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. SOA-Verfahren (SOA, Service Oriented Architecture - serviceorientierte Architektur) unterstützen Unternehmen bei der Ermittlung und Konzentration auf die wichtigsten Services für das Geschäft. Durch Hinzufügen von Richtlinien werden Punkte zur Steuerung und zur Steigerung der Beweglichkeit der Geschäftsabläufe und der Informationstechnologie hinzugefügt. Im Ergebnis macht SOA die Umgebung verbraucherfreundlicher, verbessert die Wertschöpfungszeit für Geschäftsbenutzer durch geringere Kosten für Projekte und beschleunigt die Einführung neuer SOA-Lösungen.

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 Richtlinienerstellungspunkt (PAP), dem Richtliniendurchsetzungspunkt (PEP), dem Richtlinienentscheidungspunkt (PDP), dem Richtlinieninformationspunkt (PIP) und dem Richtlinienüberwachungspunkt (PMP). In diesem Muster wird der Richtlinienerstellungspunkt (PAP) mithilfe von WSRR und der Richtliniendurchsetzungspunkt (PEP) mithilfe von WebSphere DataPower realisiert.

Die grundlegende Richtlinienarchitektur ist wie folgt aufgebaut:

- **Richtlinienerstellungspunkt** - Ein Richtlinienerstellungspunkt (PAP, Policy Authoring 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. Er enthält ein Repository zum Speichern von Richtlinien. In diesem Muster wird er mithilfe von WSRR realisiert.
- **Richtliniendurchsetzungspunkt** - Ein Richtliniendurchsetzungspunkt (PEP, Policy Enforcement Point) ist ein Funktionspunkt, der auf der Middleware ausgeführt wird, die folgende Aufgaben hat:
  - 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 tatsächlich angewendet und durchgesetzt werden, abhängig von der Lebenszyklusphase:
    - Während der Entwicklungszeit ist WebSphere Service-Registry and Repository 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 diese Funktion durch WebSphere DataPower realisiert.

- **Richtlinienentscheidungspunkt** - Ein Richtlinienentscheidungspunkt (PDP, Policy Decision Point) wertet teilnehmende Anforderungen anhand der relevanten Richtlinien oder anhand von Verträgen und Attributen aus. Er 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. Dazu gehören die folgenden Funktionen:
  - 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.

Anmerkung: Die Überwachung ist in diesem Muster nicht enthalten.

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

Funktionsweise der SOA-Richtlinienarchitektur

Der umsetzbare SOA Policy-Musterablauf wird in Abb. 1 auf Seite 3 dargestellt und nachfolgend beschrieben.

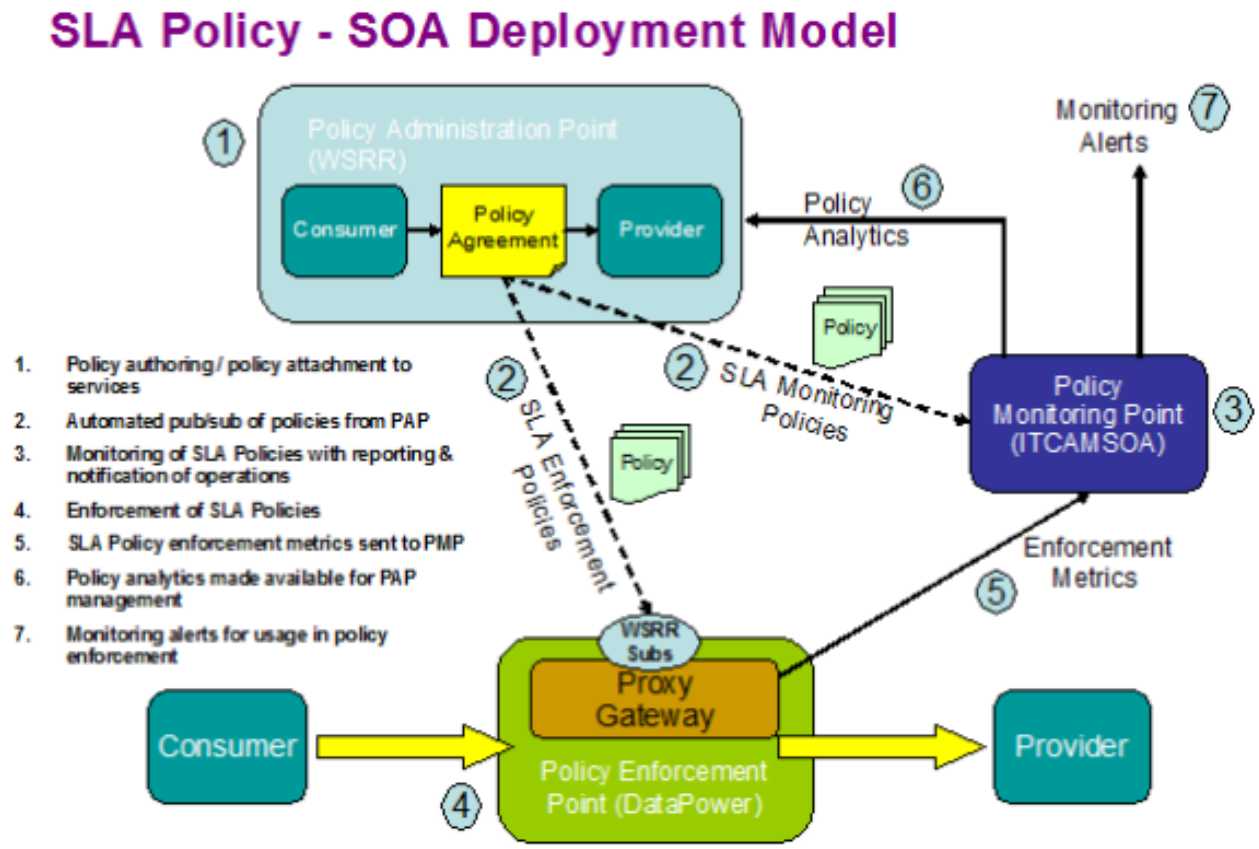


Abbildung 1. Service Level Agreement-Richtlinie (SLA-Richtlinie) - SOA-Implementierungsmodell

1. Richtlinien werden erstellt und anschließend den Services zugeordnet, für die die Richtlinie erforderlich ist. In der Regel geschieht dies in der folgenden Reihenfolge:
   a. Die Gruppe von Services wird in das Service-Repository geladen oder dort erstellt. Dies ist ein Aufgabenbereich des Richtlinienerstellungspunkts (PAP).
   b. Die Gruppe der erforderlichen Richtlinien wird im Richtlinienerstellungspunkt unter Verwendung des Richtlinienlebenszyklus erstellt:
      1) Richtlinien werden den Services zugeordnet, die diese Richtlinien erfordern - je nach Bedarf auf Service-, Operations- oder Endpunktebene.
2. Automatisierte Veröffentlichung/Subskription von Richtlinien vom Richtlinienerstellungspunkt (PAP) zu den Richtliniendurchsetzungspunkten und dem Richtlinienüberwachungspunkt:

   Anmerkung: Die Überwachung mit ITCAM for SOA ist in diesem Muster nicht enthalten.
   a. Im Rahmen der Konfiguration subskribiert ITCAM for SOA die Überwachungsrichtlinie in WSRR. Dies erfolgt nur einmal.
   b. Im Rahmen der Konfiguration werden Proxy-Gateways in jedem WebSphere DataPower-Gerät erstellt, das Servicetransaktionen mit Richtliniendurchsetzung hat. Dies erfolgt nur einmal und wird nach Bedarf hinzugefügt oder geändert.

c. Im Rahmen der Konfiguration subskribiert jedes Proxy-Gateway im Gerät Richtlinien in WSRR für Services, für die es zuständig ist. Dies erfolgt nur einmal und wird nach Bedarf hinzugefügt oder geändert.

d. Im Rahmen der Konfiguration wird WebSphere DataPower so konfiguriert, dass Richtlinien von anderen Geräten in einem Cluster gemeinsam genutzt werden können. Dies erfolgt nur einmal und wird nach Bedarf hinzugefügt oder geändert.

e. ITCAM for SOA lädt die Überwachungsrichtlinien herunter, wenn sie veröffentlicht werden.

f. ITCAM for SOA konvertiert die Richtlinien in die interne Darstellung, die als Situationsrichtlinien bezeichnet werden.

g. WebSphere DataPower lädt die WSDLs für Services herunter, für deren Transaktionen es zuständig ist.

h. WebSphere DataPower lädt die Richtlinien für Services herunter, für die es zuständig ist, wenn es von WSRR benachrichtigt wird.

i. WebSphere DataPower konvertiert die Richtlinien in die interne WebSphere DataPower-Darstellung in Form von SLM-Objekten.

3. Überwachung von SOA-Richtlinien mit Berichten und Benachrichtigungen zu Operationen:
   a. Überwachungsrichtlinien sind in der ITCAM for SOA-Situationsrichtlinie aktiv.
   b. ITCAM for SOA empfängt Überwachungsdaten und fügt diese Daten in Arbeitsbereiche ein.

   Anmerkung: Die Überwachung wird in diesem Muster nicht bereitgestellt.
4. Durchsetzung von SOA-Richtlinien:
   a. Durchsetzungsrichtlinien sind in den verschiedenen WebSphere DataPower-Geräten aktiv.
   b. WebSphere DataPower empfängt Servicetransaktionen und wendet Richtlinien für den jeweiligen Konsumentenservice und Provider-Service an.
5. Der Richtliniendurchsetzungspunkt sendet Statistikdaten zur SOA-Richtliniendurchsetzung an den Richtlinienüberwachungspunkt.

   Anmerkung: Die Überwachung ist in diesem Muster nicht enthalten.
6. Der Richtlinienüberwachungspunkt sendet Überwachungsereignisse an den Richtlinienerstellungspunkt:
   a. Ereignisse werden im Richtlinienerstellungspunkt konfiguriert, die vom Richtlinienüberwachungspunkt aus überwacht werden müssen. Dies erfolgt nur einmal und wird nach Bedarf hinzugefügt oder geändert.
   b. Wenn Situationsrichtlinien als wahr ausgewertet werden, werden Ereignisse vom Richtlinienüberwachungspunkt an den Richtlinienerstellungspunkt übertragen.

   Anmerkung: Die Überwachung ist in diesem Muster nicht enthalten.
7. Überwachung von Alerts:
   a. 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

Mediationsrichtlinien 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 den Bedarf an einer Definition einer für Web-Services anwendbaren Richtlinie zu bedienen.

- **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/WSMediationPolicy1.6-20120124.pdf.

Das WS-Policy-Datenmodell enthält folgende Elemente:

- **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. Dieses Element 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 obigen Richtlinie wäre 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 auf Seite 7 zeigt eine Richtliniendefinition.

