.
Berechtigungsnachweise zur Überprüfung	WSRRVC	Berechtigungsnachweise für die Überprüfung enthalten das Kryptozertifikat WSRRCERT. Alle anderen Einstellungen sind Standardwerte.
Kryptozertifikat	WSRRCERT	WSRRCERT verwendet das Unterzeichnerzertifikat. Dieses Zertifikat wurde entweder aus NodeDefaultKeyStore, dem Standardzertifikat für einen Einzelserver, oder aus CMSKeyStore, dem Standardzertifikat bei einer Network Deployment-Umgebung (ND), in der ein IBM HTTP Server vorhanden war, extrahiert.

Verarbeitungsregeln für den Web-Service-Proxy 'StoreWSP'

Das zentrale Gateway des Beispiels ist 'StoreWSP'. Die Richtlinie für das Gateway enthält eine Anforderungs- und eine Antwortregel.

Anforderungsregel

Die primäre Richtlinienaktion der Regel 'StoreWSP_default_request-rule' hat den Namen 'AAA'. In der AAA-Aktion wird das LTPA-Token überprüft, die Benutzergruppen werden abgerufen und eine Autorisierung durchgeführt, um festzustellen, ob der Benutzer in der LDAP-Gruppe 'Manager', 'Clerk' oder 'Customer' ist. Diese Überprüfung wird ausgeführt, wenn der Schritt AZ von AAA

den Richtlinienentscheidungspunkt (PDP, Policy Decision Point) 'StoreWSDLPDP' auf dem DataPower-Gerät aufruft. Dieser PDP verwendet die XACML-Richtlinie 'storeWSPXACML.xml'.

Antwortregel

In der Antwortregel 'StoreWSP_default_response-rule' ruft die Transformation den XML-Firewall-Service 'StoreXACMLFW' auf.

Diese Transformation bestimmt entsprechend der Zugehörigkeit des Benutzers zur Gruppe 'Manager', ob der Benutzer autorisiert ist, auf die Preisinformationen zuzugreifen. Wenn der Benutzer autorisiert ist, wird die Variable *var:///context/response/displayFilter* auf den Wert `local:///allData.xsl` gesetzt. Wenn er nicht zur LDAP-Gruppe 'Manager' gehört, wird die Variable *var:///context/response/displayFilter* auf den Wert `local:///noPriceInfo.xsl` gesetzt.

Die Transformation führt anschließend die Style-Sheet-Aktionen an der Antwort aus.

StoreXAMLFW-Verarbeitungsregeln

Das angepasste Style-Sheet 'storeSendToPDP.xsl' setzt einen Aufruf an die lokale XML-Firewall 'StoreXACMLFW' ab. In dieser Firewall werden zwei Verarbeitungsregeln verwendet. Die Regel 'StoreXACMLFW_request' enthält eine einzelne AAA-Richtlinienaktion, die die Transformation 'allData.xsl' verwendet. Diese AAA-Aktion mit dem Namen 'StoreXACMLFWAZ' ruft wiederum die XACML-PDP-Aktion 'StorePDP' auf. Anhand der XACML-Richtlinie 'storePrivateDataXACML.xml' wird ermittelt, ob der Benutzer für den Zugriff auf die Preisinformationen autorisiert ist.

Beispiel-XSL-Style-Sheets

Die Beispielanwendung enthält die nachfolgend aufgeführten Style-Sheets mit der Dateinamenerweiterung `.xsl`, die sich im lokalen Verzeichnis der installierten Domäne befinden.

Tabelle 16. Style-Sheets in der Beispielanwendung

Style-Sheet	Zweck
`allData.xsl`	Ein Identitäts-Style-Sheet, das alle Daten von der Quelle an das Ziel kopiert. Es wird für die Überarbeitungsfunktion (Redaktion) und für den Aufruf an das XACML-XML-Gateway verwendet.
`apil-xacml-binding-new.xsl`	Verwendet die Credential-Mapping-Informationen zum Erstellen einer SOAP-Anforderung, die von dem Richtlinienentscheidungspunkt (PDP) auf dem DataPower-Gerät verarbeitet werden kann. Dieses Style-Sheet ist eine Modifikation des Style-Sheets 'tspm-xacml-binding-sample.xsl', das im Verzeichnis 'store' des DataPower-Geräts bereitgestellt wird. Die Hauptfunktionalität, die von diesem adaptierten Script bereitgestellt wird, besteht darin, eine extern zugängliche Variable hinzuzufügen, über die die Betreffinformationen ('subject') der XACML-Anforderung für das Überarbeitungs-Style-Sheet verfügbar gemacht werden.
`noPriceInfo.xsl`	Dieses Style-Sheet legt das Preiselement auf den Wert 0.0 fest.

Tabelle 16. Style-Sheets in der Beispielanwendung (Forts.)

Style-Sheet	Zweck
rgxacml.xsl	Dieses Style-Sheet ist eine Anpassung des Style-Sheets 'tspm-retrieve-groups.xsl' im Verzeichnis 'store' des DataPower-Geräts. Der primäre Zweck dieses Style-Sheets besteht darin, den definierten LDAP-Namen (DN), den Hostnamen, das Kennwort, den Port usw. anzugeben, sodass der eingehende Benutzer gesucht und die zugehörigen Gruppeninformationen abgerufen werden können.
soavars.xsl	Dieses Style-Sheet ist ein reines Demo-Style-Sheet, das die LDAP-Informationen in Variablen definiert, die vom Style-Sheet 'rgxacml.xsl' verwendet werden. Im Beispiel wird das Kennwort nicht verschlüsselt, was keine empfohlene Praxis für die Produktionsumgebung ist.
storeCallPDP.xsl	Dieses Style-Sheet enthält den Code zum Aufrufen des XACML-Gateways, verarbeitet die Zulassungs-/ Zurückweisungsentscheidung ('Permit/Deny') und definiert die Filtervariable zum Ausführen entweder von 'allData.xsl' oder 'noPriceInfo.xsl'.
storeSendToPDP.xsl	Dieses Style-Sheet setzt eine SOAP-Anforderung zusammen, die an das XACML-Gateway gesendet wird. Es schließt die Betreffinformationen ('subject'), die im Style-Sheet 'apil-xacml-binding-new.xsl' abgerufen werden, die Ressourceninformationen, die Aktionsinformationen und die Umgebungsinformationen ein.

DataPower-Objekte, die die XSL-Style-Sheets verwenden

Die DataPower-Objekte verwenden einige der XSL-Style-Sheets, die mit der Beispielanwendung bereitgestellt werden.

Tabelle 17. DataPower-Objekte, die die XSL-Style-Sheets verwenden

Style-Sheet	Zweck
allData.xsl	Wird intern im Style-Sheet 'storeCallPDP.xsl' verwendet. Das Style-Sheet dient zur angepassten Umsetzung in der AAA-Richtlinie 'StoreXACMLFWAZ'.
apil-xacml-binding-new.xsl	Wird als angepasstes Style-Sheet im Schritt AZ der AAA-Richtlinie StoreWSDLAAA verwendet.
noPriceInfo.xsl	Wird intern im Style-Sheet 'storeCallPDP.xsl' verwendet.
soavars.xsl	Wird intern im Style-Sheet 'rgxacml.xsl' verwendet.
storeCallPDP.xsl	Wird als Umsetzung in der Regel 'Store_default-response' aufgerufen.
storeSendToPDP.xsl	Wird intern im Style-Sheet 'storeCallPDP.xsl' verwendet.

Kapitel 6. Mit der implementierten Instanz arbeiten

Nach der Implementierung einer IBM SOA Policy Gateway Pattern können Sie die implementierte Instanz anzeigen, indem Sie in der Workload Console auf **Instances** > **Virtual systems** klicken.

Instanzdetails anzeigen

Die Details einer implementierten Instanz können durch Auswählen einer Instanz im Fenster **Virtual System Instances** angezeigt werden. Die Details der Instanz des virtuellen Systems werden angezeigt. Zu den Details gehören eine Liste der virtuellen Maschinen, die in der Cloudinfrastruktur für die betreffende Implementierung bereitgestellt wurden, die IP-Adresse und der Status der virtuellen Maschine.

Die Statusinformation zu Bereitstellung und Implementierung der Instanz finden Sie im Wert **Current status** in der Detailsicht.

Zum Anzeigen des Status der virtuellen Maschinen und Scripts während der Bereitstellung erweitern Sie den Abschnitt **History** in der Detailsicht.

Zum Anzeigen der Details zu virtuellen Maschinen und Scriptprotokollen erweitern Sie den Abschnitt **Virtual machines** in der Detailsicht. Der Hostname und die IP-Adresse des Systems befinden sich im Wert von **Network interface 0** im Abschnitt **Hardware and network**. Die Scriptprotokolle befinden sich im Abschnitt **Script Packages**. Sie können mit jeder Konsole eine Verbindung herstellen, indem Sie die Links im Abschnitt **Consoles** verwenden.

Auf implementierte Instanzen zugreifen

Nach der Implementierung eines Musters für ein virtuelles System können Sie die erstellte virtuelle Systeminstanz anzeigen, um Ihre IBM SOA Policy Gateway Pattern-Umgebung zu prüfen und auf die Komponententeile zuzugreifen.

Vorbereitende Schritte

Zum Anzeigen einer virtuellen Systeminstanz müssen Sie zuerst ein Muster für ein virtuelles System implementieren.

Informationen zu diesem Vorgang

Durch die Implementierung eines Musters wird eine virtuelle Systeminstanz bzw. eine neu bereitgestellte Laufzeitumgebung für IBM SOA Policy Gateway Pattern erstellt. Wenn die Implementierung abgeschlossen ist, ist die virtuelle Systeminstanz aktiv.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um die virtuellen Systeminstanzen von IBM SOA Policy Gateway Pattern zu verwalten:

1. Klicken Sie auf **Instances** > **Virtual Systems**, um auf das Fenster **Virtual System Instances** zuzugreifen.

2. Wählen Sie in der Liste der Instanzen im Fenster **Virtual System Instances** die Instanz aus, die implementiert wurde.
3. Wenn die Instanz aktiv ist, können Sie sich über die Konsolenlinks in der Anzeige für virtuelle Systeme bei den Komponenten des virtuellen Systems anmelden. Die verfügbaren Komponenten hängen vom erstellten Muster ab. Sie enthalten:
   - Administrationskonsole von WebSphere Application Server
   - WSRR-Webbenutzerschnittstelle
   - WSRR Business Space
   - DataPower-Web-GUI

Verbindung zu WSRR herstellen - Business Space

Verwenden Sie die Business Space-Benutzerschnittstelle zum Arbeiten mit WSRR.

Informationen zu diesem Vorgang

Business Space ist eine der zwei grafischen Schnittstellen, die Sie beim Arbeiten mit WSRR verwenden können. Eine vollständige Beschreibung der Verwendung von Business Space mit WSRR finden Sie im WSRR Informationen Center (siehe zugehöriger Link).

Sie können eine Verbindung zum Business Space einer WSRR-Instanz in Ihrem implementierten Muster herstellen, indem Sie auf den Link in der Workload Console klicken oder die URL in einen Webbrowser eingeben.