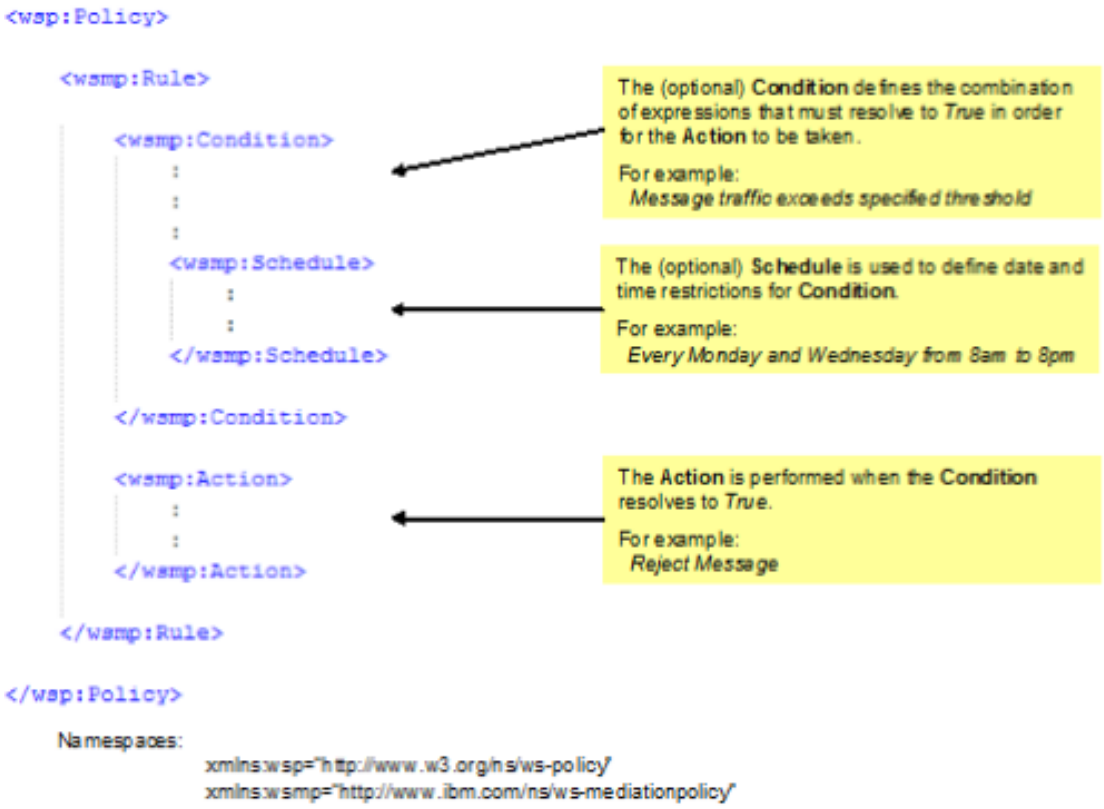


Abbildung 3. Übersicht über die Richtlinienstruktur

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 auf Seite 7 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. 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 wird durch das WebSphere DataPower-Gerät bereitgestellt, in dem bei der Implementierung des Musters für ein virtuelles System eine Domäne erstellt wird.

Es gibt Beispiele für Richtlinien in vielen, wenn nicht sogar in allen, SOA-Umgebungen (SOA - Service Orientated Architecture, serviceorientierte Architektur). Produzenten und Konsumenten von Services stimmen sich über die Funktionalität, die Leistung und die Merkmale eines Service während der Entwurfsphase ab. Zu diesem Zweck können Sie Service-Level-Definitionen (SLD) und Service-Level-Agreements (SLA) verwenden. Dieses Muster bietet Ihnen die Möglichkeit, Richtlinien für SLDs und SLAs in einer effizient verwalteten, definierten, geregelten und erprobten Weise zu definieren. 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 werden die Verfahren zur Durchsetzung der XACML-Zugriffssteuerungssicherheitsrichtlinien demonstriert. Diese werden gegenwärtig im Richtlinienverwaltungspunkt nicht durch Governance-Richtlinien geregelt.

IBM SOA Policy Gateway Pattern enthält die folgenden Muster für virtuelle Systeme:

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

Die vier Muster 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. Durch eine entsprechende Kombination lassen sich die folgenden Implementierungstopologien bereitstellen:

- Eigenständige Implementierung
- Pilotimplementierung

- Vollständige Implementierung in der Produktionsumgebung

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

Es ist möglich, das implementierte Muster für ein virtuelles System manuell zu konfigurieren, um eine Überwachung mithilfe von ITCAM for SOA Version 7 einzufügen. Dies ermöglicht eine grundlegende Überwachung von Ereignissen und erweitert die Richtlinienunterstützung um Überwachungsrichtlinien. Überwachungsrichtlinien bieten die Möglichkeit, Ereignissituationen im Richtlinienerstellungspunkt (PAP) zu definieren und einer Servicedefinition zuzuordnen, sodass der Monitor Aktionen ausführen kann, wenn die Ereignissituation eintritt.

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-Verfahren (SOA, Service Oriented Architecture - serviceorientierte Architektur) unterstützen Unternehmen bei der Ermittlung und Konzentration auf die wichtigsten Services für das Geschäft. Durch Hinzufügen von Richtlinien werden Punkte zur Steuerung und zur Steigerung der Beweglichkeit der Geschäftsabläufe und der Informationstechnologie hinzugefügt. Im Ergebnis macht SOA die Umgebung verbraucherfreundlicher, verbessert die Wertschöpfungszeit für Geschäftsbenutzer durch geringere Kosten für Projekte und beschleunigt die Einführung neuer SOA-Lösungen.

„SOA Policy Gateway Basic Runtime" auf Seite 22
SOA Policy Gateway Basic Runtime bietet ein einfaches Verfahren zur Bereitstellung einer Laufzeit, die eigenständig oder in ein implementiertes SOA Policy Gateway Governance Master-Muster integriert verwendet werden kann. Das SOA Policy Gateway Basic Runtime-Muster unterstützt die Implementierung einer DataPower-Domäne, die für die Kommunikation mit dem WSRR-Laufzeitserver konfiguriert wird, der in diesem Muster bereitgestellt wird.

„SOA Policy Gateway Basic Runtime Sample" auf Seite 18
SOA Policy Gateway Basic Runtime Sample stellt eine SOA Policy Gateway Basic Runtime mit einer Beispielschnittstelle und einer Beispielanwendung bereit, die die gegenwärtig in diesem Release unterstützten Richtlinien demonstrieren.

„SOA Policy Gateway Governance Master" auf Seite 20
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" auf Seite 24
SOA Policy Gateway Advanced Runtime enthält weitere Hochverfügbarkeitsoptionen und muss zusammen mit SOA Policy Gateway Governance Master verwendet werden.

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 den Komponenten dieses Szenarios vertraut zu machen, die Gründe zu verstehen, aus denen es sich für ein Unternehmen anbietet, diesem Szenario zu folgen, die beteiligten Benutzerrollen kennen zu lernen und sich eine Übersicht über die durch das Produkt gelieferte Funktionalität zu verschaffen.

Vorbereitende Schritte

Sie können IBM IBM SOA Policy Gateway Pattern auf IBM PureApplication System oder auf dem IBM Workload Deployer-Gerät verwenden.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um IBM SOA Policy Gateway Pattern zu verwenden:

1. Laden Sie IBM SOA Policy Gateway Pattern herunter und installieren Sie das Produkt. Weitere Informationen zum Herunterladen der Pakete von Passport Advantage finden Sie in „Muster herunterladen und installieren" auf Seite 12.
2. Optional: Konfigurieren Sie den Benutzerzugriff. Weitere Informationen finden Sie in „Benutzerzugriff konfigurieren" auf Seite 15.
3. Konfigurieren und implementieren Sie das Muster.
   a. Akzeptieren Sie die importierten Lizenzen für das virtuelle Systemimage für WSRR.
   b. Akzeptieren Sie alle Lizenzvereinbarungen für DB2 Enterprise.
   c. Implementieren Sie das Muster wie folgt:
      1) Entscheiden Sie sich für eine Implementierungstopologie. Weitere Informationen finden Sie im Information Center von IBM WebSphere Service Registry and Repository Version 8.0 - Implementierungstopologien.
      2) Wenn Sie eine eigenständige Implementierungstopologie verwenden, implementieren Sie ein einzelnes Basic Runtime-Muster ohne konfigurierte Umstufung (Promotion).
      3) Für andere Topologien implementieren Sie zuerst das SOA Policy Gateway Governance Master-Muster. Dieses Muster stellt eine Governance-Umgebung für Services und Richtlinien bereit.
      4) Nach der erfolgreichen Implementierung des Governance Master-Musters wählen Sie den Typ der Laufzeitumgebung aus, den Sie benötigen. Als Testumgebung oder Bereitstellungsumgebung (Stagingumgebung) ist eine Basic Runtime-Umgebung in der Regel ausreichend. Als Produktionsumgebung wählen Sie die Advanced Runtime-Umgebung aus. Die Runtime-Umgebungen können mit der Umstufungskonfiguration des Governance-Realisierungsprofils für den Governance Master registriert werden. Umstufungsoptionen sind 'Production', 'Staging' (Bereitstellung) oder keine Umstufung für die manuelle Umstufungskonfiguration.

   Weitere Informationen finden Sie in „Muster implementieren" auf Seite 74.

d. Überprüfen Sie die Implementierung. Siehe „Implementierung überprüfen" auf Seite 80.
e. Schützen Sie die WSRR-Umgebung. Weitere Informationen zur Planung und Konfiguration der WSRR-Sicherheit finden Sie im Information Center von IBM WebSphere Service Registry and Repository Version 8.0.
f. Konfigurieren Sie die bereitgestellte DataPower-Domäne. Weitere Informationen finden Sie in „Sicherheitsmanagement" auf Seite 66.

4. Verwenden Sie die implementierte Instanz. Informationen dazu finden Sie in Kapitel 6, „Mit der implementierten Instanz arbeiten", auf Seite 107.

Muster herunterladen und installieren

IBM SOA Policy Gateway Pattern für die Verwendung mit IBM Workload Deployer Version 3.1.0.2 oder IBM PureApplication System wird in einem Paket zum Download von Passport Advantage zur Verfügung gestellt.

Vorbereitende Schritte

Stellen Sie sicher, dass 10 GB Speicherplatz für die Datei `CI9G9ML.tar.gz` und weitere 10 bis 14 GB für die extrahierten Dateien verfügbar sind.

Die Datei `CI9G9ML.tar.gz` muss auf ein System unter dem Betriebssystem Linux oder Microsoft Windows heruntergeladen werden. Java™ Runtime Environment (JRE) Version 6 muss ebenfalls installiert sein, bevor die Installation der Muster gestartet wird. Sie können diese Version 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 `CI9G9ML.tar.gz`. 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. Navigieren Sie zur Passport Advantage-Website: Passport Advantage.
2. Laden Sie die Archivdatei mit den Images, Scriptpaketen und Mustern herunter, die verwendet werden sollen. Die Datei hat den Namen `CI9G9ML.tar.gz`.
3. Öffnen Sie ein Terminal unter Linux bzw. ein Fenster mit Eingabeaufforderung unter Windows und navigieren Sie in das Verzeichnis, in das die Datei `CI9G9ML.tar.gz` heruntergeladen wurde.
4. Extrahieren Sie den Inhalt der Datei `CI9G9ML.tar.gz` in Ihr lokales Dateisystem. Unter Linux verwenden Sie den folgenden Extraktionsbefehl: Unter Linux verwenden Sie den folgenden Extraktionsbefehl:

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

   Unter Windows verwenden Sie zusätzliche Archivsoftware zum Extrahieren des Inhalts der Datei `CI9G9ML.tar.gz`.
5. Stellen Sie sicher, dass die folgenden extrahierten Dateien die Ausführungsberechtigung auf Linux-Systemen haben:

- `chmod a+x installer/installer`
- `chmod a+x installer/deployer.cli/bin/deployer`
- `chmod a+x installer/deployer.cli/bin/3.1.0.2-20120531075842/deployer`

6. Wechseln Sie in das Verzeichnis `installer`:

```
cd installer
```

7. Führen Sie das Installationsprogramm aus, um IBM SOA Policy Gateway Pattern im Cloudgerät 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 Cloudgerät und 'benutzername' und 'kennwort' sind die Berechtigungsnachweise des Cloudadministrators. Beispiel:

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

8. 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.
9. 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 2.0.0.0 - Governance Master" ...
Import pattern "SOA Policy Gateway 2.0.0.0 - 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, bereits im Katalog vorhanden ist, wird es nicht überschrieben.

Nächste Schritte

Akzeptieren Sie die Lizenzen im IBM Workload Deployer-Gerät oder in IBM PureApplication System.

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

Installiertes Muster überprüfen

Sie können überprüfen, ob das Muster erfolgreich installiert wurde, und erforderliche Lizenzen zur Verwendung des Musters akzeptieren.

Vorbereitende Schritte

Stellen Sie sicher, dass alle Schritte in „Muster herunterladen und installieren” auf Seite 12 ausgeführt wurden.

Informationen zu diesem Vorgang

Nach der Installation des Musters können Sie die Musterinstallation überprüfen. Bevor ein virtuelles Image verwendet werden kann, müssen Sie die für das Image erforderliche Lizenz akzeptieren.

Vorgehensweise

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

1. Melden Sie sich an der IPAS-Konsole bzw. der IWD-Konsole auf dem Host an, auf dem das Muster installiert wurde.
2. Überprüfen Sie die virtuellen Images, indem Sie zu `Catalog -> Virtual Images` navigieren und nach DB2 9.7.5.0 und WebSphere Service Registry and Repository 8.0.0.1 suchen. Wenn eine Lizenz nicht akzeptiert wurde, enthält das Imagesymbol ein rotes Feld mit einem Kreuz.
   a. Zum Akzeptieren einer Lizenz klicken Sie auf das Image, um die zugehörigen Details anzuzeigen. Der aktuelle 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. Wenn dies ausgeführt wurde, zeigt der aktuelle Status 'Read-only' (schreibgeschützt) an und die Lizenzvereinbarung wird als 'Accepted' angezeigt.
3. Navigieren Sie zu `Catalog -> Script Packages` und suchen Sie nach den folgenden Elementen:
   - SOA Policy Gateway 2.0.0.0 - DataPower Domain
   - SOA Policy Gateway 2.0.0.0 - Promotion
   - SOA Policy Gateway 2.0.0.0 - Sample
   - SOA Policy Gateway 2.0.0.0 - Security

   Diese Scriptpakete sind alle in einer erfolgreichen Installation vorhanden.
4. Navigieren Sie zu `Patterns -> Virtual Systems` und suchen Sie nach den folgenden Elementen:
   - SOA Policy Gateway 2.0.0.0 - Advanced Runtime
   - SOA Policy Gateway 2.0.0.0 - Basic Runtime
   - SOA Policy Gateway 2.0.0.0 - Basic Runtime Sample
   - SOA Policy Gateway 2.0.0.0 - Governance Master

   Diese Muster sind alle 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 folgenden Abschnitt fortfahren: Kapitel 5, „Mit IBM SOA Policy Gateway Pattern arbeiten”, auf Seite 63. Wenn die Installation nicht erfolgreich war, wiederholen Sie die in „Muster herunterladen und installieren” auf Seite 12 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.

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 Schnittstelle 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. Klicken Sie im Menü auf die Optionen **Catalog** > **Virtual images**, um das Fenster 'Virtual Images' zu öffnen. Wählen Sie ein virtuelles Image von IBM SOA Policy Gateway Pattern in der linken Anzeige aus und fügen Sie dann die Benutzer bzw. die Gruppe in der rechten Anzeige 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

IBM Workload Deployer: Benutzer und Gruppen verwalten

Kapitel 4. Muster, Teile und Scriptpakete

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

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.

Teile

Teile beschreiben die Komponenten, die auf einer virtuellen Maschine konfiguriert werden. Jeder Teil besitzt einen Satz von Eigenschaften (Parametern), die bei der Implementierung verwendet werden, um die Definition der Gesamtkonfiguration des virtuellen Systems zu vereinfachen. Wenn Sie die IBM SOA Policy Gateway Pattern-Images auf IBM Workload Deployer laden, werden die Teile einbezogen.

Muster

IBM SOA Policy Gateway Pattern enthält vier Muster:

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

Detaillierte Informationen zur Verwendung von IBM Workload Deployer für den Zugriff auf vorhandene Muster bzw. zur Erstellung angepasster Muster finden Sie in http://publib.boulder.ibm.com/infocenter/worlodep/v3r0m0/topic/com.ibm.worlodep.doc/welcome.html.

Muster

Wenn die virtuellen Images in IBM Workload Deployer oder IBM PureApplication System geladen wurden und der Zugriff den Benutzern ordnungsgemäß erteilt wurde, können Benutzer mit der Arbeit mit den Mustern der Images 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

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

- DB2 Enterprise
- Eigenständiger WSRR-Server

SOA Policy Gateway Basic Runtime Sample

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

- DB2 Enterprise
- Eigenständiger WSRR-Server

SOA Policy Gateway Advanced Runtime

Das SOA Policy Gateway Advanced Runtime-Muster enthält die folgenden erforderlichen Teile:

- WSRR-Deployment Manager
- DB2 Enterprise-HADR-Primärdatenbank
- DB2 Enterprise-HADR-Bereitschaftsdatenbank (Standby)
- Angepasster WSRR-Knoten

SOA Policy Gateway Governance Master

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

- WSRR-Deployment Manager
- DB2 Enterprise-HADR-Primärdatenbank
- DB2 Enterprise-HADR-Bereitschaftsdatenbank (Standby)
- Angepasster WSRR-Knoten

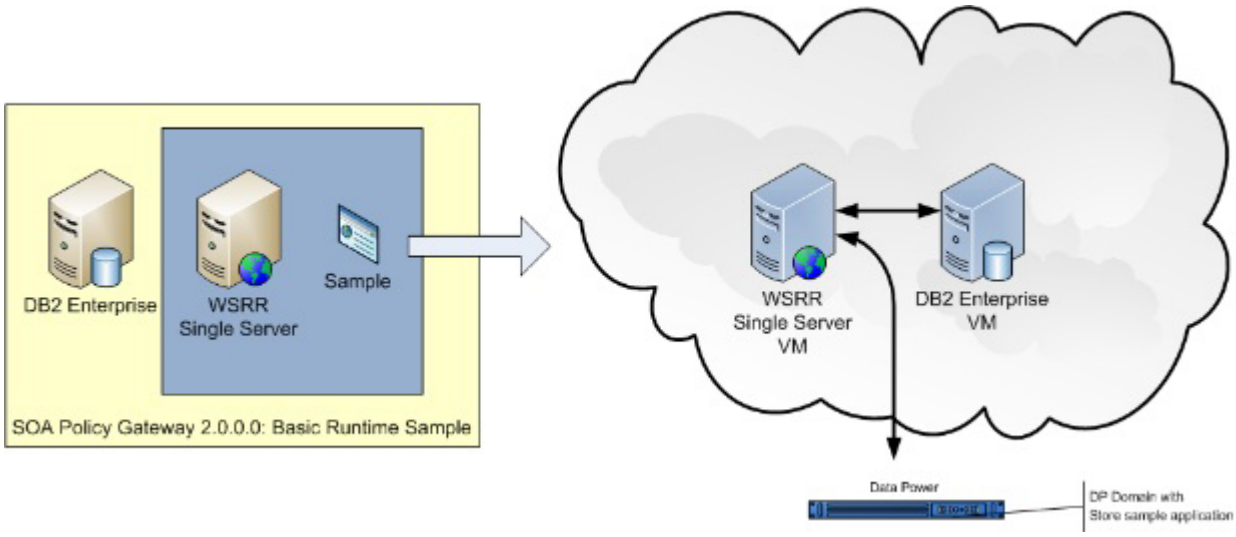
SOA Policy Gateway Basic Runtime Sample

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

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

- Eigenständiger WSRR-Server
- DB2 Enterprise

Das SOA Policy Gateway Basic Runtime Sample-Muster installiert eine Beispielanwendung in der implementierten Umgebung. Es installiert die Beispieldomäne in DataPower, die einen einfachen Service 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 83. 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.



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 SOA Policy Gateway Basic Runtime-Muster erfordert die folgenden Scripts.

Im Teil für den eigenständigen WSRR-Server:

- SOA Policy Gateway 2.0.0.0 - Sample

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

- „Konfigurationsparameter des DB2 Enterprise-Teils für das SOA Policy Gateway Basic Runtime Sample-Muster" auf Seite 30
- „Konfigurationsparameter des Teils für den eigenständigen WSRR-Server für das SOA Policy Gateway Basic Runtime Sample-Muster" auf Seite 42

- „SOA Policy Gateway 2.0.0.0 - Konfigurationsparameter des Sample-Scripts für das SOA Policy Gateway Basic Runtime Sample-Muster" auf Seite 55

Zugehörige Konzepte:

„DB2 Enterprise-Teil" auf Seite 27
Der DB2 Enterprise-Teil stellt einige Konfigurationsoptionen bereit.

„Teil für eigenständigen WSRR-Server" auf Seite 41
Der Teil für eigenständigen WSRR-Server stellt einige Konfigurationsoptionen bereit.

„Script: SOA Policy Gateway 2.0.0.0 - Sample" auf Seite 54
Das Beispielscript 'Sample' konfiguriert die Beispielanwendungsparameter für die Verwendung mit dem SOA Policy Gateway Basic Runtime Sample-Muster.

„Beispielanwendung" auf Seite 83
Die Beispielanwendung besteht aus einer konfigurierbaren DataPower-Domäne und einer Gruppe von WSRR-Artefakten, die zur Demonstration der Funktionen des Musters verwendet werden können.

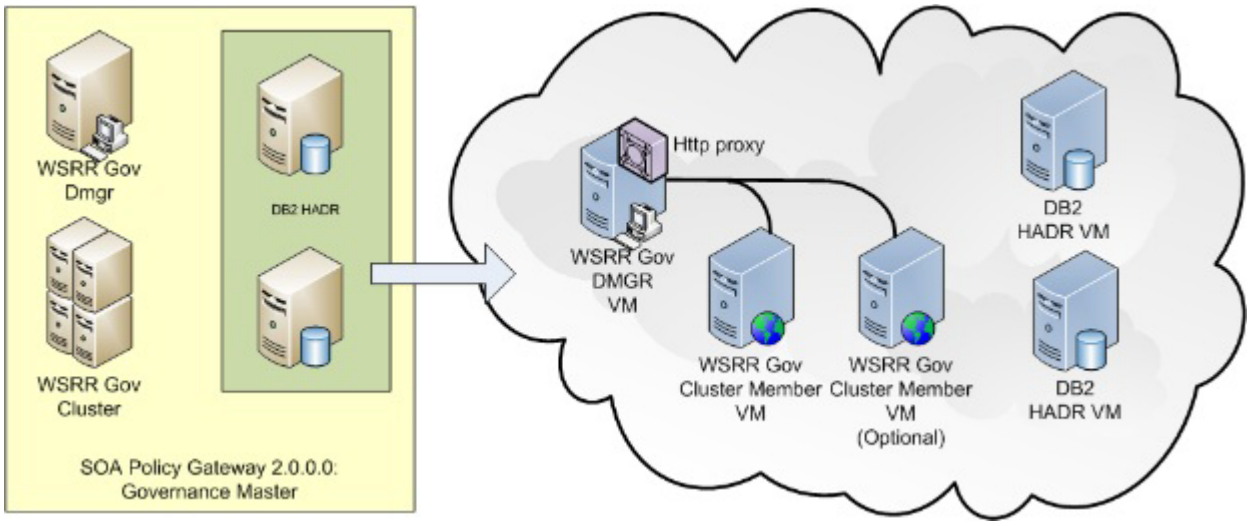
SOA Policy Gateway Governance Master

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. Nur das SOA Policy Gateway Basic Runtime-Muster oder das SOA Policy Gateway Advanced Runtime-Muster kann im Governance Master konfiguriert werden.



Scripts und erweiterte Optionen

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

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

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

- „Konfigurationsparameter des Teils für die DB2 Enterprise-HADR-Primärdatenbank für das SOA Policy Gateway Governance Master-Muster" auf Seite 35
- „Konfigurationsparameter des Teils für die DB2 Enterprise-HADR-Bereitschaftsdatenbank für das SOA Policy Gateway Governance Master-Muster" auf Seite 39
- „Konfigurationsparameter des WSRR-Deployment Manager-Teils für das SOA Policy Gateway Governance Master-Muster" auf Seite 45
- „Konfigurationsparameter des Teils für angepasste WSRR-Knoten für das SOA Policy Gateway Governance Master-Muster" auf Seite 48

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 SOA Policy Gateway Basic Runtime-Muster und das SOA Policy Gateway Advanced Runtime-Muster können in dieser Integration als Umstufungsziele (Promotionsziele) implementiert werden. Weitere Informationen dazu, wie dies konfiguriert wird, finden Sie in „Szenario: Zusätzliche Laufzeit dem Muster hinzufügen" auf Seite 81.

Zugehörige Konzepte:

„Teil für DB2 Enterprise-HADR-Primärdatenbank" auf Seite 32
Der Teil für die DB2 Enterprise-HADR-Primärdatenbank stellt einige Konfigurationsoptionen bereit.