Vorgehensweise

1. Gehen Sie wie folgt vor, um eine Verbindung zur Workload Console herzustellen:
   a. Klicken Sie auf **Instances** > **Virtual Systems**, um auf das Fenster **Virtual System Instances** zuzugreifen.
   b. Wählen Sie im Fenster **Virtual System Instances** aus der Liste der Instanzen Ihr implementiertes System aus.
   c. Klicken Sie auf **Virtual machines** in der Detailansicht des implementierten Systems, um die Liste zu erweitern.
   d. Suchen Sie in der Liste der virtuellen Maschinen nach WSRR und klicken Sie auf das Pluszeichen, um die Details anzuzeigen.
   e. Klicken Sie unter dem Abschnitt **Consoles** auf **WSRR_Business_Space**.
   f. Geben Sie die Benutzer-ID mit Administratorberechtigung und das Kennwort für WSRR ein.
2. Gehen Sie wie folgt vor, um eine Verbindung von einem Webbrowser aus herzustellen:
   a. Öffnen Sie einen Webbrowser.
   b. Suchen Sie nach dem Hostnamen und nach den Portnummern für WSRR. Zeigen Sie die Details Ihrer Implementierung an, wie in Schritt 1 beschrieben. Erweitern Sie den Abschnitt **Virtual machines** und wählen Sie die virtuelle Maschine für den WSRR-Server aus, um die Details zur virtuellen Maschine anzuzeigen. Im Abschnitt **Hardware and network** ist der Hostname der Wert **Network interface 0**.
   c. Geben Sie die URL der WSRR-Webbenutzerschnittstelle ein: http://*hostname*:9443/BusinessSpace, wobei *hostname* der Hostname des WSRR-Servers ist.

d. Geben Sie die Benutzer-ID mit Administratorberechtigung und das Kennwort für WSRR ein.

Ergebnisse

Business Space wird angezeigt und kann zum Hinzufügen, Bearbeiten oder Entfernen von Mediationsrichtlinien und anderen WSRR-Artefakten verwendet werden.

Nächste Schritte

Wenn Sie Business Space zum ersten Mal auf dem WSRR-System verwenden, finden Sie relevante Informationen in „Business Space für die Erstverwendung konfigurieren". Führen Sie die Schritte zur Erstellung des Space für SOA-Governance aus.

Zugehörige Informationen:

Information Center von IBM WebSphere Service Registry and Repository Version 8.0

Business Space für die Erstverwendung konfigurieren

Bevor die Business Space-Benutzerschnittstelle zum Erstellen von Richtlinien verwendet werden kann, muss der SOA-Governance-Space erstellt werden.

Vorbereitende Schritte

Informationen zum Zugriff auf Business Space finden Sie in „Verbindung zu WSRR herstellen - Business Space" auf Seite 86.

Informationen zu diesem Vorgang

Zur Verwendung der Business Space-Widgets müssen Sie einen Space erstellen. Spaces werden für bestimmte Rollen definiert. Die Richtlinienerstellung (Authoring) wird am geeignetsten im SOA-Governance-Space durchgeführt. Wenn noch kein SOA-Governance-Space erstellt wurde, müssen Sie einen erstellen. Führen Sie die folgenden Schritte aus, um einen Space auf der Basis der Schablone für die Service-Registry für SOA-Governance ('Service Registry for SOA Governance') zu erstellen:

Vorgehensweise

1. Klicken Sie oben auf der Seite auf **Manage Spaces**. Der Space Manager-Dialog wird angezeigt.
2. Klicken Sie auf **Create Space**. Der Dialog 'Create Space' wird angezeigt.
3. Geben Sie einen Namen in das Feld für den Space-Namen ein. Beispiel: `SOA Governance`. Geben Sie optional eine Beschreibung ein.
4. Wählen Sie **Service Registry for SOA Governance** in der Liste **Create a new space using a template** aus und klicken Sie auf **Save**.
5. Der neue Space wird in der Liste **Space Manager** angezeigt. Klicken Sie auf den neuen Space, um ihn zu öffnen.

Ergebnisse

Der Space 'SOA Governance' wurde erstellt. Gehen Sie wie folgt vor, um den Space 'SOA Governance' zu öffnen:

1. Klicken Sie oben auf der Seite auf **Go To Spaces**. Der Dialog 'Go To Spaces' wird angezeigt.
2. Klicken Sie auf den Space für SOA-Governance-Benutzer. Der jeweilige Name hängt davon ab, was bei der Erstellung des Space angegeben wurde.

Nächste Schritte

Sie können dem Widget 'Service Registry Actions' zusätzliche Aktionen hinzufügen:

1. Klicken Sie in Business Space auf **Edit Page**.
2. Klicken Sie im Widget 'Service Registry Actions' auf **Edit Settings**.
3. Wählen Sie die folgenden Aktionen zum Anzeigen aus:
   - Service-Level-Definition erstellen
   - Serviceversion erstellen
   - Service-Level-Agreement erstellen
   - Geschäftsfunktion (Business Capability) erstellen
4. Klicken Sie im Widget 'Service Registry Actions' auf **Save and Close**.
5. Klicken Sie auf **Finish Editing**.

Verbindung zu WSRR herstellen - WSRR-Webbenutzerschnittstelle

Verwenden Sie die WSRR-Webbenutzerschnittstelle, um mit WSRR zu arbeiten.

Informationen zu diesem Vorgang

Die WSRR-Webbenutzerschnittstelle ist eine der zwei grafischen Schnittstellen, die Sie beim Arbeiten mit WSRR verwenden können. Eine vollständige Beschreibung der Verwendung der WSRR-Webbenutzerschnittstelle finden Sie im WSRR Informationen Center (siehe zugehöriger Link). In den meisten Fällen werden Sie mit der Business Space-Schnittstelle arbeiten. Es gibt jedoch Tasks (z. B. das Erstellen von Überwachungsrichtlinien), die in der WSRR-Webbenutzerschnittstelle durchgeführt werden müssen.

Sie können eine Verbindung zur WSRR-Webbenutzerschnittstelle einer WSRR-Instanz in Ihrem implementierten Muster herstellen, indem Sie auf den Link in der Workload Console klicken oder die URL in einen Webbrowser eingeben.

Vorgehensweise

1. Gehen Sie wie folgt vor, um eine Verbindung zur Workload Console herzustellen:
   a. Klicken Sie auf **Instances** > **Virtual Systems**, um auf das Fenster **Virtual System Instances** zuzugreifen.
   b. Wählen Sie im Fenster **Virtual System Instances** aus der Liste der Instanzen Ihr implementiertes System aus.
   c. Klicken Sie auf **Virtual machines** in der Detailansicht des implementierten Systems, um die Liste zu erweitern.
   d. Suchen Sie in der Liste der virtuellen Maschinen nach WSRR und klicken Sie auf das Pluszeichen, um die Details anzuzeigen.
   e. Klicken Sie unter dem Abschnitt **Consoles** auf **WSRR_Web_UI**.
   f. Geben Sie die Benutzer-ID mit Administratorberechtigung und das Kennwort für WSRR ein.

2. Gehen Sie wie folgt vor, um eine Verbindung von einem Webbrowser aus herzustellen:
   a. Öffnen Sie einen Webbrowser.
   b. Suchen Sie nach dem Hostnamen und nach den Portnummern für WSRR. Zeigen Sie die Details Ihrer Implementierung an, wie in Schritt 1 beschrieben. Erweitern Sie den Abschnitt **Virtual machines** und wählen Sie die virtuelle Maschine für den WSRR-Server aus, um die Details zur virtuellen Maschine anzuzeigen. Im Abschnitt **Hardware and network** ist der Hostname der Wert **Network interface 0**.
   c. Geben Sie die URL der WSRR-Webbenutzerschnittstelle ein: http://*hostname*:9443/ServiceRegistry, wobei *hostname* der Hostname des WSRR-Servers ist.
   d. Geben Sie die Benutzer-ID mit Administratorberechtigung und das Kennwort für WSRR ein.

Zugehörige Informationen:

Information Center von IBM WebSphere Service Registry and Repository Version 8.0

Verbindung zur Administrationskonsole von WebSphere Application Server herstellen

Verwenden Sie die Administrationskonsole von WebSphere Application Server, um die Sicherheitseinstellungen zu optimieren und andere Verwaltungstasks auszuführen.

Informationen zu diesem Vorgang

Vollständige Informationen zum Arbeiten mit der Administrationskonsole von WebSphere Application Server finden Sie im Informationen Center. Folgen Sie dem zugehörigen Link.

Sie können eine Verbindung Administrationskonsole von WebSphere Application Server in Ihrem implementierten Muster herstellen, indem Sie auf den Link in der Workload Console klicken oder die URL in einen Webbrowser eingeben.

Vorgehensweise

1. Gehen Sie wie folgt vor, um eine Verbindung zur Workload Console herzustellen:
   a. Klicken Sie auf **Instances** > **Virtual Systems**, um auf das Fenster **Virtual System Instances** zuzugreifen.
   b. Wählen Sie im Fenster **Virtual System Instances** aus der Liste der Instanzen Ihr implementiertes System aus.
   c. Klicken Sie auf **Virtual machines** in der Detailansicht des implementierten Systems, um die Liste zu erweitern.
   d. Suchen Sie in der Liste der virtuellen Maschinen nach WSRR und klicken Sie auf das Pluszeichen, um die Details anzuzeigen.
   e. Klicken Sie unter dem Abschnitt **Consoles** auf **WebSphere_Business_Space**.
   f. Geben Sie die Benutzer-ID mit Administratorberechtigung und das Kennwort für WSRR ein.
2. Gehen Sie wie folgt vor, um eine Verbindung von einem Webbrowser aus herzustellen:
   a. Öffnen Sie einen Webbrowser.

b. Suchen Sie nach dem Hostnamen und nach den Portnummern für WSRR. Zeigen Sie die Details Ihrer Implementierung an, wie in Schritt 1 beschrieben. Erweitern Sie den Abschnitt **Virtual machines** und wählen Sie die virtuelle Maschine für den WSRR-Server aus, um die Details zur virtuellen Maschine anzuzeigen. Im Abschnitt **Hardware and network** ist der Hostname der Wert **Network interface 0**.

c. Geben Sie die URL der WSRR-Webbenutzerschnittstelle ein: http://*hostname*:9043/ibm/console, wobei *hostname* der Hostname des WSRR-Servers ist.

d. Geben Sie die Benutzer-ID mit Administratorberechtigung und das Kennwort für WSRR ein.

Zugehörige Informationen:

Informationen Center von WebSphere Application Server Version 8.0

Verbindung zur Konsole einer virtuellen DataPower-Maschine herstellen

Verwenden Sie die DataPower-Konsole, um den Richtliniendurchsetzungspunkt zu konfigurieren.

Informationen zu diesem Vorgang

Vollständige Details zur Konfiguration Ihres Gateways finden Sie im Information Center von WebSphere DataPower. Folgen Sie dem zugehörigen Link.

Mithilfe eines Webbrowsers stellen Sie eine Verbindung zur Konsole her. Sie rufen die Verbindungsdetails ab, indem Sie Details Ihres implementierten Musters in der Workload Console anzeigen.

Vorgehensweise

1. Rufen Sie die benötigten Details mit der Workload Console ab:
   a. Klicken Sie auf **Instances** > **Virtual Systems**, um auf das Fenster **Virtual System Instances** zuzugreifen.
   b. Wählen Sie im Fenster **Virtual System Instances** aus der Liste der Instanzen Ihr implementiertes System aus.
   c. Erweitern Sie in der Detailansicht den Abschnitt **Virtual machines** und wählen Sie die virtuelle Maschine für das DataPower-Gerät aus, um die Details zur virtuellen Maschine anzuzeigen. Im Abschnitt **Hardware and network** ist der Hostname der Wert **Network interface 0**.
2. Öffnen Sie einen Webbrowser und geben Sie die URL `https://`*`hostname`*`:9090/dp` ein, wobei *hostname* der Hostname Ihres virtuellen Geräts ist.

Zugehörige Informationen:

Informationen Center von WebSphere DataPower Version 6.0

Verbindung zur Überwachungskonsole herstellen

Verwenden Sie die Überwachungskonsole zur Überwachung von Informationen.