„Teil für DB2 Enterprise-HADR-Bereitschaftsdatenbank" auf Seite 37
Der Teil für die DB2 Enterprise-HADR-Bereitschaftsdatenbank stellt einige Konfigurationsoptionen bereit.

„WSRR-Deployment Manager-Teil" auf Seite 43
Der WSRR-Deployment Manager-Teil stellt einige Konfigurationsoptionen bereit.

„Teil für angepasste WSRR-Knoten" auf Seite 46
Der Teil für angepasste WSRR-Knoten stellt einige Konfigurationsoptionen bereit.

Zugehörige Informationen:

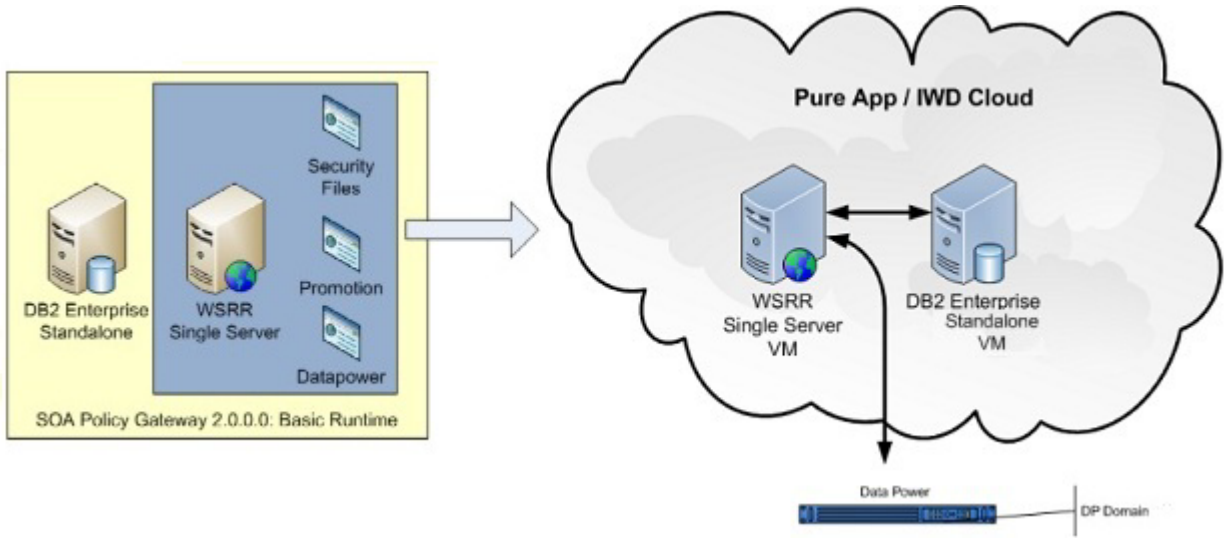
Information Center von IBM WebSphere Service Registry and Repository Version 8.0 - Governance-Realisierungsprofil

SOA Policy Gateway Basic Runtime

SOA Policy Gateway Basic Runtime bietet ein einfaches Verfahren zur Bereitstellung einer Laufzeit, die eigenständig oder in ein implementiertes SOA Policy Gateway Governance Master-Muster integriert verwendet werden kann. Das SOA Policy Gateway Basic Runtime-Muster unterstützt die Implementierung einer DataPower-Domäne, die für die Kommunikation mit dem WSRR-Laufzeitserver konfiguriert wird, der in diesem Muster bereitgestellt wird.

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

- Eigenständiger WSRR-Server
- DB2 Enterprise



Scripts und erweiterte Optionen

Das SOA Policy Gateway Basic Runtime-Muster erfordert die folgenden Scripts.

Im Teil für den eigenständigen WSRR-Server:

- SOA Policy Gateway 2.0.0.0 - Security
- SOA Policy Gateway 2.0.0.0 - Promotion

- SOA Policy Gateway 2.0.0.0 - DataPower Domain

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

- „Konfigurationsparameter des Teils für den eigenständigen WSRR-Server für das SOA Policy Gateway Basic Runtime-Muster" auf Seite 42
- „Konfigurationsparameter des DB2 Enterprise-Teils für das SOA Policy Gateway Basic Runtime-Muster" auf Seite 28
- „SOA Policy Gateway 2.0.0.0 - Konfigurationsparameter des Security-Scripts für das SOA Policy Gateway Basic Runtime-Muster" auf Seite 59
- „SOA Policy Gateway 2.0.0.0 - Konfigurationsparameter des Promotion-Scripts für das SOA Policy Gateway Basic Runtime-Muster" auf Seite 52
- „SOA Policy Gateway 2.0.0.0 - Konfigurationsparameter des DataPower Domain-Scripts für das SOA Policy Gateway Basic Runtime-Muster" auf Seite 50

SOA Policy Gateway Basic Runtime in eine Governance-Laufzeit umstufen (Promotion)

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')
- Sonstig oder nicht festgelegt ('other' oder 'Unset')

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.

Zugehörige Konzepte:

„Beispielanwendung" auf Seite 83
Die Beispielanwendung besteht aus einer konfigurierbaren DataPower-Domäne und einer Gruppe von WSRR-Artefakten, die zur Demonstration der Funktionen des Musters verwendet werden können.

„DB2 Enterprise-Teil" auf Seite 27
Der DB2 Enterprise-Teil stellt einige Konfigurationsoptionen bereit.

„Teil für eigenständigen WSRR-Server" auf Seite 41
Der Teil für eigenständigen WSRR-Server stellt einige Konfigurationsoptionen bereit.

„Script: SOA Policy Gateway 2.0.0.0 - Security" auf Seite 58
Das Sicherheitsscript 'Security' kopiert Sicherheitsinformationen, die in einer ZIP-Datei enthalten und die für die Kommunikation mit einem DataPower-Gerät erforderlich sind, auf das Deployment Manager-System ('Dmgr') oder das WSRR-System. Die Daten werden von einem externen Dateiserver kopiert, der Linux Secure Copy Protocol (SCP) unterstützt.

„Script: SOA Policy Gateway 2.0.0.0 - Promotion" auf Seite 52
Durch das Umstufungsscript 'Promotion' kann ein SOA Policy Gateway Basic Runtime- oder SOA Policy Gateway 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.

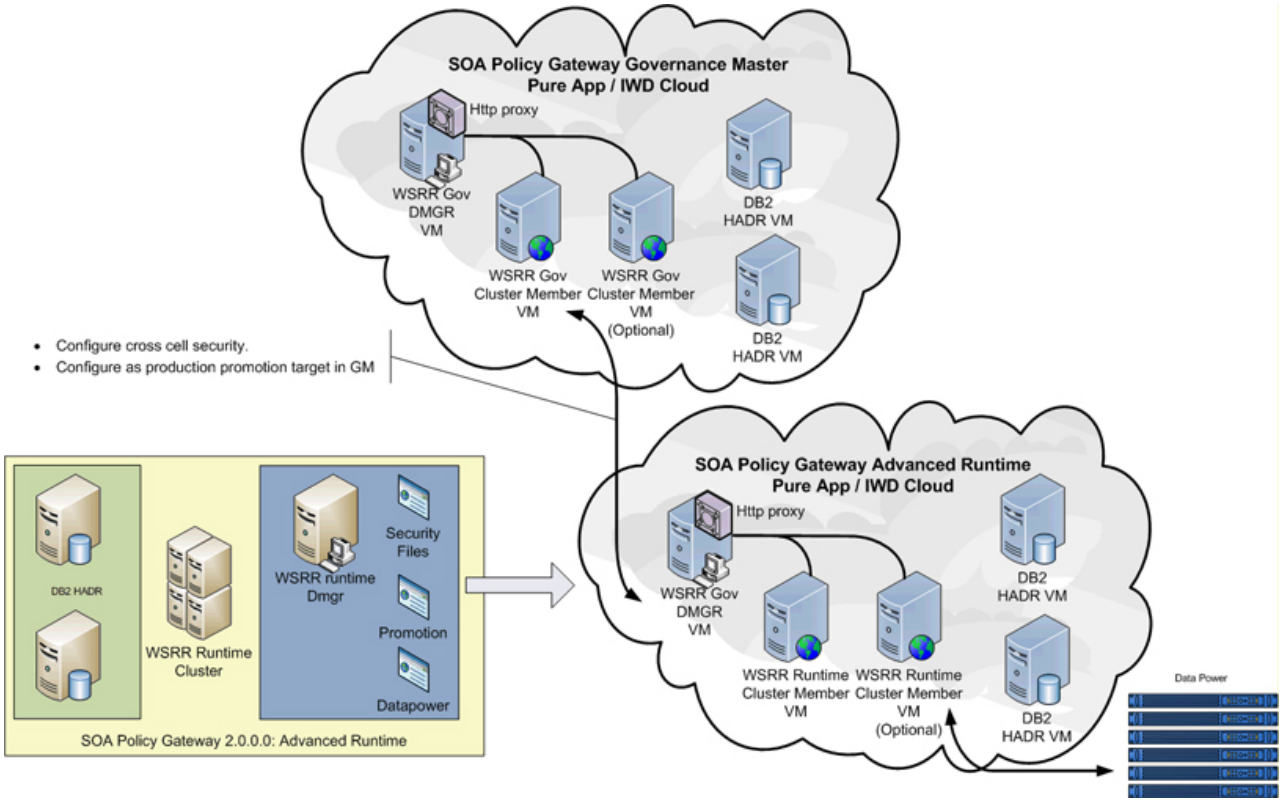
„Script: SOA Policy Gateway 2.0.0.0 - DataPower Domain" auf Seite 49
Das DataPower Domain-Script stellt die DataPower-Domäne während der Implementierung bereit. Das Script konfiguriert die Verbindung zwischen einer einzelnen DataPower-Domäne und der WSRR-Laufzeit. Für jede DataPower-Domäne, die mit der WSRR-Laufzeit verbunden wird, ist ein separates DataPower Domain-Script erforderlich.

SOA Policy Gateway Advanced Runtime

SOA Policy Gateway Advanced Runtime enthält weitere Hochverfügbarkeitsoptionen und muss zusammen mit SOA Policy Gateway Governance Master verwendet werden.

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

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



Scripts und erweiterte Optionen

Das SOA Policy Gateway Governance Master-Muster erfordert die folgenden Scripts im WSRR-Deployment Manager-Teil:

- SOA Policy Gateway 2.0.0.0 - Security
- SOA Policy Gateway 2.0.0.0 - Promotion
- SOA Policy Gateway 2.0.0.0 - DataPower Domain (ein Script pro DataPower-Domäne)

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

- „Konfigurationsparameter des Teils für die DB2 Enterprise-HADR-Primärdatenbank für das SOA Policy Gateway Advanced Runtime-Muster" auf Seite 33
- „Konfigurationsparameter des Teils für die DB2 Enterprise-HADR-Bereitschaftsdatenbank für das SOA Policy Gateway Advanced Runtime-Muster" auf Seite 38
- „Konfigurationsparameter des WSRR-Deployment Manager-Teils für das SOA Policy Gateway Advanced Runtime-Muster" auf Seite 44
- „Konfigurationsparameter des Teils für angepasste WSRR-Knoten für das SOA Policy Gateway Advanced Runtime-Muster" auf Seite 47
- „SOA Policy Gateway 2.0.0.0 - Konfigurationsparameter des Security-Scripts für das SOA Policy Gateway Advanced Runtime-Muster" auf Seite 60
- „SOA Policy Gateway 2.0.0.0 - Konfigurationsparameter des Promotion-Scripts für das SOA Policy Gateway Advanced Runtime-Muster" auf Seite 53

- „SOA Policy Gateway 2.0.0.0 - Konfigurationsparameter des DataPower Domain-Scripts für das SOA Policy Gateway Advanced Runtime-Muster" auf Seite 51

SOA Policy Gateway Advanced Runtime in eine Governance-Laufzeit umstufen (Promotion)

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')
- Sonstig oder nicht festgelegt ('other' oder „Unset")

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

Zugehörige Konzepte:

„Teil für DB2 Enterprise-HADR-Primärdatenbank" auf Seite 32
Der Teil für die DB2 Enterprise-HADR-Primärdatenbank stellt einige Konfigurationsoptionen bereit.

„Teil für DB2 Enterprise-HADR-Bereitschaftsdatenbank" auf Seite 37
Der Teil für die DB2 Enterprise-HADR-Bereitschaftsdatenbank stellt einige Konfigurationsoptionen bereit.

„WSRR-Deployment Manager-Teil" auf Seite 43
Der WSRR-Deployment Manager-Teil stellt einige Konfigurationsoptionen bereit.

„Teil für angepasste WSRR-Knoten" auf Seite 46
Der Teil für angepasste WSRR-Knoten stellt einige Konfigurationsoptionen bereit.

„Script: SOA Policy Gateway 2.0.0.0 - Security" auf Seite 58
Das Sicherheitsscript 'Security' kopiert Sicherheitsinformationen, die in einer ZIP-Datei enthalten und die für die Kommunikation mit einem DataPower-Gerät erforderlich sind, auf das Deployment Manager-System ('Dmgr') oder das WSRR-System. Die Daten werden von einem externen Dateiserver kopiert, der Linux Secure Copy Protocol (SCP) unterstützt.

„Script: SOA Policy Gateway 2.0.0.0 - Promotion" auf Seite 52
Durch das Umstufungsscript 'Promotion' kann ein SOA Policy Gateway Basic Runtime- oder SOA Policy Gateway 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.

„Script: SOA Policy Gateway 2.0.0.0 - DataPower Domain" auf Seite 49
Das DataPower Domain-Script stellt die DataPower-Domäne während der Implementierung bereit. Das Script konfiguriert die Verbindung zwischen einer einzelnen DataPower-Domäne und der WSRR-Laufzeit. Für jede DataPower-Domäne, die mit der WSRR-Laufzeit verbunden wird, ist ein separates DataPower Domain-Script erforderlich.

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 9.7.5 werden in der folgenden Tabelle beschrieben:

Tabelle 2. Konfigurierbare Parameter

Parametername	Beschreibung
Virtuelle CPUs (Virtual CPUs)	Die Anzahl der virtuellen Prozessoren, die für die durch diesen Teil dargestellte virtuelle Maschine zugeordnet werden.
Speicherkapazität (Memory size, MB)	Die Speicherkapazität in MB, die dieser virtuellen Maschine zugeordnet wird.
Kennwort (Password) - db2inst1	Das Kennwort für die Benutzer-ID 'db2inst1' des Betriebssystems. Diese Benutzer-ID wird als Installationseigner der DB2-Instanz und als Eigner der Datenbankschemas verwendet.
Kennwort überprüfen (Verify password)	Überprüft das Kennwort für 'db2inst1'.

Tabelle 2. Konfigurierbare Parameter (Forts.)

Parametername	Beschreibung
Kennwort (Password) - db2fenc1	Das Kennwort für die Benutzer-ID, die zur Ausführung benutzerdefinierter Funktionen (UDFs) und gespeicherter Prozeduren außerhalb des von der DB2-Datenbank verwendeten Adressraums verwendet wird. Ein abgeschirmter ('fenced') Benutzer ist ein Benutzer, unter dem einige gespeicherte Prozeduren ("abgeschirmte" gespeicherte Prozeduren) mit eingeschränkten Betriebssystemberechtigungen ausgeführt werden können. Auf diese Weise lässt sich ein Überschreiben von Instanzdateien durch gespeicherte Prozeduren besser vermeiden, da das Betriebssystem dies verhindert.
Kennwort überprüfen (Verify password)	Überprüft das Kennwort für 'db2fenc1'.
Kennwort (Password) - dasusr1	Die Benutzer-ID, die für den DB2-Verwaltungsserver verwendet wird, der zur Ausführung des DB2-Verwaltungsservers auf Ihrem System verwendet wird. Die Standardbenutzer-ID ist 'dasusr1', die Standardgruppe 'dasadm1'. Diese Benutzer-ID wird außerdem von den DB2-GUI-Tools zur Ausführung von Verwaltungstasks für die lokalen Datenbankinstanzen und Datenbanken des Servers verwendet.
Kennwort überprüfen (Verify password)	Überprüft das Kennwort für 'dasusr1'.
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'.

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

Konfigurationsparameter des DB2 Enterprise-Teils für das SOA Policy Gateway Basic Runtime-Muster

Erforderliche Parameter ohne Standardwert müssen konfiguriert werden, bevor das Muster implementiert werden kann.

Tabelle 3. Konfigurierbare Parameter

Parametername	Erforderlich	Standardwert	Beschreibung
Virtuelle CPUs (Virtual CPUs)	Ja	1	Die Anzahl der virtuellen Prozessoren, die für die durch diesen Teil dargestellte virtuelle Maschine zugeordnet werden.
Speicherkapazität (Memory size, MB)	Ja	2048	Die Speicherkapazität in MB, die dieser virtuellen Maschine zugeordnet wird.
Kennwort (Password) - db2inst1	Ja		Das Kennwort für die Benutzer-ID 'db2inst1' des Betriebssystems. Diese Benutzer-ID wird als Installationseigner der DB2-Instanz und als Eigner der Datenbankschemas verwendet.

Tabelle 3. Konfigurierbare Parameter (Forts.)

Parametername	Erforderlich	Standardwert	Beschreibung
Kennwort überprüfen (Verify password)	Ja		Überprüft das Kennwort für 'db2inst1'.
Kennwort (Password) - db2fenc1	Ja		Das Kennwort für die Benutzer-ID, die zur Ausführung benutzerdefinierter Funktionen (UDFs) und gespeicherter Prozeduren außerhalb des von der DB2-Datenbank verwendeten Adressraums verwendet wird. Ein abgeschirmter ('fenced') Benutzer ist ein Benutzer, unter dem einige gespeicherte Prozeduren ("abgeschirmte" gespeicherte Prozeduren) mit eingeschränkten Betriebssystemberechtigungen ausgeführt werden können. Auf diese Weise lässt sich ein Überschreiben von Instanzdateien durch gespeicherte Prozeduren besser vermeiden, da das Betriebssystem dies verhindert.
Kennwort überprüfen (Verify password)	Ja		Überprüft das Kennwort für 'db2fenc1'.
Kennwort (Password) - dasusr1	Ja		Die Benutzer-ID, die für den DB2-Verwaltungsserver verwendet wird, der zur Ausführung des DB2-Verwaltungsservers auf Ihrem System verwendet wird. Die Standardbenutzer-ID ist 'dasusr1', die Standardgruppe 'dasadm1'. Diese Benutzer-ID wird außerdem von den DB2-GUI-Tools zur Ausführung von Verwaltungstasks für die lokalen Datenbankinstanzen und Datenbanken des Servers verwendet.
Kennwort überprüfen (Verify password)	Ja		Überprüft das Kennwort für 'dasusr1'.
Kennwort (Password) - Root	Ja		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)	Ja		Überprüft das Kennwort für 'root'.

Tabelle 3. Konfigurierbare Parameter (Forts.)

Parametername	Erforderlich	Standardwert	Beschreibung
Kennwort (Password) - virtuser	Ja		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)	Ja		Überprüft das Kennwort für 'virtuser'.

Konfigurationsparameter des DB2 Enterprise-Teils für das SOA Policy Gateway Basic Runtime Sample-Muster

In SOA Policy Gateway Basic Runtime Sample sind für alle Parameter Standardwerte vorkonfiguriert.

Tabelle 4. Konfigurierte Parameter

Parametername	Erforderlich	Standardwert	Beschreibung
Virtuelle CPUs (Virtual CPUs)	Ja	1	Die Anzahl der virtuellen Prozessoren, die für die durch diesen Teil dargestellte virtuelle Maschine zugeordnet werden.
Speicherkapazität (Memory size, MB)	Ja	2048	Die Speicherkapazität in MB, die dieser virtuellen Maschine zugeordnet wird.
Kennwort (Password) - db2inst1	Ja	password	Das Kennwort für die Benutzer-ID 'db2inst1' des Betriebssystems. Diese Benutzer-ID wird als Installationseigner der DB2-Instanz und als Eigner der Datenbankschemas verwendet.
Kennwort überprüfen (Verify password)	Ja	password	Überprüft das Kennwort für 'db2inst1'.

Tabelle 4. Konfigurierte Parameter (Forts.)

Parametername	Erforderlich	Standardwert	Beschreibung
Kennwort (Password) - db2fenc1	Ja	password	Das Kennwort für die Benutzer-ID, die zur Ausführung benutzerdefinierter Funktionen (UDFs) und gespeicherter Prozeduren außerhalb des von der DB2-Datenbank verwendeten Adressraums verwendet wird. Ein abgeschirmter ('fenced') Benutzer ist ein Benutzer, unter dem einige gespeicherte Prozeduren ("abgeschirmte" gespeicherte Prozeduren) mit eingeschränkten Betriebssystemberechtigungen ausgeführt werden können. Auf diese Weise lässt sich ein Überschreiben von Instanzdateien durch gespeicherte Prozeduren besser vermeiden, da das Betriebssystem dies verhindert.
Kennwort überprüfen (Verify password)	Ja	password	Überprüft das Kennwort für 'db2fenc1'.
Kennwort (Password) - dasusr1	Ja	password	Die Benutzer-ID, die für den DB2-Verwaltungsserver verwendet wird, der zur Ausführung des DB2-Verwaltungsservers auf Ihrem System verwendet wird. Die Standardbenutzer-ID ist 'dasusr1', die Standardgruppe 'dasadm1'. Diese Benutzer-ID wird außerdem von den DB2-GUI-Tools zur Ausführung von Verwaltungstasks für die lokalen Datenbankinstanzen und Datenbanken des Servers verwendet.
Kennwort überprüfen (Verify password)	Ja	password	Überprüft das Kennwort für 'dasusr1'.
Kennwort (Password) - Root	Ja	password	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)	Ja	password	Überprüft das Kennwort für 'root'.

Tabelle 4. Konfigurierte Parameter (Forts.)

Parametername	Erforderlich	Standardwert	Beschreibung
Kennwort (Password) - virtuser	Ja	password	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)	Ja	password	Überprüft das Kennwort für 'virtuser'.

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 5. Konfigurierbare Parameter

Parametername	Beschreibung
Virtuelle CPUs (Virtual CPUs)	Die Anzahl der virtuellen Prozessoren, die für die durch diesen Teil dargestellte virtuelle Maschine zugeordnet werden.
Speicherkapazität (Memory size, MB)	Die Speicherkapazität in MB, die dieser virtuellen Maschine zugeordnet wird.
Kennwort (Password) - db2inst1	Das Kennwort für die Benutzer-ID 'db2inst1' des Betriebssystems. Diese Benutzer-ID wird als Installationseigner der DB2-Instanz und als Eigner der Datenbankschemas verwendet.
Kennwort überprüfen (Verify password)	Überprüft das Kennwort für 'db2inst1'.
Kennwort (Password) - db2fenc1	Das Kennwort für die Benutzer-ID, die zur Ausführung benutzerdefinierter Funktionen (UDFs) und gespeicherter Prozeduren außerhalb des von der DB2-Datenbank verwendeten Adressraums verwendet wird. Ein abgeschirmter ('fenced') Benutzer ist ein Benutzer, unter dem einige gespeicherte Prozeduren ("abgeschirmte" gespeicherte Prozeduren) mit eingeschränkten Betriebssystemberechtigungen ausgeführt werden können. Auf diese Weise lässt sich ein Überschreiben von Instanzdateien durch gespeicherte Prozeduren besser vermeiden, da das Betriebssystem dies verhindert.
Kennwort überprüfen (Verify password)	Überprüft das Kennwort für 'db2fenc1'.
Kennwort (Password) - dasusr1	Das Kennwort für die Benutzer-ID für den DB2-Verwaltungsserver, der zur Ausführung des DB2-Verwaltungsservers auf Ihrem System verwendet wird. Die Standardbenutzer-ID ist 'dasusr1', die Standardgruppe 'dasadm1'. Diese Benutzer-ID wird außerdem von den DB2-GUI-Tools zur Ausführung von Verwaltungstasks für die lokalen Datenbankinstanzen und Datenbanken des Servers verwendet.
Kennwort überprüfen (Verify password)	Überprüft das Kennwort für 'dasusr1'.
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'.