Informationen zu diesem Vorgang

Sie können die Überwachungskonsole im Fenster **Virtual System Instances** aufrufen.

Die Überwachungsfunktion wird von ITCAM for SOA bereitgestellt. Laden Sie sich die Dokumentation aus dem zugehörigen Link herunter, um weitere Informationen zu erhalten, und suchen Sie nach Informationen zu den DataPower-Installationen.

Vorgehensweise

1. Klicken Sie auf **Instances** > **Virtual Systems**, um auf das Fenster **Virtual System Instances** zuzugreifen.
2. Wählen Sie in der Liste der Instanzen im Fenster **Virtual System Instances** die Instanz aus, die implementiert wurde. Die Instanzdetails werden angezeigt.
3. Erweitern Sie den Abschnitt **Virtual machines** und wählen Sie die virtuelle Maschine aus, die Sie überwachen möchten.
4. Suchen Sie unter **General information** die Option **Monitoring** und klicken Sie auf den Link **Click to open**.

Zugehörige Informationen:

ITCAM for SOA 7.2.1 - Dokumentation (von Fix Central)

Die implementierte Instanz stoppen und starten

Sie können mit der Workload Console die implementierte Instanz stoppen und starten. Sie können auch einzelne virtuelle Maschinen im Muster stoppen und starten.

Gehen Sie wie folgt vor, um eine ausgeführte implementierte Instanz zu stoppen:

1. Wählen Sie **Instances** > **Virtual Systems** und dann die Instanz in der Liste **Virtual System Instances** aus.
2. Klicken Sie auf das Symbol **Stop** in der Instanztitelleiste.

Gehen Sie wie folgt vor, um eine gestoppte implementierte Instanz zu starten:

1. Wählen Sie **Instances** > **Virtual Systems** und dann die Instanz in der Liste **Virtual System Instances** aus.
2. Klicken Sie auf das Symbol **Start** in der Instanztitelleiste.

Anmerkung: Ein bekannter Fehler in DB2 10.1.0.2 führt dazu, dass die DB2-Prozesse nicht immer neu starten, wenn die Instanz gestoppt und neu gestartet wird. In diesem Fall müssen Sie den DB2-Prozess manuell starten, indem Sie sich beim DB2-Knoten als 'db2inst1' anmelden und **`db2start`** ausführen. Sie müssen außerdem die WSRR-Prozesse in den WSRR-Knoten neu starten.

Gehen Sie wie folgt vor, um einzelne virtuelle Maschinen zu stoppen:

1. Erweitern Sie den Abschnitt **Virtual Machines** in der Instanzansicht.
2. Wählen Sie den Link **Manage** für die Maschine aus, die Sie stoppen möchten.
3. Klicken Sie auf das Stoppsymbol in der Leiste 'Manage'.

Gehen Sie wie folgt vor, um einzelne virtuelle Maschinen zu starten:

1. Erweitern Sie den Abschnitt **Virtual Machines** in der Instanzansicht.
2. Wählen Sie den Link **Manage** für die Maschine aus, die Sie stoppen möchten.
3. Klicken Sie auf das Startsymbol in der Leiste 'Manage'.

Sie können auch WSRR und DB2 über die Befehlszeile stoppen und starten. Klicken Sie auf den Link **Login**, um eine Verbindung herzustellen, indem Sie die SSH-Konsole verwenden.

Sie stoppen und Starten WSRR, indem Sie das WebSphere Application Server-Profil stoppen und starten. Siehe Profile mit Befehlen verwalten im Information Center von WebSphere Application Server.

Das WSRR-Cluster muss im Advanced-Muster nach dem Neustart der DMGR- und angepassten Knoten neu gestartet werden. Öffnen Sie dazu die Administrationskonsole von WebSphere Application Server und wählen Sie **Servers** > **Clusters** > **WebSphere Application Server Clusters** aus. Wählen Sie **WSRRCluster_1** aus und klicken Sie dann auf **Start**.

Sie können mithilfe von Systembefehlen DB2 stoppen und starten. Siehe Systembefehle im DB2 Information Center.

Musterkonfiguration nach der Implementierung

Nach der Implementierung der Muster müssen Sie Sicherheitseinstellungen und andere Einstellungen konfigurieren.

Richtliniendurchsetzungspunkt konfigurieren

Das DataPower-Gerät oder die DataPower-Instanz ist der Richtliniendurchsetzungspunkt (PEP) von IBM SOA Policy Gateway Pattern. Wenn die Anwendungsdomäne implementiert ist, kann der Inhalt dieser Domäne erstellt werden.

Vorgehensweise

Wenn Sie Ihre Konfigurationen einrichten, stellen Sie sicher, dass auf jedem DataPower-Gerät verschiedene Domänennamen verwendet werden. Anderenfalls zeigt der ITCAM for SOA-Topologiearbeitsbereich falsche Daten an.
Erstellen Sie einen Web-Service-Proxy (WSP):

1. Klicken Sie auf dem DataPower Control Panel auf die Option **Web Service Proxy**.
2. Klicken Sie auf **Add** und geben Sie einen Namen für den Proxy ein.
3. Öffnen Sie die Registerkarte **WSRR Subscription**. Klicken Sie in der Liste der WSRR-Server auf **WSRRSVR**.
4. Geben Sie die anderen erforderlichen Informationen an, wie zum Beispiel den Front-End-Handler, den Namensbereich (Namespace), den Objektnamen usw., um die Konfiguration des Web-Service-Proxys zu erstellen.

Erstellen Sie Richtlinien für den WSP:

5. Öffnen Sie die Registerkarte **Policy** für den WSP-Editor.
6. Klicken Sie auf der entsprechenden Ebene auf **Processing Rules** (Verarbeitungsregeln). Sie können entweder eine neue Regel erstellen oder die bereitgestellte Standardregel bearbeiten. Die wichtigste Richtlinienaktion, die hinzugefügt werden muss, ist **AAA Action**. Diese Aktion führt die Identifikation, Authentifizierung und Autorisierung durch, die für das Muster entscheidend sind.

   Wichtige Elemente, die Sie für die AAA-Aktion angeben müssen, sind Eingabe ('Input') und Ausgabe ('Output') sowie die AAA-Richtlinie. Sie können die Richtlinie während der Erstellung der AAA-Richtlinienaktion erstellen oder Sie haben sie möglicherweise schon zuvor mithilfe des AAA-Editors erstellt.

   - Die Identifikation ist der Schritt, in dem der Benutzer identifiziert wird. Im Beispiel werden zwei Formen der Identifikation verwendet. In der XML-Firewall 'StoreAddLTPA' wurde die Identifikation durch eine

Basisauthentifizierung ausgeführt. In der Firewall 'StoreWSP' wurde die Identifikation durch ein LTPA-Token bereitgestellt.

- Die Autorisierung ist der Schritt, in dem der Benutzer als für das System bekannter Benutzer ermittelt wird. Es stehen viele Optionen zur Auswahl. Im Beispiel gibt es zwei Optionen: Bei der ersten wurde der Benutzer mithilfe von LDAP überprüft und bei der zweiten wurde ein gültiges LTPA-Token akzeptiert.
- Die Autorisierung ist der Schritt, in dem dem Benutzer die Berechtigung für eine Ressource, in diesem Fall für die Web-Service-Operationen, erteilt wird. Die folgenden Schlüsselelemente müssen angegeben werden, um eine boxinterne XACML-PDP-Autorisierung verwenden zu können:
  - Die Methode: **Use XACML Authorization** (XACML-Autorisierung verwenden).
  - Die XACML-Version, zum Beispiel 2.0.
  - Der PDP-Typ, zum Beispiel verweigerungsbasierter PDP.
  - Use On box PDP (boxinternen PDP verwenden): **On**
  - Der Name des PDP, für den das XACML angegeben ist.
  - Konfigurieren Sie den PDP. Weitere Informationen finden Sie in „XACML-PDP in DataPower ändern" auf Seite 74.
  - Das angepasste XSL-Style-Sheet zum Binden von AAA und XACML: Verwenden Sie `apil-xacml-bindingnew.xsl` als Ausgangspunkt.

Gehen Sie wie folgt vor, um das Gateway zur Verwendung der Überarbeitung (Redaktion) zu konfigurieren:

7. Ändern Sie die XACML-Datei (`.xml`), um sie an die speziellen Sicherheitsrichtlinien anzupassen, die für die Überarbeitung durchgesetzt werden sollen.
8. Erstellen Sie eine XML-Firewall mit einer AAA-Aktion, die sich an dem Überarbeitungsbeispiel orientiert.
9. Modifizieren Sie den PDP, der von der obigen AAA-Aktion verwendet wird, sodass er auf das Style-Sheet verweist, das Sie zur Durchsetzung der Überarbeitung verwenden.
10. Kopieren und ändern Sie das Style-Sheet `storeCallPDP.xsl`, das die SOAP-Nutzdaten für den XACML-Service erstellt. Stellen Sie insbesondere sicher, dass die Aktion und die Ressource Ihren Anforderungen für das von Ihnen erstellte XACML-Richtliniendokument entspricht.
11. Stellen Sie sicher, dass Ihr geändertes Style-Sheet den richtigen Port für Ihre neue XACML-XML-Firewall aufruft.

Im Basic Runtime-Muster und Advanced Runtime-Muster erstellte DataPower-Objekte

Dieser Abschnitt enthält eine Übersicht über die DataPower-Objekte, die im Basic Runtime-Muster und im Advanced Runtime-Muster erstellt werden, und ihre Funktion.

Tabelle 18. Objekte des DataPower-Musters

Objekt	Beschreibung
Domäne	Eine Domäne, die für die Benutzeranwendung verwendet werden kann.

Tabelle 18. Objekte des DataPower-Musters (Forts.)

Objekt	Beschreibung
WSRR-Server	Hat den Namen WSRRSVR. Die SOAP-URL, der Benutzername und das Kennwort sowie ein SSL-Proxy-Profil mit Berechtigungsnachweisen zur Überprüfung werden konfiguriert.
SSL-Proxy-Profil	Hat den Namen WSRRPP und ist ein Weiterleitungsprofil (Client). Es verwendet das Kryptoprofil WSRRCP. Alle anderen Standardwerte werden verwendet.
Kryptoprofil	WSRRCP enthält ein Objekt zur Überprüfung von Berechtigungsnachweisen mit dem Namen WSRRVC, das das Unterzeichnerzertifikat enthält, das mithilfe der Musterscripts hochgeladen wurde.
Berechtigungsnachweise zur Überprüfung	Die WSRR-Berechtigungsnachweise zur Überprüfung enthalten das Kryptozertifikat WSRRCERT. Alle anderen Einstellungen sind Standardwerte.
Kryptozertifikat	WSRRCERT verwendet das Unterzeichnerzertifikat. Dieses Zertifikat wurde entweder aus NodeDefaultKeyStore, dem Standardzertifikatspeicher für einen Einzelserver, oder aus CMSKeyStore, dem Standardzertifikat bei einer Network Deployment-Umgebung (ND), in der ein IBM HTTP Server vorhanden war, extrahiert.

Beispiel für die Verwendung der WSRR-Serverdefinition in einem Web-Service-Proxy:

1. Klicken Sie auf dem DataPower Control Panel auf die Option **Web Service Proxy**.
2. Klicken Sie auf **Add** und geben Sie einen Wert im Feld **Name** für den Proxy an.
3. Wählen Sie als Nächstes die Registerkarte **WSRR Subscription** aus.
4. Wählen Sie im Menü den WSRR-Server aus. Das Objekt WSRRSVR ist verfügbar.
5. Geben Sie die anderen erforderlichen Informationen an, wie zum Beispiel den Front-End-Handler, den Namensbereich (Namespace), den Objektnamen usw., um die Konfiguration des Web-Service-Proxys zu erstellen.