Tabelle 5. Konfigurierbare Parameter (Forts.)

Parametername	Beschreibung
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'.

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

Konfigurationsparameter des Teils für die DB2 Enterprise-HADR-Primärdatenbank für das SOA Policy Gateway Advanced Runtime-Muster

Erforderliche Parameter ohne Standardwert müssen konfiguriert werden, bevor das Muster implementiert werden kann.

Tabelle 6. Konfigurierbare Parameter

Parametername	Erforderlich	Standardwert	Beschreibung
Virtuelle CPUs (Virtual CPUs)	Ja	1	Die Anzahl der virtuellen Prozessoren, die für die durch diesen Teil dargestellte virtuelle Maschine zugeordnet werden.
Speicherkapazität (Memory size, MB)	Ja	2048	Die Speicherkapazität in MB, die dieser virtuellen Maschine zugeordnet wird.
Kennwort (Password) - db2inst1	Ja		Das Kennwort für die Benutzer-ID 'db2inst1' des Betriebssystems. Diese Benutzer-ID wird als Installationseigner der DB2-Instanz und als Eigner der Datenbankschemas verwendet.
Kennwort überprüfen (Verify password)	Ja		Überprüft das Kennwort für 'db2inst1'.

Tabelle 6. Konfigurierbare Parameter (Forts.)

Parametername	Erforderlich	Standardwert	Beschreibung
Kennwort (Password) - db2fenc1	Ja		Das Kennwort für die Benutzer-ID, die zur Ausführung benutzerdefinierter Funktionen (UDFs) und gespeicherter Prozeduren außerhalb des von der DB2-Datenbank verwendeten Adressraums verwendet wird. Ein abgeschirmter ('fenced') Benutzer ist ein Benutzer, unter dem einige gespeicherte Prozeduren ("abgeschirmte" gespeicherte Prozeduren) mit eingeschränkten Betriebssystemberechtigungen ausgeführt werden können. Auf diese Weise lässt sich ein Überschreiben von Instanzdateien durch gespeicherte Prozeduren besser vermeiden, da das Betriebssystem dies verhindert.
Kennwort überprüfen (Verify password)	Ja		Überprüft das Kennwort für 'db2fenc1'.
Kennwort (Password) - dasusr1	Ja		Das Kennwort für die Benutzer-ID für den DB2-Verwaltungsserver, der zur Ausführung des DB2-Verwaltungsservers auf Ihrem System verwendet wird. Die Standardbenutzer-ID ist 'dasusr1', die Standardgruppe 'dasadm1'. Diese Benutzer-ID wird außerdem von den DB2-GUI-Tools zur Ausführung von Verwaltungstasks für die lokalen Datenbankinstanzen und Datenbanken des Servers verwendet.
Kennwort überprüfen (Verify password)	Ja		Überprüft das Kennwort für 'dasusr1'.
Kennwort (Password) - Root	Ja		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)	Ja		Überprüft das Kennwort für 'root'.

Tabelle 6. Konfigurierbare Parameter (Forts.)

Parametername	Erforderlich	Standardwert	Beschreibung
Kennwort (Password) - virtuser	Ja		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)	Ja		Überprüft das Kennwort für 'virtuser'.

Konfigurationsparameter des Teils für die DB2 Enterprise-HADR-Primärdatenbank für das SOA Policy Gateway Governance Master-Muster

Erforderliche Parameter ohne Standardwert müssen konfiguriert werden, bevor das Muster implementiert werden kann.

Tabelle 7. Konfigurierbare Parameter

Parametername	Erforderlich	Standardwert	Beschreibung
Virtuelle CPUs (Virtual CPUs)	Ja	1	Die Anzahl der virtuellen Prozessoren, die für die durch diesen Teil dargestellte virtuelle Maschine zugeordnet werden.
Speicherkapazität (Memory size, MB)	Ja	2048	Die Speicherkapazität in MB, die dieser virtuellen Maschine zugeordnet wird.
Kennwort (Password) - db2inst1	Ja		Das Kennwort für die Benutzer-ID 'db2inst1' des Betriebssystems. Diese Benutzer-ID wird als Installationseigner der DB2-Instanz und als Eigner der Datenbankschemas verwendet.
Kennwort überprüfen (Verify password)	Ja		Überprüft das Kennwort für 'db2inst1'.

Tabelle 7. Konfigurierbare Parameter (Forts.)

Parametername	Erforderlich	Standardwert	Beschreibung
Kennwort (Password) - db2fenc1	Ja		Das Kennwort für die Benutzer-ID, die zur Ausführung benutzerdefinierter Funktionen (UDFs) und gespeicherter Prozeduren außerhalb des von der DB2-Datenbank verwendeten Adressraums verwendet wird. Ein abgeschirmter ('fenced') Benutzer ist ein Benutzer, unter dem einige gespeicherte Prozeduren ("abgeschirmte" gespeicherte Prozeduren) mit eingeschränkten Betriebssystemberechtigungen ausgeführt werden können. Auf diese Weise lässt sich ein Überschreiben von Instanzdateien durch gespeicherte Prozeduren besser vermeiden, da das Betriebssystem dies verhindert.
Kennwort überprüfen (Verify password)	Ja		Überprüft das Kennwort für 'db2fenc1'.
Kennwort (Password) - dasusr1	Ja		Das Kennwort für die Benutzer-ID für den DB2-Verwaltungsserver, der zur Ausführung des DB2-Verwaltungsservers auf Ihrem System verwendet wird. Die Standardbenutzer-ID ist 'dasusr1', die Standardgruppe 'dasadm1'. Diese Benutzer-ID wird außerdem von den DB2-GUI-Tools zur Ausführung von Verwaltungstasks für die lokalen Datenbankinstanzen und Datenbanken des Servers verwendet.
Kennwort überprüfen (Verify password)	Ja		Überprüft das Kennwort für 'dasusr1'.
Kennwort (Password) - Root	Ja		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)	Ja		Überprüft das Kennwort für 'root'.

Tabelle 7. Konfigurierbare Parameter (Forts.)

Parametername	Erforderlich	Standardwert	Beschreibung
Kennwort (Password) - virtuser	Ja		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)	Ja		Überprüft das Kennwort für 'virtuser'.

Teil für DB2 Enterprise-HADR-Bereitschaftsdatenbank

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

Tabelle 8. Konfigurierbare Parameter

Parametername	Beschreibung
Virtuelle CPUs (Virtual CPUs)	Die Anzahl der virtuellen Prozessoren, die für die durch diesen Teil dargestellte virtuelle Maschine zugeordnet werden.
Speicherkapazität (Memory size, MB)	Die Speicherkapazität in MB, die dieser virtuellen Maschine zugeordnet wird.
Kennwort (Password) - db2inst1	Das Kennwort für die Benutzer-ID 'db2inst1' des Betriebssystems. Diese Benutzer-ID wird als Installationseigner der DB2-Instanz und als Eigner der Datenbankschemas verwendet.
Kennwort überprüfen (Verify password)	Überprüft das Kennwort für 'db2inst1'.
Kennwort (Password) - db2fenc1	Das Kennwort für die Benutzer-ID, die zur Ausführung benutzerdefinierter Funktionen (UDFs) und gespeicherter Prozeduren außerhalb des von der DB2-Datenbank verwendeten Adressraums verwendet wird. Ein abgeschirmter ('fenced') Benutzer ist ein Benutzer, unter dem einige gespeicherte Prozeduren ("abgeschirmte" gespeicherte Prozeduren) mit eingeschränkten Betriebssystemberechtigungen ausgeführt werden können. Auf diese Weise lässt sich ein Überschreiben von Instanzdateien durch gespeicherte Prozeduren besser vermeiden, da das Betriebssystem dies verhindert.
Kennwort überprüfen (Verify password)	Überprüft das Kennwort für 'db2fenc1'.
Kennwort (Password) - dasusr1	Das Kennwort für die Benutzer-ID für den DB2-Verwaltungsserver, der zur Ausführung des DB2-Verwaltungsservers auf Ihrem System verwendet wird. Die Standardbenutzer-ID ist 'dasusr1', die Standardgruppe 'dasadm1'. Diese Benutzer-ID wird außerdem von den DB2-GUI-Tools zur Ausführung von Verwaltungstasks für die lokalen Datenbankinstanzen und Datenbanken des Servers verwendet.
Kennwort überprüfen (Verify password)	Überprüft das Kennwort für 'dasusr1'.
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'.

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

Konfigurationsparameter des Teils für die DB2 Enterprise-HADR-Bereitschaftsdatenbank für das SOA Policy Gateway Advanced Runtime-Muster

Erforderliche Parameter ohne Standardwert müssen konfiguriert werden, bevor das Muster implementiert werden kann.

Tabelle 9. Konfigurierbare Parameter

Parametername	Erforderlich	Standardwert	Beschreibung
Virtuelle CPUs (Virtual CPUs)	Ja	1	Die Anzahl der virtuellen Prozessoren, die für die durch diesen Teil dargestellte virtuelle Maschine zugeordnet werden.
Speicherkapazität (Memory size, MB)	Ja	2048	Die Speicherkapazität in MB, die dieser virtuellen Maschine zugeordnet wird.
Kennwort (Password) - db2inst1	Ja		Das Kennwort für die Benutzer-ID 'db2inst1' des Betriebssystems. Diese Benutzer-ID wird als Installationseigner der DB2-Instanz und als Eigner der Datenbankschemas verwendet.
Kennwort überprüfen (Verify password)	Ja		Überprüft das Kennwort für 'db2inst1'.
Kennwort (Password) - db2fenc1	Ja		Das Kennwort für die Benutzer-ID, die zur Ausführung benutzerdefinierter Funktionen (UDFs) und gespeicherter Prozeduren außerhalb des von der DB2-Datenbank verwendeten Adressraums verwendet wird. Ein abgeschirmter ('fenced') Benutzer ist ein Benutzer, unter dem einige gespeicherte Prozeduren ("abgeschirmte" gespeicherte Prozeduren) mit eingeschränkten Betriebssystemberechtigungen ausgeführt werden können. Auf diese Weise lässt sich ein Überschreiben von Instanzdateien durch gespeicherte Prozeduren besser vermeiden, da das Betriebssystem dies verhindert.
Kennwort überprüfen (Verify password)	Ja		Überprüft das Kennwort für 'db2fenc1'.

Tabelle 9. Konfigurierbare Parameter (Forts.)

Parametername	Erforderlich	Standardwert	Beschreibung
Kennwort (Password) - dasusr1	Ja		Das Kennwort für die Benutzer-ID für den DB2-Verwaltungsserver, der zur Ausführung des DB2-Verwaltungsservers auf Ihrem System verwendet wird. Die Standardbenutzer-ID ist 'dasusr1', die Standardgruppe 'dasadm1'. Diese Benutzer-ID wird außerdem von den DB2-GUI-Tools zur Ausführung von Verwaltungstasks für die lokalen Datenbankinstanzen und Datenbanken des Servers verwendet.
Kennwort überprüfen (Verify password)	Ja		Überprüft das Kennwort für 'dasusr1'.
Kennwort (Password) - Root	Ja		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)	Ja		Überprüft das Kennwort für 'root'.
Kennwort (Password) - virtuser	Ja		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)	Ja		Überprüft das Kennwort für 'virtuser'.

Konfigurationsparameter des Teils für die DB2 Enterprise-HADR-Bereitschaftsdatenbank für das SOA Policy Gateway Governance Master-Muster

Erforderliche Parameter ohne Standardwert müssen konfiguriert werden, bevor das Muster implementiert werden kann.

Tabelle 10. Konfigurierbare Parameter

Parametername	Erforderlich	Standardwert	Beschreibung
Virtuelle CPUs (Virtual CPUs)	Ja	1	Die Anzahl der virtuellen Prozessoren, die für die durch diesen Teil dargestellte virtuelle Maschine zugeordnet werden.
Speicherkapazität (Memory size, MB)	Ja	2048	Die Speicherkapazität in MB, die dieser virtuellen Maschine zugeordnet wird.

Tabelle 10. Konfigurierbare Parameter (Forts.)

Parametername	Erforderlich	Standardwert	Beschreibung
Kennwort (Password) - db2inst1	Ja		Das Kennwort für die Benutzer-ID 'db2inst1' des Betriebssystems. Diese Benutzer-ID wird als Installationseigner der DB2-Instanz und als Eigner der Datenbankschemas verwendet.
Kennwort überprüfen (Verify password)	Ja		Überprüft das Kennwort für 'db2inst1'.
Kennwort (Password) - db2fenc1	Ja		Das Kennwort für die Benutzer-ID, die zur Ausführung benutzerdefinierter Funktionen (UDFs) und gespeicherter Prozeduren außerhalb des von der DB2-Datenbank verwendeten Adressraums verwendet wird. Ein abgeschirmter ('fenced') Benutzer ist ein Benutzer, unter dem einige gespeicherte Prozeduren ("abgeschirmte" gespeicherte Prozeduren) mit eingeschränkten Betriebssystemberechtigungen ausgeführt werden können. Auf diese Weise lässt sich ein Überschreiben von Instanzdateien durch gespeicherte Prozeduren besser vermeiden, da das Betriebssystem dies verhindert.
Kennwort überprüfen (Verify password)	Ja		Überprüft das Kennwort für 'db2fenc1'.
Kennwort (Password) - dasusr1	Ja		Das Kennwort für die Benutzer-ID für den DB2-Verwaltungsserver, der zur Ausführung des DB2-Verwaltungsservers auf Ihrem System verwendet wird. Die Standardbenutzer-ID ist 'dasusr1', die Standardgruppe 'dasadm1'. Diese Benutzer-ID wird außerdem von den DB2-GUI-Tools zur Ausführung von Verwaltungstasks für die lokalen Datenbankinstanzen und Datenbanken des Servers verwendet.
Kennwort überprüfen (Verify password)	Ja		Überprüft das Kennwort für 'dasusr1'.

Tabelle 10. Konfigurierbare Parameter (Forts.)

Parametername	Erforderlich	Standardwert	Beschreibung
Kennwort (Password) - Root	Ja		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)	Ja		Überprüft das Kennwort für 'root'.
Kennwort (Password) - virtuser	Ja		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)	Ja		Überprüft das Kennwort für 'virtuser'.

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 11. Konfigurierte Parameter

Parametername	Beschreibung
Virtuelle CPUs (Virtual CPUs)	Die Anzahl der virtuellen Prozessoren, die für die durch diesen Teil dargestellte virtuelle Maschine zugeordnet werden.
Speicherkapazität (Memory size, MB)	Die Speicherkapazität in MB, die dieser virtuellen Maschine zugeordnet wird.
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)	Der Name des Benutzers mit Administratorberechtigung für die WebSphere-Umgebung.
Kennwort (Password) für den WebSphere-Administrator	Das Kennwort für den Benutzer mit Administratorberechtigung für die WebSphere-Umgebung.
Kennwort überprüfen (Verify password)	Überprüft die Benutzereingabe für das Kennwort des WebSphere-Benutzers mit Administratorberechtigung.
Physischen Hauptspeicher reservieren (Reserve physical memory)	Der physische Hauptspeicher, der für die exklusive Nutzung durch diese virtuelle Maschine reserviert wird.

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

Konfigurationsparameter des Teils für den eigenständigen WSRR-Server für das SOA Policy Gateway Basic Runtime-Muster

Erforderliche Parameter ohne Standardwert müssen konfiguriert werden, bevor das Muster implementiert werden kann.

Tabelle 12. Konfigurierbare Parameter

Parametername	Erforderlich	Standardwert	Beschreibung
Virtuelle CPUs (Virtual CPUs)	Ja	1	Die Anzahl der virtuellen Prozessoren, die für die durch diesen Teil dargestellte virtuelle Maschine zugeordnet werden.
Speicherkapazität (Memory size, MB)	Ja	4096	Die Speicherkapazität in MB, die dieser virtuellen Maschine zugeordnet wird.
Physischen Hauptspeicher reservieren (Reserve physical memory)	Ja	Falsch (False)	Der physische Hauptspeicher, der für die exklusive Nutzung durch diese virtuelle Maschine reserviert wird.
Zellenname (Cell name)	Ja	SOAPolicyBasicCell	Der Name der WebSphere-Zelle auf der virtuellen Maschine im Basic Runtime-Muster.
Knotenname (Node name)	Ja	SOAPolicyBasicNode	Der Name des WebSphere-Knoten auf der virtuellen Maschine im Basic Runtime-Muster.
Kennwort (Password) - Root	Ja		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)	Ja		Überprüft die Benutzereingabe für das Kennwort (root).
Name des WebSphere-Benutzers mit Verwaltungsaufgaben (Administrator)	Ja	virtuser	Der Name des Benutzers mit Administratorberechtigung für die WebSphere-Umgebung.
Kennwort (Password) für den WebSphere-Administrator	Ja		Das Kennwort für den Benutzer mit Administratorberechtigung für die WebSphere-Umgebung.
Kennwort überprüfen (Verify password)	Ja		Überprüft die Benutzereingabe für das Kennwort des WebSphere-Benutzers mit Administratorberechtigung.

Konfigurationsparameter des Teils für den eigenständigen WSRR-Server für das SOA Policy Gateway Basic Runtime Sample-Muster

In SOA Policy Gateway Basic Runtime Sample sind für alle Parameter Standardwerte vorkonfiguriert.

Tabelle 13. Konfigurierte Parameter

Parametername	Erforderlich	Standardwert	Beschreibung
Virtuelle CPUs (Virtual CPUs)	Ja	1	Die Anzahl der virtuellen Prozessoren, die für die durch diesen Teil dargestellte virtuelle Maschine zugeordnet werden.
Speicherkapazität (Memory size, MB)	Ja	4096	Die Speicherkapazität in MB, die dieser virtuellen Maschine zugeordnet wird.
Physischen Hauptspeicher reservieren (Reserve physical memory)	Ja	Falsch (False)	Der physische Hauptspeicher, der für die exklusive Nutzung durch diese virtuelle Maschine reserviert wird.
Kennwort (Password) - Root	Ja	password	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)	Ja	password	Überprüft die Benutzereingabe für das Kennwort (root).
Name des WebSphere-Benutzers mit Verwaltungsaufgaben (Administrator)	Ja	virtuser	Der Name des Benutzers mit Administratorberechtigung für die WebSphere-Umgebung.
Kennwort (Password) für den WebSphere-Administrator	Ja	password	Das Kennwort für den Benutzer mit Administratorberechtigung für die WebSphere-Umgebung.
Kennwort überprüfen (Verify password)	Ja	password	Überprüft die Benutzereingabe für das Kennwort des WebSphere-Benutzers mit Administratorberechtigung.

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 14. Konfigurierbare Parameter

Parametername	Beschreibung
Virtuelle CPUs (Virtual CPUs)	Die Anzahl der virtuellen Prozessoren, die für die durch diesen Teil dargestellte virtuelle Maschine zugeordnet werden.
Speicherkapazität (Memory size, MB)	Die Speicherkapazität in MB, die dieser virtuellen Maschine zugeordnet wird.
Physische CPUs reservieren (Reserve physical CPUs)	Die physischen CPUs, die für die exklusive Nutzung durch diese virtuelle Maschine reserviert werden.
Physischen Hauptspeicher reservieren (Reserve physical memory)	Der physische Hauptspeicher, der für die exklusive Nutzung durch diese virtuelle Maschine reserviert wird.
Zellenname (Cell name)	Der WebSphere-Zellenname für das Advanced Runtime-Muster.

Tabelle 14. Konfigurierbare Parameter (Forts.)

Parametername	Beschreibung
Knotenname (Node name)	Der Knotenname für den WebSphere-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)	Der Name des Benutzers mit Administratorberechtigung für die WebSphere-Umgebung.
Kennwort (Password) für den WebSphere-Administrator	Das Kennwort für den Benutzer mit Administratorberechtigung für die WebSphere-Umgebung.
Kennwort überprüfen (Verify password)	Überprüft die Benutzereingabe für das Kennwort des WebSphere-Benutzers mit Administratorberechtigung.

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

Konfigurationsparameter des WSRR-Deployment Manager-Teils für das SOA Policy Gateway Advanced Runtime-Muster

Erforderliche Parameter ohne Standardwert müssen konfiguriert werden, bevor das Muster implementiert werden kann.

Tabelle 15. Konfigurierbare Parameter

Parametername	Erforderlich	Standardwert	Beschreibung
Virtuelle CPUs (Virtual CPUs)	Ja	1	Die Anzahl der virtuellen Prozessoren, die für die durch diesen Teil dargestellte virtuelle Maschine zugeordnet werden.
Speicherkapazität (Memory size, MB)	Ja	2048	Die Speicherkapazität in MB, die dieser virtuellen Maschine zugeordnet wird.
Physische CPUs reservieren (Reserve physical CPUs)	Ja	Falsch (False)	Die physischen CPUs, die für die exklusive Nutzung durch diese virtuelle Maschine reserviert werden.
Physischen Hauptspeicher reservieren (Reserve physical memory)	Ja	Falsch (False)	Der physische Hauptspeicher, der für die exklusive Nutzung durch diese virtuelle Maschine reserviert wird.
Zellenname (Cell name)	Ja	SOAPolicyAdvancedCell	Der WebSphere-Zellenname für das Advanced Runtime-Muster.
Knotenname (Node name)	Ja	SOAPolicyAdvancedNode	Der Knotenname für den WebSphere-Knoten, der sich auf der virtuellen Maschine des Deployment Managers im Advanced Runtime-Muster befindet.

Tabelle 15. Konfigurierbare Parameter (Forts.)

Parametername	Erforderlich	Standardwert	Beschreibung
Kennwort (Password) - Root	Ja		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)	Ja		Überprüft die Benutzereingabe für das Kennwort (root).
Name des WebSphere-Benutzers mit Verwaltungsaufgaben (Administrator)	Ja	virtuser	Der Name des Benutzers mit Administratorberechtigung für die WebSphere-Umgebung.
Kennwort (Password) für den WebSphere-Administrator	Ja		Das Kennwort für den Benutzer mit Administratorberechtigung für die WebSphere-Umgebung.
Kennwort überprüfen (Verify password)	Ja		Überprüft die Benutzereingabe für das Kennwort des WebSphere-Benutzers mit Administratorberechtigung.

Konfigurationsparameter des WSRR-Deployment Manager-Teils für das SOA Policy Gateway Governance Master-Muster

Erforderliche Parameter ohne Standardwert müssen konfiguriert werden, bevor das Muster implementiert werden kann.

Tabelle 16. Konfigurierbare Parameter

Parametername	Erforderlich	Standardwert	Beschreibung
Virtuelle CPUs (Virtual CPUs)	Ja	1	Die Anzahl der virtuellen Prozessoren, die für die durch diesen Teil dargestellte virtuelle Maschine zugeordnet werden.
Speicherkapazität (Memory size, MB)	Ja	2048	Die Speicherkapazität in MB, die dieser virtuellen Maschine zugeordnet wird.
Physische CPUs reservieren (Reserve physical CPUs)	Ja	Falsch (False)	Die physischen CPUs, die für die exklusive Nutzung durch diese virtuelle Maschine reserviert werden.
Physischen Hauptspeicher reservieren (Reserve physical memory)	Ja	Falsch (False)	Der physische Hauptspeicher, der für die exklusive Nutzung durch diese virtuelle Maschine reserviert wird.
Zellenname (Cell name)	Ja	SOAPolicyGMCell	Der WebSphere-Zellenname für das Advanced Runtime-Muster.

Tabelle 16. Konfigurierbare Parameter (Forts.)