DN-Werte für DataPower-Zertifikate

Bei Verwendung von SSL mit den durch IBM SOA Policy Gateway Pattern bereitgestellten Mustern ist die Überprüfung durch den DN-Host (DN - Distinguished Name, definierter Name) strikter als bei der Standardsicherheit von WebSphere Application Server. (Dieses Thema bezieht sich auf externe DataPower-Geräte.)

In WebSphere Application Server ist die Überprüfung durch den DN-Host standardmäßig nicht aktiviert. In den Scriptpaketen, die von Mustern in IBM SOA Policy Gateway Pattern verwendet werden, wird die DN-Hostüberprüfung jedoch aktiviert und kann nicht inaktiviert werden. Ein spezielles Zertifikat, das zwischen dem standardmäßigen WebSphere Application Server und DataPower funktioniert, funktioniert möglicherweise nicht für das Scriptpaket „SOA Policy Gateway 2.5.0.0 - Security" oder „SOA Policy Gateway 2.5.0.0 - Sample", das mit IBM SOA Policy Gateway Pattern verwendet wird. Beispielsweise könnte ein DN der Form `meinserver.ihrunternehmen.com` zwar von den WebSphere Application Server-Standardeinstellungen, jedoch nicht von den Scriptpaketen akzeptiert

werden. Informationen zum Hinzufügen oder Entfernen der DataPower-Zertifikate, die mit der Implementierung verwendet werden, finden Sie in „DataPower-Zertifikate im WSRR-Truststore entfernen oder hinzufügen".

DataPower-Zertifikate im WSRR-Truststore entfernen oder hinzufügen

In dieser Task wird beschrieben, wie DataPower-Zertifikate hinzugefügt oder entfernt werden. Dieses Thema bezieht sich auf implementierte Muster mit externen DataPower-Geräten.

Informationen zu diesem Vorgang

Die DataPower-Zertifikate werden in den WSRR-Truststore hochgeladen, um die Synchronisationsaktualisierung zwischen WSRR und DataPower für Richtlinienaktualisierungen zu vereinfachen. Wenn diese Funktion nicht benötigt wird, können Sie die DataPower-Zertifikate entfernen. Sie können außerdem neue DataPower-Zertifikate hinzufügen, wenn die Zertifikate geändert werden müssen.

Vorgehensweise

1. Vorgehensweise beim Entfernen von Zertifikaten:
   a. Melden Sie sich bei der WebSphere Application Server-Administrationskonsole unter `https://`*`hostname`*`:9043/ibm/console` an, wobei *hostname* der Hostname des WSRR-Systems ist. Geben Sie den Namen und das Kennwort des Benutzers mit Verwaltungsaufgaben ein.
   b. Navigieren Sie zu **Security, SSL certficates and key management**.
   c. Klicken Sie auf **Key Stores and Certificates**.
   d. Klicken Sie auf **NodeDefaultTrustStore**, wenn Ihre Implementierung auf einem Basic Runtime-Muster basiert, oder auf **CellDefaultTruststore**, wenn Sie ein Advanced Runtime-Muster implementiert haben.
   e. Klicken Sie auf **Signer Certificates**.
   f. Aktivieren Sie die Kontrollkästchen aller Zertifikate, die Sie entfernen möchten.
   g. Klicken Sie auf **Delete**.
   h. Klicken Sie auf **Save**.
2. Klicken Sie zum Hinzufügen neuer DataPower-Zertifikate auf **Add**.
   a. Melden Sie sich bei der WebSphere Application Server-Administrationskonsole unter `https://`*`hostname`*`:9043/ibm/console` an, wobei *hostname* der Hostname des WSRR-Systems ist. Geben Sie den Namen und das Kennwort des Benutzers mit Verwaltungsaufgaben ein.
   b. Navigieren Sie zu **Security, SSL certficates and key management**.
   c. Klicken Sie auf **Key Stores and Certificates**.
   d. Klicken Sie auf **NodeDefaultTrustStore**, wenn Ihre Implementierung auf einem Basic Runtime-Muster basiert, oder auf **CellDefaultTruststore**, wenn Sie ein Advanced Runtime-Muster implementiert haben.
   e. Klicken Sie auf **Signer Certificates**.
   f. Klicken Sie auf **Add** und geben Sie die neuen Zertifikate an.
   g. Klicken Sie auf **Save**.

LTPA-Schlüssel ändern

In dieser Prozedur wird beschrieben, wie der LTPA-Schlüssel geändert wird. Der LTPA-Schlüssel wird von allen Zellen in den Mustern gemeinsam genutzt. Im SOA Policy Gateway Basic Runtime Sample-Muster wird er nicht verwendet. Der LTPA-Schlüssel wird vom Governance Master exportiert und in Laufzeitumgebungen vom Typ 'staging' oder 'production' importiert.

Informationen zu diesem Vorgang

Sie führen diese Aktionen in der Administrationskonsole von WebSphere Application Server aus. Weitere Informationen erhalten Sie unter dem zugehörigen Link.

Vorgehensweise

1. Exportieren Sie den neuen LTPA-Schlüssel aus dem WSRR-Deployment Manager (Dmgr) für den Governance Master.
2. Importieren Sie den LTPA-Schlüssel in die Laufzeit-WSRR-Instanzen, bei denen es sich um den 'Dmgr' oder einen eigenständigen Server handelt.
3. Wenn die Laufzeitinstanz auf einem Advanced Runtime-Muster basiert, führen Sie die Schritte in der folgenden Reihenfolge aus:
   a. Synchronisieren Sie alle Knoten.
   b. Stoppen Sie den WSRR-Cluster.
   c. Stoppen Sie die Knotenagenten.
   d. Stoppen Sie den Dmgr.
4. Wenn das WSRR-System auf einem Advanced Runtime-Muster basiert, führen Sie in umgekehrter Reihenfolge einen Neustart aus:
   a. Starten Sie den Dmgr.
   b. Starten Sie die Knotenagenten.
   c. Starten Sie den WSRR-Cluster.
5. Wenn der WSRR-Server ein eigenständiger Server (basierend auf einem Basic Runtime-Muster) ist, muss er gestoppt und erneut gestartet werden, damit die Änderung des LTPA-Schlüssels wirksam wird.

Zugehörige Informationen:

Informationen Center von WebSphere Application Server Version 8.0

Erstellung und Governance von Services

In der WSRR Business Space-Benutzerschnittstelle können Sie Geschäftsservices und die zugehörigen Objekte erstellen und durch Governance-Richtlinien regeln.

Der SOA Governance-Space muss in Business Space erstellt sein, bevor Richtlinien erstellt werden können. Wenn der SOA-Governance-Space noch nicht vorhanden ist, finden Sie Informationen in „Business Space für die Erstverwendung konfigurieren" auf Seite 87. Führen Sie die beschriebenen Schritte aus, um den Space zu erstellen.

Weitere Informationen zur Erstellung eines neuen, durch Governance-Richtlinien geregelten Service finden Sie im Information Center von IBM WebSphere Service Registry and Repository Version 8.0 - Lernprogramm: Neuen Service regeln (Governance).

Weitere Informationen zur Governance eines vorhandenen Service finden Sie im Information Center von IBM WebSphere Service Registry and Repository Version 8.0 - Lernprogramm: Vorhandenen Service regeln (Governance).

Zugehörige Tasks:

„Verbindung zu WSRR herstellen - Business Space" auf Seite 86
Verwenden Sie die Business Space-Benutzerschnittstelle zum Arbeiten mit WSRR.

Richtlinien

In diesem Abschnitt werden Implementierungsdetails für die Verwendung von WSRR als Richtlinienerstellungspunkt (PAP, Policy Authoring Point) und WebSphere DataPower als Richtliniendurchsetzungspunkt (PEP, Policy Enforcement Point) bei der Erstellung von Mediationsrichtlinien beschrieben.

Richtlinien in WSRR

WSRR (WebSphere Service Registry and Repository) kann zum Erstellen aller SOA-Richtlinien verwendet werden. Dazu gehören SLA-Richtlinien (SLA, Service-Level-Agreement), Mediationsrichtlinien und angepasste Richtlinien. Über die Business Space-Benutzerschnittstelle können Sie ein Richtliniendokument in WSRR erstellen, aktualisieren oder löschen. Das Richtliniendokument kann einen Richtlinienausdruck enthalten, der eine Reihe von Richtlinien für eine bestimmte Richtliniendomäne angibt. Alternativ können Sie ein Richtliniendokument erstellen, das vorhandene Richtlinien aus anderen Dokumenten zusammenstellt. Einzelne Richtlinien werden durch Richtlinienkennungen (IDs) angesprochen, die Sie angeben, wenn Sie Ihrem Dokument Richtlinien hinzufügen. Ein Richtlinienausdruck stellt die Deklaration einer Richtlinie dar und entspricht einem Element `<wsp:Policy>` in einem WS-Policy-Dokument.

Informationen zur Erstellung einer Mediationsrichtlinie in Business Space finden Sie in „Neue Mediationsrichtlinien erstellen" auf Seite 103.

Zusicherungen für Mediationsrichtlinien

Service-Level-Agreements (SLAs) ergeben sich für ein Unternehmen meist aus der Anforderung, dass die Servicequalität, die durch einen Service bereitgestellt wird, einem angegebenen Standard entsprechen muss. Beim Entwurf eines Service werden Funktionsanforderungen ausgearbeitet, um die Logik der Aktionen des Service vorzugeben. Parallel dazu werden im Rahmen der Analyse und des Entwurfs dieses Service nicht funktionale Anforderungen definiert, um die Servicequalität (QOS, Quality of Service) festzulegen, die von diesem Service erwartet wird. Zum Beispiel könnte das Unternehmen einen Service haben, der Informationen als Antwort auf eine Internetabfrage eines Kunden liefert. Ziel ist es, die Antwort binnen drei Sekunden zurückzugeben. Bei der Entwicklung der Gesamttransaktion könnte festgelegt werden, dass dieser Service seine Informationen innerhalb von zwei Sekunden zurückgeben muss, um die nicht funktionalen Anforderungen des Unternehmens zu erfüllen.

Es kann eine Richtlinie verfasst werden, die Laufzeitprüfungen der Leistung des Service implementiert und Aktionen ausführt, wenn die Anforderungen nicht erfüllt werden, um zu garantieren, dass der Service das für ihn definierte SLA erfüllt. Es könnte zum Beispiel ein primärer Serviceendpunkt vorhanden sein, der normalerweise (in 95 % der Fälle) eine Serviceantwort innerhalb von zwei Sekunden liefert. Der SOA-Architekt hat einen zweiten Serviceendpunkt auf einem anderen Server erstellt, der als Server im Bereitschaftsmodus für Ausfälle des

primären Endpunkts eingesetzt wird, jedoch auch bei hoher Frequentierung genutzt werden darf, wenn der primäre Endpunkt mit der Transaktionslast nicht Schritt halten kann. Für diese Situation kann eine Richtlinie verfasst werden, die die Serviceantwortzeit überprüft und den Netzdatenverkehr umleitet, wenn dies zur Erfüllung des SLA erforderlich ist.

Ein weiteres Beispiel, in dem SLAs durch eine Laufzeitrichtlinie verwaltet werden, ist eine Situation, in der ein Service auf Transaktionen antwortet, die eine größere Anzahl von Konsumenten mit jeweils unterschiedlichen Prioritäten haben. Ein einfaches Beispiel könnten Kunden der Kategorien 'Gold' und 'Bronze' sein, wobei nur für Kunden der Kategorie "Gold" eine bestimmte Servicequalität garantiert wird. In diesem Beispiel könnte geprüft werden, ob es sich bei dem Kunden um einen Kunden der Kategorie 'Gold' handelt. Wenn dies der Fall ist, könnte der Kunde an den sekundären Endpunkt umgeleitet werden, während ein Kunde der Kategorie 'Bronze' mit einer langsameren Antwortzeit bedient würde. Das Unternehmen hat diese Entscheidung getroffen, da 'Bronze'-Kunden nicht ausreichend Umsatzwachstum generieren, um den Aufwand für die Entwicklung einer Antwortzeit zu rechtfertigen, die das SLA für 'Gold'-Kunden erfüllt.

Ein drittes Beispiel könnte eine Situation sein, in der ein Service am Leistungslimit arbeitet, jedoch Nachrichten von Konsumentenservices niedriger Priorität in eine Warteschlange stellt oder sogar zurückweist, wenn er feststellt, dass er sich unter hoher Auslastung befindet. Ein Beispiel wäre eine Stapelroutine, die das System mit Konsumentenanfragen zu einem unerwarteten Zeitpunkt überflutet. Zur Aufrechterhaltung der Servicequalität könnte eine Laufzeitrichtlinie erstellt werden, die nur während der Geschäftsstunden in Kraft ist und die alle Stapelverarbeitungsanforderungen in diesem Zeitraum zurückweist.

Allgemeiner formuliert ermöglicht eine Mediationsrichtlinie eine Überprüfung und Transformation der vom Client (Konsumenten) eingehenden Nachricht, bevor die Nachricht dem Server (Provider) zugestellt wird.

Richtlinien unterstützen eine solche Überprüfung und Transformation von Nachrichten. Richtlinien können für einen Provider-Service allein, für ein bestimmtes Konsumenten-Provider-Paar oder für anonyme Konsumenten für einen Provider-Service angegeben werden. Richtlinien für anonyme Konsumenten stellen eine Methode bereit, eine Standardrichtlinie zu definieren, die nur für Konsumenten gilt, für die keine anderen Richtlinien gelten. Mithilfe dieser Funktionalität können Richtlinien für Fremdkonsumenten angegeben werden, die ihre Identität nicht preisgeben. Für solche Konsumentenservices könnten Transaktionen dann zum Beispiel zurückgewiesen werden. Dies kann zum Schutz gegen Denial-of-Service-Attacken von Konsumentenhackern nützlich sein, die versuchen, das System mit Transaktionen zu überfluten, um einen Provider-Service außer Gefecht zu setzen.

Bedingungen für Mediationsrichtlinien

Es können Mediationszusicherungen ('Assertions') erstellt werden, die es der Laufzeitrichtlinie ermöglichen, das Service-Level-Agreement (SLA) des Service zu steuern, die Umwandlung (Transformation) von Nachrichten vom Kunden zum Provider zu steuern oder das Nachrichtenschema der Kundennachricht zu validieren.

SLA-Richtlinienbedingungen stellen einen besonderen Typ von Mediationsrichtlinie dar, der ein klassisches If-Then-Else-Konstrukt mit einer Bedingung und einem Satz von Aktionen ermöglicht, die je nach Auswertung der Bedingung ausgeführt

werden. Die Angabe einer Bedingung ist optional. Wenn keine Bedingung angegeben wird, ist dies mit der Auswertung der logischen Bedingung als 'wahr' äquivalent, sodass alle angegebenen Aktionen entsprechend umgesetzt werden.

Wenn eine Bedingung angegeben wird, muss sie aus einem booleschen Ausdruck oder einer Zeitplanangabe bestehen. Sie kann auch beides beinhalten.

Zeitplan

Der Zeitplan ('schedule'), sofern angegeben, definiert, wann die Richtlinie in Kraft ist. Der Wert für Datum und Uhrzeit wird durch den lokalen Richtliniendurchsetzungspunkt (PEP) ausgewertet, wobei die Zeitzone des Richtliniendurchsetzungspunkts verwendet wird. Wenn kein Zeitplan angegeben wird, wird die Richtlinie gestartet, sobald sie vom Richtlinienerstellungspunkt (PAP) auf den Richtliniendurchsetzungspunkt heruntergeladen wird. Die Ausführung wird unbegrenzt fortgesetzt.

Der Zeitplan definiert ein optionales Startdatum und ein optionales Stoppdatum, einen optionalen täglichen Zeitrahmen und eine optionale Liste von Wochentagen. Zum Beispiel kann ein Zeitplan so definiert werden, dass die Richtlinie vom 1. Oktober 2012 bis zum 30. Oktober 2012 jeweils von 08:00 bis 17:00 Uhr mittwochs und sonntags in Kraft ist.

Für den Zeitplan können die folgenden Parameter angegeben werden:

- **StartDate** - Dieses optionale Attribut gibt das Datum im xs:date-Format an, an dem der Zeitplan wirksam wird. Das Attribut 'StartDate' wird inklusiv interpretiert. Wenn dieses Attribut nicht vorhanden ist, tritt der Zeitplan unverzüglich am selben Tag in Kraft. (Klicken Sie auf den Hyperlink 'xs:time', um Informationen zu diesem Industriestandard anzuzeigen.)
- **StopDate** - Dieses optionale Attribut gibt das Datum im xs:date-Format an, an dem der Zeitplan beendet wird. Das Attribut 'StopDate' wird exklusiv interpretiert und das angegebene Datum muss nach dem Startdatum liegen. Wenn das Stoppdatum vor dem Startdatum liegt oder mit dem Startdatum identisch ist, wird der Zeitplan nie wirksam. Wenn dieses Attribut nicht angegeben wird, wird der Zeitplan für unbegrenzte Zeit in Kraft gesetzt.
- **Daily** - Dieses optionale Element gibt den täglichen Zeitrahmen an, in dem der Zeitplan in Kraft ist. Wenn dieses Element nicht angegeben wird, ist der Zeitplan für die Dauer des gesamten Tags in Kraft.
  - **StartTime** – Dieses Attribut ist bei Angabe von 'Daily' erforderlich. Es gibt die Uhrzeit im xs:time-Format an, zu der der Zeitplan täglich gestartet wird. (Klicken Sie auf den Hyperlink 'xs:time', um Informationen zu diesem Industriestandard anzuzeigen.)
  - **StopTime** - Dieses Attribut ist bei Angabe von 'Daily' erforderlich. Es gibt die Uhrzeit im xs:time-Format an, zu der der Zeitplan täglich beendet wird. Das Attribut 'StopTime' wird exklusiv interpretiert. Wenn die angegebene Zeit vor der Startzeit liegt oder mit dieser identisch ist, wird der Zeitplan zur angegebenen Zeit am darauf folgenden Tag gestoppt.
- **Weekdays** - Dieses optionale Element gibt die Tage der Woche an, die in den Zeitplan einbezogen werden. Wenn dieses Element nicht angegeben wird, werden alle Wochentage in den Zeitplan einbezogen. Dieses Element betrifft nur den Start des täglichen Zeitrahmens, da Zeitpläne über Mitternacht hinaus ausgeführt werden können. Wenn ein Zeitplan zum Beispiel zum Start um 23:00 Uhr und zur Ausführung für 2 Stunden am Mittwoch eingestellt ist, wird der Zeitplan tatsächlich am Donnerstag um 01:00 Uhr beendet.

– **Days** - Dieses Attribut ist bei Angabe von 'Weekdays' erforderlich. Es listet die Wochentage auf, die in den Zeitplan einbezogen werden. Dies erfolgt in Form einer Liste von Namen, die durch ein Pluszeichen ('+') getrennt werden. Beispiel:
“Monday+Tuesday+Wednesday+Thursday+Friday+Saturday+Sunday”.

Bedingungsausdruck für eine Mediationsrichtlinie

Der Bedingungsausdruck, sofern er angegeben wird, ist ein sich nicht wiederholendes Element, das einen booleschen Ausdruck angibt.

Der Ausdruck enthält drei Parameter: Attribut, Operator und Wert sowie zwei optionale Parameter für ein Intervall und eine Begrenzung. Wenn die Anwendung des Operators mit dem Attribut und dem Wert sowie das Intervall und die Begrenzung, sofern zutreffend, als wahr ausgewertet werden, wird der Ausdruck als wahr ausgewertet. Das Begrenzungselement 'Limit' wird nur in den Operatoren 'HighLow' und 'TokenBucket' verwendet. Wenn es nicht angegeben wird, ist der Wert von Limit gleich 0. Wenn kein Intervall angegeben wird, gilt der Standardwert von 60 Sekunden.

Die folgenden Parameter können für den Ausdruck angegeben werden:

- **Attribut** - In der folgenden Tabelle sind die definierten Attribute mit ihrem jeweiligen Typ aufgeführt.

Tabelle 19. Definierte Attribute

Attribut	Beschreibung und Typ
ErrorCount	Die Anzahl der Fehler, die in diesem Überwachungsintervall festgestellt wurden.
MessageCount	Die Anzahl der tatsächlichen Nachrichten, die während des Überwachungsintervalls abgefangen wurden.
InternalLatency	Die interne Latenzzeit (Verarbeitungszeit) in Sekunden.
BackendLatency	Die Gerät-zu-Server-Latenzzeit in Sekunden.
TotalLatency	Die Summe der Back-End-Latenzzeit und der internen Latenzzeit in Sekunden.

- **Operator** - In der folgenden Tabelle sind die verfügbaren Operatoren und ihre Bedeutung aufgeführt:

Tabelle 20. Operatoren

Operator	Bedeutung
GreaterThan	Ein einfacher numerischer Algorithmus, der das Auswertungsergebnis 'wahr' liefert, wenn das Attribut größer als der definierte Wert ist.
LessThan	Ein einfacher numerischer Algorithmus, der das Auswertungsergebnis 'wahr' liefert, wenn das Attribut kleiner als der definierte Wert ist.

Tabelle 20. Operatoren (Forts.)

Operator	Bedeutung
TokenBucket	Ein ratenbasierter Algorithmus, der eine Geschwindigkeitssteuerung (Bursting) ermöglicht. Der Algorithmus besteht aus einem Bucket (Tokenbehälter) mit einer maximalen Kapazität von 'Limit' Tokens. Der Bucket wird mit einer konstanten Rate von 'Value' Tokens pro Intervall neu gefüllt, während gleichzeitig für jede Attributeinheit ein Token entfernt wird. Dieser Algorithmus liefert das Ergebnis 'wahr', wenn keine Tokens im Bucket vorhanden sind. Ansonsten liefert er das Ergebnis 'falsch'. Das folgende Beispiel soll diesen Algorithmus veranschaulichen. Nehmen Sie folgende Werte an: Limit = 100, Value = 5 und Interval = 1 Sekunde sowie Attribute=MessageCount. 1. Der Bucket beginnt voll mit einer maximalen Kapazität von 100 Tokens. 2. Wenn eine Nachricht eintrifft, überprüft der Algorithmus, ob der Bucket Tokens enthält: a. Ist dies der Fall, liefert der Algorithmus das Ergebnis 'falsch' und ein Token wird aus dem Bucket entfernt. b. Ist dies nicht der Fall, liefert der Algorithmus das Ergebnis 'wahr'. 3. Währenddessen fügt der Algorithmus jede Sekunde je nach Platz fünf Tokens dem Bucket wieder hinzu.
HighLow	Ein Algorithmus, der das Ergebnis 'wahr' liefert, wenn das Attribut den oberen Schwellenwert, der als 'Value' angegeben ist, erreicht, und anschließend so lange das Ergebnis 'wahr' liefert, bis das Attribut den unteren Schwellenwert erreicht, der als 'Limit' angegeben ist.

- **Value** – Dies ist ein Element für den Wert einer positiven ganzen Zahl (Integer). Der Wert “0” ist gültig.
- **Interval** - Dieses optionale Element definiert im xs:duration-Format das Zeitintervall, das als gleitendes Fenster zum Messen des Elements 'wsme:Attribute' bei der Auswertung des Ausdrucks verwendet wird. Wenn dieses Element nicht angegeben wird, wird ein Intervall von 60 Sekunden verwendet. Wenn es angegeben wird, muss ein angemessener Wert angegeben werden, der die konfigurierten Funktionen des Richtliniendurchsetzungspunkts (PEP) berücksichtigt. Das heißt, je höher dieser Wert ist, desto mehr Speicher benötigt der Richtliniendurchsetzungspunkt zur Verfolgung des Attributs. (Klicken Sie auf den Hyperlink 'xs:duration', um Informationen zu diesem Industriestandard anzuzeigen.)
- **Limit** - Dieses optionale Ganzzahlelement definiert das zusätzliche Begrenzungsargument, das erforderlich ist, wenn für 'wsme:Operator' der Operator 'TokenBucket' oder 'HighLow' angegeben wird. Die Einheit hängt vom angegebenen Element 'wsme:Operator' ab.

  Wenn für 'wsme:Operator' der Wert 'HighLow' angegeben wird, definiert dieses Element den unteren Schwellenwert, während 'wsme:Value' den oberen Schwellenwert definiert. Der angegebene Schwellenwert muss niedriger als der für 'wsme:Value' angegebene Wert sein. Wenn es nicht angegeben wird, ist der Standardwert für 'Limit' gleich 0.

  Wenn für 'wsme:Operator' der Wert 'TokenBucket' angegeben wird, definiert dieses Element den maximalen Steigerungswert (Burst) bzw. die maximale

Anzahl von Tokens im Bucket, während 'Value' die Rate als Anzahl von Tokens pro Intervall angibt, mit der der Bucket wieder gefüllt wird. Wenn dieses Element nicht angegeben wird, ist das Standardlimit 0 und 'TokenBucket' ist in diesem Fall mit einer GreaterThan-Operation äquivalent.

Aktionen von Mediationsrichtlinien

Das Mediationsaktionselement gibt die Aktionen an, die auszuführen sind. Obwohl die Syntax viele Kombinationen zulässt, sind nicht alle von ihnen sinnvoll. Wenn widersprüchliche Aktionen angegeben werden, zum Beispiel, dass eine Nachricht sowohl in die Warteschlange gestellt als auch zurückgewiesen werden soll, wird dieses Verhalten vom Richtlinienerstellungspunkt zurückgewiesen. Die folgenden Aktionen sind für Mediationsrichtlinien zulässig:

- **QueueMessage** – Diese Aktion gibt an, dass Transaktionen in die Warteschlange eingereiht werden, wenn die logische Bedingung zutrifft. Die Nachrichtenverarbeitung wird erst wieder begonnen, wenn die logische Bedingung nicht mehr erfüllt ist. Die Warteschlangenmethodik und damit verbundene Zeitlimits werden durch den Richtliniendurchsetzungspunkt definiert. In diesem Fall ist dies WebSphere DataPower. Wenn mehrere Aktionen innerhalb eines Aktionselements angegeben werden, muss 'QueueMessage' die erste Aktion sein.
- **RejectMessage** – Diese Aktion gibt an, dass Transaktionen zurückgewiesen werden, wenn die logische Bedingung zutrifft. Transaktionen werden so lange zurückgewiesen, bis die logische Bedingung nicht mehr zutrifft. Wenn Transaktionen zurückgewiesen werden, wird ein SOAP-Fehler an den Client-Service (Konsumentenservice) zurückgegeben. Wenn mehrere Aktionen innerhalb eines Aktionselements angegeben werden, muss 'RejectMessage' die erste Aktion sein. Die Aktionen 'QueueMessage' und 'RejectMessage' schließen sich gegenseitig aus.
- **Notify** - Dieses optionale Element gibt an, dass eine Benachrichtigung generiert wird, wenn die logische Bedingung zutrifft. Für DataPower wird eine Nachricht in das DataPower-Systemprotokoll geschrieben.
- **RouteMessage** - Dieses optionale Element gibt an, dass Nachrichten an das angegebene Endpunktziel geleitet werden, wenn die logische Bedingung zutrifft. Nachrichten werden so lange an den angegebenen Endpunkt geleitet, bis die logische Bedingung nicht mehr zutrifft.
  - **EndPoint** – Dieser Parameter ist erforderlich, wenn die Aktion 'RouteMessage' angegeben wird. Als Endpunktwert wird eine IP-Adresse, ein Hostname oder ein virtueller Host, zum Beispiel die Lastausgleichsgruppe, unterstützt.
- **ValidateMessage** - Dieses optionale Element gibt an, dass Nachrichten an den angegebenen Grammatiken überprüft werden. Nachrichten werden zurückgewiesen, wenn die Überprüfung fehlschlägt. Wenn 'ValidateMessage' angegeben wird, muss als Unterparameter entweder 'XSD' oder 'WSDL' angegeben werden. 'SCOPE' ist optional. Wenn 'SCOPE' nicht angegeben wird, wird 'SOAPBody' für die Überprüfung verwendet.
  - **XSD** - Gibt an, dass Nachrichten an dem XML-Schema überprüft werden, das durch die enthaltene URI-Adresse angegeben wird.
  - **WSDL** - Gibt an, dass Nachrichten an der Web-Service-Beschreibung (WSDL) überprüft werden, die durch die enthaltene URI-Adresse angegeben wird.
  - **SCOPE** – Gibt an, welcher Teil der Nachricht überprüft wird. In der folgenden Tabelle sind die möglichen Werte mit ihrer Bedeutung aufgeführt:

Tabelle 21. ValidateMessage-Elemente

Wert	Beschreibung
SOAPBody	Der Inhalt des SOAP-Body-Elements ohne besondere Verarbeitung in Bezug auf SOAP-Fehler (Standardwert).
SOAPBodyOrDetails	Der Inhalt des Detailelements für SOAP-Fehler sowie ansonsten der Inhalt des Hauptteils (Body).
SOAPEnvelope	Die gesamte SOAP-Nachricht, einschließlich Umschlag (Envelope).
SOAPIgnoreFaults	Keine Überprüfung, ob die Nachricht ein SOAP-Fehler ist, ansonsten der Inhalt des SOAP-Hauptteils (Body).

- **ExecuteXSL** - Gibt an, dass eine XSL-Transformation mit dem angegebenen Style-Sheet und den angegebenen Parametern ausgeführt wird. Transaktionen werden zurückgewiesen, wenn die Ausführung fehlschlägt. Für 'Style' müssen Informationen angegeben werden, während Informationen für 'Parameter' optional sind und angegeben werden sollten, wie dies für das jeweils angegebene Style-Sheet erforderlich ist.
  - **Stylesheet** - Gibt an, dass die Transformationsoperation das durch die enthaltene URI-Adresse angegebene Style-Sheet verwendet. Das Style-Sheet muss eine XSLT-Datei sein.
  - **Parameter** - Dieses optionale, sich wiederholende Element gibt einen Style-Sheet-Parameter an, der für die ExecuteXSL-Operation zu verwenden ist.
    - **Name** – Dieses Attribut ist für jeden entsprechenden Parameter 'Parameter' erforderlich und gibt den Namen des Parameters an.
    - **Value** - Dieses Attribut ist für jeden entsprechenden Parameter 'Name' erforderlich und gibt den Wert des Parameters an.

Neue Mediationsrichtlinien erstellen

Sie können mit der Business Space-Benutzerschnittstelle neue Mediationsrichtlinien erstellen. Wenn Sie Mediationsrichtlinien verfassen, legen Sie die Bedingungen und Aktionen für die Richtlinie fest.

Vorbereitende Schritte

Informationen zum Zugriff auf Business Space finden Sie in „Verbindung zu WSRR herstellen - Business Space” auf Seite 86.

Der SOA Governance-Space muss erstellt werden, bevor Richtlinien erstellt werden können. Wenn der SOA-Governance-Space noch nicht vorhanden ist, finden Sie Informationen in „Business Space für die Erstverwendung konfigurieren” auf Seite 87. Führen Sie die beschriebenen Schritte aus, um den Space zu erstellen.

Außerdem müssen Sie Business Space für die Erstellung von WS-MediationPolicy 1.7-Mediationsrichtlinien im "Actions"-Widget konfigurieren. Siehe Widget "Service Registry Actions".

Informationen zu diesem Vorgang

Verfassen Sie neue Richtlinien mit dem SOA-Governance-Space.

Vorgehensweise

1. Öffnen Sie den SOA-Governance-Space:
   a. Klicken Sie auf **Go To Spaces**. Der Dialog 'Go To Spaces' wird angezeigt.
   b. Klicken Sie auf den Space für SOA-Governance-Benutzer. Der jeweilige Name hängt davon ab, was bei der Erstellung des Space angegeben wurde.
2. Klicken Sie auf der Registerkarte 'Overview' auf **Create a Mediation Policy**.
3. Geben Sie einen aussagekräftigen Namen und eine optionale Beschreibung ein.
4. Fügen Sie Bedingungen und Aktionen nach Bedarf hinzu. Weitere Informationen zu den Bedingungen und Aktionen finden Sie in „Richtlinien" auf Seite 97 und im Information Center von IBM WebSphere Service Registry and Repository Version 8.0 - Mediationsrichtlinie erstellen.
5. Klicken Sie auf **Finish**.

Ergebnisse

Die Richtlinie wurde erstellt und in WSRR gespeichert. Zum Anzeigen des Richtliniendokuments für die Richtlinie, die Sie erstellt haben, wählen Sie das Richtliniendokument im Widget 'Service Registry Navigator' aus. Alternativ können Sie nach dem Namen (einschließlich der Dateinamenerweiterung `.xml`) suchen, den Sie angegeben haben. Das Richtliniendokument wird im Widget 'Service Registry Detail' auf der rechten Seite angezeigt.

Zugehörige Konzepte:

„Richtlinien" auf Seite 97
In diesem Abschnitt werden Implementierungsdetails für die Verwendung von WSRR als Richtlinienerstellungspunkt (PAP, Policy Authoring Point) und WebSphere DataPower als Richtliniendurchsetzungspunkt (PEP, Policy Enforcement Point) bei der Erstellung von Mediationsrichtlinien beschrieben.

Zugehörige Informationen:

Information Center von IBM WebSphere Service Registry and Repository Version 8.0 - Mediationsrichtlinie erstellen

Neue Überwachungsrichtlinien erstellen

Sie können mit der WSRR-Webbenutzerschnittstelle neue Überwachungsrichtlinien erstellen. Wenn Sie Überwachungsrichtlinien verfassen, legen Sie die Bedingungen und Aktionen für die Richtlinie fest.

Vorbereitende Schritte

Informationen zum Zugriff auf die WSRR-Webbenutzerschnittstelle finden Sie in „Verbindung zu WSRR herstellen - WSRR-Webbenutzerschnittstelle" auf Seite 88.

Vorgehensweise

1. Öffnen Sie die WSRR-Webbenutzerschnittstelle.
2. Klicken Sie auf **View** > **Service Documents** > **Policy Documents** und klicken Sie in der Ansicht 'Collection' auf **New**.
3. Wählen Sie aus der Liste der Richtlinien-Frameworks die Option **Monitoring** aus. Klicken Sie auf **Next**. Dadurch wird ein Richtliniendokument mit einem Rootrichtlinienausdruck erstellt.
4. Geben Sie einen aussagekräftigen Namen und eine optionale Beschreibung ein.

5. Klicken Sie auf die Registerkarte 'Policy' und auf **Edit policy document** und fügen Sie dann die gewünschten Bedingungen und Aktionen zu. Weitere Informationen zu den Bedingungen und Aktionen finden Sie in den zugehörigen Links.
6. Klicken Sie auf **Publish**.

Ergebnisse

Die Richtlinie wurde erstellt und in WSRR gespeichert. Sie können das Richtliniendokument für die Richtlinie in Business Space anzeigen: Wählen Sie das Richtliniendokument im Widget 'Service Registry Navigator' aus. Alternativ können Sie nach dem Namen (einschließlich der Dateinamenerweiterung `.xml`) suchen, den Sie angegeben haben. Das Richtliniendokument wird im Widget 'Service Registry Detail' auf der rechten Seite angezeigt.

Zugehörige Konzepte:

„Richtlinien" auf Seite 97
In diesem Abschnitt werden Implementierungsdetails für die Verwendung von WSRR als Richtlinienerstellungspunkt (PAP, Policy Authoring Point) und WebSphere DataPower als Richtliniendurchsetzungspunkt (PEP, Policy Enforcement Point) bei der Erstellung von Mediationsrichtlinien beschrieben.

Zugehörige Informationen:

Richtlinienerstellungstasks

Mit dem Richtlinienerstellungstool arbeiten

Richtlinien verwalten

Richtlinien können über die Business Space-Benutzerschnittstelle bearbeitet oder entfernt werden.

Vorbereitende Schritte

Konfigurieren Sie den SOA-Governance-Space. Weitere Informationen finden Sie in „Business Space für die Erstverwendung konfigurieren" auf Seite 87.

Vorgehensweise

1. Zum Öffnen des Richtliniendokuments für die Richtlinie wählen Sie das Richtliniendokument im Widget 'Service Registry Navigator' in der linken unteren Ecke der Anzeige aus. Alternativ können Sie nach dem Namen (einschließlich der Dateinamenerweiterung `.xml`) suchen, den Sie angegeben haben. Das Richtliniendokument wird im Widget 'Service Registry Detail' auf der rechten Seite angezeigt.
2. Gehen Sie wie folgt vor, um die Richtliniendetails zu ändern:
   a. Klicken Sie auf das Bearbeitungssymbol in diesem Widget, um das Richtliniendokument zu bearbeiten. Ein Fenster mit Optionen zum Bearbeiten der Richtliniendetails wird angezeigt.
   b. Wenn die Richtlinie Bedingungen oder Aktionen enthält, werden diese angezeigt. Erstellen und ändern Sie Bedingungen und Aktionen nach Bedarf.
   c. Klicken Sie auf **Finish**, um die Änderungen zu speichern und den Richtlinieneditor zu schließen. Das Widget 'Service Registry Detail' wird aktualisiert, um die vorgenommenen Änderungen anzuzeigen.
3. Gehen Sie wie folgt vor, um die Richtlinie zu löschen:

a. Versetzen Sie die Richtlinie durch einen Übergang in einen Governance-Zustand, der das Bearbeiten oder Löschen des Richtliniendokuments zulässt. Weitere Informationen zur Ausführung von Übergängen für eine Richtlinie durch den SOA-Richtlinienzyklus finden Sie in „Lebenszyklus der Richtlinie verwalten".
b. Klicken Sie auf **Action** > **Delete**. Die Löschoption wird im Menü aufgeführt.
c. Wählen Sie **Delete** aus, um die Richtlinie zu löschen.
d. Klicken Sie auf **Yes**, um die Löschung zu bestätigen.

Zugehörige Informationen:

Information Center von IBM WebSphere Service Registry and Repository Version 8.0

Information Center von IBM WebSphere Service Registry and Repository Version 8.0 - Richtlinien im Governance-Realisierungsprofil

Lebenszyklus der Richtlinie verwalten

Richtlinien können in der Business Space-Benutzerschnittstelle durch Übergänge von einem Governance-Zustand in einen anderen versetzt werden. Die Richtlinien müssen sich im Zustand 'Approved' befinden, damit sie von DataPower durchgesetzt werden können.

Informationen zu diesem Vorgang

Weitere Informationen zur Governance finden Sie in „SOA Policy-Lebenszyklus" auf Seite 5.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um den Übergang einer Richtlinien zu einem anderen Lebenszykluszustand auszuführen. Wiederholen Sie diese Schritte so oft, wie es erforderlich ist, um den gewünschten Lebenszykluszustand zu erreichen:

1. Öffnen Sie in Business Space das Richtliniendokument für die Richtlinie, indem Sie das Richtliniendokument im Widget 'Service Registry Navigator' auswählen. Alternativ können Sie nach dem Namen (einschließlich der Dateinamenerweiterung `.xml`) suchen, den Sie angegeben haben. Das Richtliniendokument wird im Widget 'Service Registry Detail' angezeigt. Die Eigenschaft **Governance state** zeigt den aktuellen Governance-Zustand für das Profil an.
2. Klicken Sie auf **Action**. Eine Liste der möglichen Lebenszyklusübergänge wird zusammen mit anderen möglichen Operationen angezeigt.
3. Wählen Sie den erforderlichen Lebenszyklusübergang aus, um die Richtlinie in den erforderlichen Zustand zu versetzen. Die Eigenschaft **Governance state** der Richtlinie wird aktualisiert, um den neuen Lebenszykluszustand anzuzeigen.

Zugehörige Konzepte:

„SOA Policy-Lebenszyklus" auf Seite 5
Richtlinien werden durch den SOA Policy-Lebenszyklus geregelt. Der Lebenszyklus definiert die verschiedenen Phasen, in denen eine Richtlinie zu Anfang erkannt wird, später in einer Produktionsumgebung implementiert wird und schließlich außer Funktion gesetzt wird, wenn sie nicht mehr erforderlich ist.

Zugehörige Informationen:

Information Center von IBM WebSphere Service Registry and Repository Version 8.0 - SOA-Richtlinienlebenszyklus

Einem Service zugeordnete Richtlinien

Richtlinien können in WSRR einem Service zugeordnet werden.

Weitere Informationen finden Sie im Information Center von IBM WebSphere Service Registry and Repository Version 8.0 - Richtlinienzuordnungstasks.

Kapitel 7. Fehlerbehebung

Nutzen Sie die Unterstützung bei der Diagnose von Problemen, die vor, bei und nach der Implementierung eines Musters auftreten können.

Über die Links finden Sie Themen, die für die Behebung eines Problems mit den Mustern relevant sind.

Fehlerbehebung bei Problemen mit der Implementierung

Sie können eine Fehlerbehebung bei Problemen durchführen, die bei der Implementierung der Muster in IBM SOA Policy Gateway Pattern auftreten können.

Verbindung zum externen DataPower-Gerät wird während der Implementierung nicht hergestellt

Versuchen Sie die folgenden Lösungen:

- Überprüfen Sie zusammen mit dem DataPower-Administrator, ob der Benutzer und das Kennwort gültig sind:
  - Überprüfen Sie in der DataPower-Web-GUI, ob der Benutzer vorhanden ist, indem Sie zu **Control Panel** > **Manage User Accounts** navigieren.
  - Überprüfen Sie, ob der Benutzer vorhanden ist.
  - Überprüfen Sie, ob der Benutzer berechtigt ist, XML Management Interface zu verwenden. Er muss zum Beispiel die Systemadministratorberechtigung besitzen.
  - Der DataPower-Administrator muss möglicherweise überprüfen, ob das Benutzerkonto in den Benutzeragenteneinstellungen, zum Beispiel in den Einstellungen der Basisauthentifizierung (Basic Authentication Settings), aktiviert ist.
- Überprüfen Sie, ob der DataPower-Hostname korrekt ist.
- Überprüfen Sie, ob XML Management Interface in DataPower aktiviert ist.

Fehlerbehebung bei einem Fehler wegen bereits vorhandener Domäne

Versuchen Sie die folgende Lösung:

- Öffnen Sie im DataPower Control Panel die Option 'Application Domains'. Überprüfen Sie, ob die Domäne bereits vorhanden ist.

Fehlerbehebung bei Portüberschneidungsfehler für die Beispielanwendung

Wenn einer der Beispielservices nicht verfügbar ist, überprüfen Sie, ob die Ports in Ihrer Domäne mit anderen Domänen im Konflikt stehen.

Versuchen Sie die folgenden Lösungen:

- Melden Sie sich bei DataPower an und wechseln Sie zur Beispieldomäne. Öffnen Sie anschließend die Anzeige 'Control Panel' und klicken Sie auf das Symbol für die XML-Firewall. Stellen Sie sicher, dass die XML-Firewalls alle einen aktiven Status haben.
- Suchen Sie nach 'HTTP Front Side Handler'. Überprüfen Sie, ob sich der einzelne HTTP-Front-Side-Handler im aktiven Status befindet.

Fehlerbehebung bei einem Umstufungsfehler (Promotionsfehler)

Es können zahlreiche Probleme bei einer Umstufung (Promotion) auftreten. Dazu gehören auch Fehler bei der Verbindung zum Governance Master während der Implementierung.

Versuchen Sie die folgenden Lösungen:

- Überprüfen Sie die Parameter:
  - Überprüfen Sie den Benutzer der WSRR-Zelle für den Governance Master (WSRRCELL).
  - Überprüfen Sie das Kennwort für den Benutzer der WSRR-Zelle für den Governance Master.
  - Überprüfen Sie den Hostnamen der WSRR-Zelle für den Governance Master.
  - Überprüfen Sie den Zellennamen der WSRR-Zelle für den Governance Master.
- Überprüfen Sie den Austausch der Unterzeichnerzertifikate:
  - Navigieren Sie zum Standardtruststore der Governance Master-Zelle (CellDefaultTrustStore) und stellen Sie sicher, dass ein Zertifikatseintrag für den Deployment Manager (Dmgr) oder den eigenständigen Server der Laufzeitumgebung vorhanden ist.
  - Prüfen Sie in jeder Laufzeitumgebung den Standardtruststore 'CellDefaultTruststore' der Zelle (im Fall einer Network Deployment-Umgebung) oder den Standardtruststore 'NodeDefaultTrustStore' des Knotens (für eigenständige WSRR-Server), um sicherzustellen, dass ein Zertifikat für den Dmgr des Governance Masters vorhanden ist.
  - Exportieren Sie die LTPA-Schlüssel aus beiden Zellen mit demselben Kennwort und überprüfen Sie, ob sie identisch sind (z. B. die Byte).
- Stellen Sie sicher, dass die Promotionseigenschaftendatei Serverabschnitte mit dem entsprechenden Informationen zu Host und Port sowie zu Benutzer und Kennwort enthält. Diese Informationen sind in der Service-Registry-Konsole für den Governance Master zu finden:
  - Navigieren Sie zu 'GovernanceMasterDMgrHost' oder 'ServiceRegistry' und wechseln Sie zur Perspektive für Konfigurationen ('Configurations'). Suchen Sie im Abschnitt 'Actions' den Eintrag **Promotion** und öffnen Sie die Promotionseigenschaftendatei. Für jede Umgebung sollten XML-Elemente für jeden Server im WSRR-Staging-Knoten oder -Cluster vorhanden sein. Wenn ein Cluster oder Knoten vom Typ 'production' vorhanden ist, sollten Einträge 'server:port' für jeden vorhanden sein und es sollten Benutzer- und Kennwortinformationen vorhanden sein.
- Überprüfen Sie, ob die Serviceversion und der SOAP-Endpunkt beide die Klassifikation für 'Staging' und 'Production' haben.
  - Wählen Sie in der Service-Registry-Konsole die SOA-Governance-Perspektive aus. Öffnen Sie die Serviceversion und wählen Sie die Registerkarte für Klassifikationen ('Classifications') aus. Die Werte 'Staging' und 'Production' müssen aktiviert sein.

Fehlerbehebung bei Fehlern mit der angepassten CLI

Versuchen Sie die folgenden Lösungen:

- Überprüfen Sie die Datei 'defaultLog' auf Fehlernachrichten in der DataPower-Domäne.
- Aktivieren Sie das CLI-Debugging und überprüfen Sie die entsprechenden Protokolle, bevor Sie die CLI ein weiteres Mal ausführen.

Fehlerbehebung bei Problemen in der implementierten Instanz

Sie können eine Fehlerbehebung bei häufig auftretenden Problemen in der implementierten Instanz durchführen.

Fehlgeschlagene Verbindungen zum LDAP-Server oder zum StoreWSP-Port in DataPower

Es liegen möglicherweise Probleme mit den Domäneneinstellungen vor, wenn die DataPower-Protokolle einen Verbindungsfehler zeigen, der mit dem LDAP-Server oder dem StoreWSP-Gateway aufgetreten ist, und wenn Sie den Hostaliasnamen verwenden. Beispiel: `xyz` anstelle des vollständig qualifizierten Hostnamens `xyz.company.com`. Davon kann einer der folgenden Parameter im Scriptpaket betroffen sein:

- DataPower-Hostname
- LDAP-Hostname

Versuchen Sie die folgende Lösung:

1. Wechseln Sie in der DataPower-Administrationskonsole zur Standarddomäne.
2. Suchen Sie nach `Configure DNS Settings`.
3. Klicken Sie auf die Registerkarte 'Search Domains'.
4. Stellen Sie sicher, dass Ihre Domäne, zum Beispiel `company.com`, in der Liste enthalten ist. Falls sie nicht in der Liste enthalten ist, klicken Sie auf `Add` und fügen sie der Liste hinzu.

Probleme mit der Überwachung

Wenn auf den implementierten Knoten keine Überwachung verfügbar ist, müssen Sie überprüfen, dass die erforderlichen, gemeinsam genutzten Services ausgeführt werden. Navigieren Sie zu **Instances** > **Shared Services**.

Überprüfen Sie, ob System Monitoring und System Monitoring for WebSphere DataPower in derselben Cloudgruppe wie Ihre implementierten Instanzen ausgeführt werden. Überprüfen Sie für die WSRR-Überwachung auch, ob System Monitoring for WebSphere Application Server in Ihrer Cloudgruppe ausgeführt wird.

Diagnoseinformationen erfassen

Mithilfe von Protokollen können Sie Probleme ermitteln und untersuchen. Protokolle werden auf dem Gerät gespeichert und können über die Benutzerschnittstelle angezeigt werden. Alternativ können sie auch in das lokale Dateisystem heruntergeladen werden.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um Diagnoseinformationen zusammenzustellen:

1. Zeigen Sie die virtuellen Instanzen an:
   a. Klicken Sie auf **Instances** > **Virtual system**.
   b. Wählen Sie die Instanz in der Instanzliste im Fenster **Virtual System Instances** aus.
2. Für die virtuelle WSRR-Maschine:
   a. Erweitern Sie im Abschnitt **Virtual machines** die virtuelle WSRR-Maschine und untersuchen den Abschnitt **Script Packages** (Scriptpakete) auf Fehler. Wenn Scriptpakete Fehler haben, klicken Sie auf die Protokolllinks für **remote_std_out.log** und **remote_std_err.log** neben den Namen der Scriptpakete.
   b. Melden Sie sich an der WSRR-Instanz an und prüfen Sie die Serverfehler.
   c. Ziehen Sie die Informationen der WSRR-Fehlerbehebungshandbücher zu Rate: http://pic.dhe.ibm.com/infocenter/sr/v8r0/topic/com.ibm.sr.doc/cwsr_troubleshootingandsupport.html
3. Für DataPower:
   a. Rufen Sie die Datei **default.log** für die Domäne ab, die vom Muster erstellt wurde.
   b. Rufen Sie die Datei **default.log** für die Standarddomäne ab.
4. Erfassen Sie bei Überwachungsproblemen diese Protokolle vom Basisbetriebssystem und von den WSRR-Knoten (außer von den angepassten WSRR-Knoten):
   - `/0config/0config.log`
   - `/opt/IBM/maestro/ITCAMSOADP/lx8266/d4/KD4/logs/*` (x86)
   - `/opt/IBM/maestro/ITCAMSOADP/aix523/d4/KD4/logs/*` (Power)

Kapitel 8. Service und Unterstützung

Sie können Wartungsfunktionen wie das Anwenden provisorischer Änderungen ('Emergency Fixes') ausführen.

Provisorische Änderung dem Katalog hinzufügen

Vorläufige Fixes und Fixpacks werden auf virtuelle Systeminstanzen in Form von provisorischen Änderungen ('Emergency Fixes') angewendet. Sie können provisorische Änderungen Ihrem Katalog hinzufügen, der auf Ihre virtuellen Images anzuwenden ist.

Vorbereitende Schritte

Sie müssen die Berechtigung *Create new catalog content* oder die Rolle *Administrator* im IBM Workload Deployer-Gerät mit vollständigen Berechtigungen haben, um diese Schritte ausführen zu können.

Informationen zu diesem Vorgang

Fixes werden von IBM oder einem Image-Provider bereitgestellt und müssen heruntergeladen werden. Neue Fixes werden von IBM Fix Central heruntergeladen. Die Fixes werden anschließend in den Katalog hochgeladen und können auf alle gültigen virtuellen Systeminstanzen angewendet werden.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine provisorische Änderung ('Emergency Fix') auf Ihren Katalog anzuwenden.

1. Lokalisieren Sie die provisorische Änderung (bzw. Änderungen) auf Fix Central.
2. Optional: Sie können mehrere vorläufige Fixes gleichzeitig hinzufügen. Wenn Sie mehrere Fixes gleichzeitig hinzufügen möchten, laden Sie die komprimierten Dateien von Fix Central herunter und packen sie in eine komprimierte Datei zusammen.
3. Wählen Sie im Menü die Optionen **Catalog** > **Emergency Fixes** aus.
4. Klicken Sie auf das Symbol zum Hinzufügen auf der linken Anzeige.
5. Geben Sie einen Namen für den hinzuzufügenden Fix ein. Optional können Sie auch eine Beschreibung des Fix hinzufügen. Der Fix wird in der linken Anzeige des Fensters **Emergency Fixes** angezeigt. Informationen zu dem Fix werden auf der rechten Anzeige angezeigt.
6. Navigieren Sie zu der Position, an der Sie den Fix gespeichert haben, und klicken Sie auf **Upload**. Aus Sicherheitsgründen können nur Dateien der Typen .zip, .tgz und .pak hochgeladen werden. Red Hat RPM wird ebenfalls unterstützt.
7. Füllen Sie die Informationen zu dem Fix aus. Sie können Benutzern Zugriff erteilen und eine Sicherheitseinstufung angeben. Geben Sie im Feld **Applicable to** das virtuelle Image bzw. die virtuellen Images an, für die dieser Fix gilt.

Ergebnisse

Die provisorische Änderung befindet sich jetzt im Katalog und steht für die Anwendung auf virtuelle Systemimages zur Verfügung.

Provisorische Änderung anwenden

Vorläufige Fixes und Fixpacks werden auf virtuelle Systeminstanzen in Form von provisorischen Änderungen ('Emergency Fixes') angewendet. Sie können provisorische Änderungen auf Ihre virtuellen Systemimages anwenden.

Vorbereitende Schritte

Sie müssen über den Gesamtzugriff auf die virtuelle Systeminstanz verfügen oder die Geräteadministratorrolle mit vollständigen Berechtigungen besitzen, um diese Schritte ausführen zu können. Die virtuelle Systeminstanz muss gestartet sein, damit die Wartung terminiert oder angewendet werden kann. Die provisorische Änderung muss dem Katalog hinzugefügt werden, bevor sie auf ein virtuelles System angewendet werden kann.

Informationen zu diesem Vorgang

Wenn Sie eine provisorische Änderung hinzufügen, definieren Sie die virtuellen Images, auf die die Änderung anwendbar ist. Wenn Sie eine Serviceanforderung terminieren, wird die Liste der verfügbaren Änderungen aus allen Änderungen zusammengestellt, die auf das virtuelle Image anwendbar sind, das zum Erstellen Ihrer virtuellen Systeminstanz verwendet wurde. Wenn bereits eine provisorische Änderung auf Ihr virtuelles System angewendet wurde, wird sie in der Verlaufsliste (**History**) aufgeführt und ist nicht in der Liste der verfügbaren provisorischen Änderungen enthalten.

Anmerkung: Sie müssen alle WSRR- und WAS-Prozesse beenden, bevor Sie eine provisorische Änderungen installieren können. Melden Sie sich über SSH bei allen WSRR-Knoten an und beenden Sie alle Prozesse mit den Befehlen **`stopServer.sh`** und **`stopNode.sh`** (nur angepasste Knoten).

Vorgehensweise

Führen Sie die folgenden Schritte aus, um einen vorläufigen Fix anzuwenden.

1. Wählen Sie im Fenster **Virtual System Instances** die virtuelle Systeminstanz aus, auf die der Fix angewendet werden soll.
2. Klicken Sie auf das Symbol zum Anwenden des Service (**Apply service**).
3. Optional: Terminieren Sie eine Serviceanforderung. Standardmäßig wird der Fix unverzüglich angewendet. Zur Terminierung der Anwendung zu einem späteren Zeitpunkt klicken Sie auf **Schedule service** und geben die erforderlichen Informationen an.
4. Klicken Sie auf **Select service level or fixes**.
5. Klicken Sie auf **Apply emergency fixes**, um den Fix anzuzeigen und zur Anwendung auszuwählen. Die provisorische Änderung wird auf alle virtuellen Maschinen in der virtuellen Systeminstanz angewendet. Der Status der virtuellen Systeminstanz zeigt an, dass der Service auf das virtuelle System angewendet wurde.

6. Prüfen Sie auf Fehler. Prüfen Sie die folgenden Dateien, um sicherzustellen, dass während der Anwendung der provisorischen Änderungen keine Fehler aufgetreten sind:
   - Remote_std_out.log
   - Remote_std_err.log

   Sie können auf die Protokolldateien über das Fenster **Virtual System Instances** zugreifen.

Kapitel 9. Appendices

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

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

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

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

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:
INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION „AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

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

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Programming interface information

Programming interface information, if provided, is intended to help you create application software for use with this program.

However, this information may also contain diagnosis, modification, and tuning information. Diagnosis, modification and tuning information is provided to help you debug your application software.

Important: Do not use this diagnosis, modification, and tuning information as a programming interface because it is subject to change.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at Copyright and trademark information (www.ibm.com/legal/copytrade.shtml).

Sending your comments to IBM

If you especially like or dislike anything about this book, please use one of the methods listed below to send your comments to IBM.

Feel free to comment on what you regard as specific errors or omissions, and on the accuracy, organization, subject matter, or completeness of this book.

Please limit your comments to the information in this book and the way in which the information is presented.

To make comments about the functions of IBM products or systems, talk to your IBM representative or to your IBM authorized remarketer.

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate, without incurring any obligation to you.

You can send your comments to IBM in any of the following ways:

- By mail, to this address:

  User Technologies Department (MP095)
  IBM United Kingdom Laboratories
  Hursley Park

WINCHESTER,
Hampshire
SO21 2JN
United Kingdom

- By fax:
  - From outside the U.K., after your international access code use 44-1962-816151
  - From within the U.K., use 01962-816151
- Electronically, use the appropriate network ID:
  - IBM Mail Exchange: GBIBM2Q9 at IBMMAIL
  - IBMLink: HURSLEY(IDRCF)
  - Internet: idrcf@hursley.ibm.com

Whichever method you use, ensure that you include:

- The publication title and order number
- The topic to which your comment applies
- Your name and address/telephone number/fax number/network ID.