Parametername	Erforderlich	Standardwert	Beschreibung
Knotenname (Node name)	Ja	SOAPolicyGMNode	Der Knotenname für den WebSphere-Knoten, der sich auf der virtuellen Maschine des Deployment Managers im Advanced Runtime-Muster befindet.
Kennwort (Password) - Root	Ja		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)	Ja		Überprüft die Benutzereingabe für das Kennwort (root).
Name des WebSphere-Benutzers mit Verwaltungsaufgaben (Administrator)	Ja	virtuser	Der Name des Benutzers mit Administratorberechtigung für die WebSphere-Umgebung.
Kennwort (Password) für den WebSphere-Administrator	Ja		Das Kennwort für den Benutzer mit Administratorberechtigung für die WebSphere-Umgebung.
Kennwort überprüfen (Verify password)	Ja		Überprüft die Benutzereingabe für das Kennwort des WebSphere-Benutzers mit Administratorberechtigung.

Teil für angepasste WSRR-Knoten

Der 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 17. Konfigurierbare Parameter

Parametername	Beschreibung
Virtuelle CPUs (Virtual CPUs)	Die Anzahl der virtuellen Prozessoren, die für die durch diesen Teil dargestellte virtuelle Maschine zugeordnet werden.
Speicherkapazität (Memory size, MB)	Die Speicherkapazität in MB, die dieser virtuellen Maschine zugeordnet wird.
Physische CPUs reservieren (Reserve physical CPUs)	Die physischen CPUs, die für die exklusive Nutzung durch diese virtuelle Maschine reserviert werden.
Physischen Hauptspeicher reservieren (Reserve physical memory)	Der physische Hauptspeicher, der für die exklusive Nutzung durch diese virtuelle Maschine reserviert wird.
Zellenname (Cell name)	Der Wert für den Zellennamen in der Konfiguration des Teils für angepasste Knoten wird ignoriert. Der Zellenname, der in der Konfiguration des Deployment Manager-Teils angegeben wird, wird verwendet.
Knotenname (Node name)	Der Knotenname für den WebSphere-Knoten, der sich auf der virtuellen Maschine des angepassten Knotens im Advanced Runtime-Muster befindet.

Tabelle 17. Konfigurierbare Parameter (Forts.)

Parametername	Beschreibung
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)	Der Name des Benutzers mit Administratorberechtigung für die WebSphere-Umgebung.
Kennwort (Password) für den WebSphere-Administrator	Das Kennwort für den Benutzer mit Administratorberechtigung für die WebSphere-Umgebung.
Kennwort überprüfen (Verify password)	Überprüft die Benutzereingabe für das Kennwort des WebSphere-Benutzers mit Administratorberechtigung.

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

Konfigurationsparameter des Teils für angepasste WSRR-Knoten für das SOA Policy Gateway Advanced Runtime-Muster

Erforderliche Parameter ohne Standardwert müssen konfiguriert werden, bevor das Muster implementiert werden kann.

Tabelle 18. Konfigurierbare Parameter

Parametername	Erforderlich	Standardwert	Beschreibung
Virtuelle CPUs (Virtual CPUs)	Ja	2	Die Anzahl der virtuellen Prozessoren, die für die durch diesen Teil dargestellte virtuelle Maschine zugeordnet werden.
Speicherkapazität (Memory size, MB)	Ja	4096	Die Speicherkapazität in MB, die dieser virtuellen Maschine zugeordnet wird.
Physische CPUs reservieren (Reserve physical CPUs)	Ja	Falsch (False)	Die physischen CPUs, die für die exklusive Nutzung durch diese virtuelle Maschine reserviert werden.
Physischen Hauptspeicher reservieren (Reserve physical memory)	Ja	Falsch (False)	Der physische Hauptspeicher, der für die exklusive Nutzung durch diese virtuelle Maschine reserviert wird.
Knotenname (Node name)	Ja	SOAPolicyAdvancedNode	Der Knotenname für den WebSphere-Knoten, der sich auf der virtuellen Maschine des angepassten Knotens im Advanced Runtime-Muster befindet.
Kennwort (Password) - Root	Ja		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)	Ja		Überprüft die Benutzereingabe für das Kennwort (root).

Tabelle 18. Konfigurierbare Parameter (Forts.)

Parametername	Erforderlich	Standardwert	Beschreibung
Name des WebSphere-Benutzers mit Verwaltungsaufgaben (Administrator)	Ja	virtuser	Der Name des Benutzers mit Administratorberechtigung für die WebSphere-Umgebung.
Kennwort (Password) für den WebSphere-Administrator	Ja		Das Kennwort für den Benutzer mit Administratorberechtigung für die WebSphere-Umgebung.
Kennwort überprüfen (Verify password)	Ja		Überprüft die Benutzereingabe für das Kennwort des WebSphere-Benutzers mit Administratorberechtigung.

Konfigurationsparameter des Teils für angepasste WSRR-Knoten für das SOA Policy Gateway Governance Master-Muster

Erforderliche Parameter ohne Standardwert müssen konfiguriert werden, bevor das Muster implementiert werden kann.

Tabelle 19. Konfigurierbare Parameter

Parametername	Erforderlich	Standardwert	Beschreibung
Virtuelle CPUs (Virtual CPUs)	Ja	2	Die Anzahl der virtuellen Prozessoren, die für die durch diesen Teil dargestellte virtuelle Maschine zugeordnet werden.
Speicherkapazität (Memory size, MB)	Ja	4096	Die Speicherkapazität in MB, die dieser virtuellen Maschine zugeordnet wird.
Physische CPUs reservieren (Reserve physical CPUs)	Ja	Falsch (False)	Die physischen CPUs, die für die exklusive Nutzung durch diese virtuelle Maschine reserviert werden.
Physischen Hauptspeicher reservieren (Reserve physical memory)	Ja	Falsch (False)	Der physische Hauptspeicher, der für die exklusive Nutzung durch diese virtuelle Maschine reserviert wird.
Knotenname (Node name)	Ja	SOAPolicyGMNode	Der Knotenname für den WebSphere-Knoten, der sich auf der virtuellen Maschine des angepassten Knotens im Advanced Runtime-Muster befindet.
Kennwort (Password) - Root	Ja		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)	Ja		Überprüft die Benutzereingabe für das Kennwort (root).

Tabelle 19. Konfigurierbare Parameter (Forts.)

Parametername	Erforderlich	Standardwert	Beschreibung
Name des WebSphere-Benutzers mit Verwaltungsaufgaben (Administrator)	Ja	virtuser	Der Name des Benutzers mit Administratorberechtigung für die WebSphere-Umgebung.
Kennwort (Password) für den WebSphere-Administrator	Ja		Das Kennwort für den Benutzer mit Administratorberechtigung für die WebSphere-Umgebung.
Kennwort überprüfen (Verify password)	Ja		Überprüft die Benutzereingabe für das Kennwort des WebSphere-Benutzers mit Administratorberechtigung.

Scriptpakete

Mit IBM SOA Policy Gateway Pattern werden vier Scriptpakete bereitgestellt.

In diesem Muster sind die folgenden Scriptpakete enthalten:

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

Script: SOA Policy Gateway 2.0.0.0 - DataPower Domain

Das DataPower Domain-Script stellt die DataPower-Domäne während der Implementierung bereit. Das Script konfiguriert die Verbindung zwischen einer einzelnen DataPower-Domäne und der WSRR-Laufzeit. Für jede DataPower-Domäne, die mit der WSRR-Laufzeit verbunden wird, ist ein separates DataPower Domain-Script erforderlich.

Parameter

Tabelle 20. Konfigurierbare Parameter

Parametername	Beschreibung
DataPower_hostname	Der Hostname des DataPower-Geräts, auf dem die Beispielanwendung installiert wird.
DataPower_XML_mgmt_port	Der Port, der für DataPower XML Management Interface verwendet wird, in der Regel 5550.
Datapower_admin_id	Die Administrator-ID mit den entsprechenden Berechtigungen zur Verwendung von XML Management Interface.
DataPower_admin_password	Das Kennwort für 'DataPower_admin_id'.
Kennwort überprüfen (Verify password)	Überprüft die Benutzereingabe für 'DataPower_admin_password'.
New_DataPower_domain	Der neue Domänenname, der auf dem DataPower-Gerät 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.

Tabelle 20. Konfigurierbare Parameter (Forts.)

Parametername	Beschreibung
securityFileCleanUp	Legt fest, ob die Datei `DomainZipFile.zip` und die WSRR-Zertifikate, die in DataPower hochgeladen wurden, von der WSRR-Instanz, auf der die Scriptpakete ausgeführt werden, gelöscht werden. Wenn diese Datei nicht entfernt wird, könnte sie ein Sicherheitsrisiko darstellen, wenn die Zertifikate auf der Instanz verbleiben.

SOA Policy Gateway 2.0.0.0 - Konfigurationsparameter des DataPower Domain-Scripts für das SOA Policy Gateway Basic Runtime-Muster

Erforderliche Parameter ohne Standardwert müssen konfiguriert werden, bevor das Muster implementiert werden kann.

Tabelle 21. Konfigurierbare Parameter

Parametername	Erforderlich	Standardwert	Beschreibung
DataPower_hostname	Ja		Der Hostname des DataPower-Geräts, auf dem die Beispielanwendung installiert wird.
DataPower_XML_mgmt_port	Ja	5550	Der Port, der für DataPower XML Management Interface verwendet wird, in der Regel 5550.
Datapower_admin_id	Ja		Die Administrator-ID mit den entsprechenden Berechtigungen zur Verwendung von XML Management Interface.
DataPower_admin_password	Ja		Das Kennwort für 'DataPower_admin_id'.
Kennwort überprüfen (Verify password)	Ja		Überprüft die Benutzereingabe für 'DataPower_admin_password'.
New_DataPower_domain	Ja		Der neue Domänenname, der auf dem DataPower-Gerät 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.

Tabelle 21. Konfigurierbare Parameter (Forts.)

Parametername	Erforderlich	Standardwert	Beschreibung
Remove_security_files	Ja	true	Legt fest, ob die Datei `DomainZipFile.zip` und die WSRR-Zertifikate, die in DataPower hochgeladen wurden, von der WSRR-Instanz, auf der die Scriptpakete ausgeführt werden, gelöscht werden. Wenn diese Datei nicht entfernt wird, könnte sie ein Sicherheitsrisiko darstellen, wenn die Zertifikate auf der Instanz verbleiben.

SOA Policy Gateway 2.0.0.0 - Konfigurationsparameter des DataPower Domain-Scripts für das SOA Policy Gateway Advanced Runtime-Muster

Erforderliche Parameter ohne Standardwert müssen konfiguriert werden, bevor das Muster implementiert werden kann.

Tabelle 22. Konfigurierbare Parameter

Parametername	Erforderlich	Standardwert	Beschreibung
DataPower_hostname	Ja		Der Hostname des DataPower-Geräts, auf dem die Beispielanwendung installiert wird.
DataPower_XML_mgmt_port	Ja	5550	Der Port, der für DataPower XML Management Interface verwendet wird, in der Regel 5550.
Datapower_admin_id	Ja		Die Administrator-ID mit den entsprechenden Berechtigungen zur Verwendung von XML Management Interface.
DataPower_admin_password	Ja		Das Kennwort für 'DataPower_admin_id'.
Kennwort überprüfen (Verify password)	Ja		Überprüft die Benutzereingabe für 'DataPower_admin_password'.
New_DataPower_domain	Ja		Der neue Domänenname, der auf dem DataPower-Gerät 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.

Tabelle 22. Konfigurierbare Parameter (Forts.)

Parametername	Erforderlich	Standardwert	Beschreibung
Remove_security_files	Ja	true	Legt fest, ob die Datei `DomainZipFile.zip` und die WSRR-Zertifikate, die in DataPower hochgeladen wurden, von der WSRR-Instanz, auf der die Scriptpakete ausgeführt werden, gelöscht werden. Wenn diese Datei nicht entfernt wird, könnte sie ein Sicherheitsrisiko darstellen, wenn die Zertifikate auf der Instanz verbleiben.

Script: SOA Policy Gateway 2.0.0.0 - Promotion

Durch das Umstufungsscript 'Promotion' kann ein SOA Policy Gateway Basic Runtime- oder SOA Policy Gateway 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 23. Konfigurierbare Parameter

Parametername	Beschreibung
WSRR_GOV_DMGR_hostname	Der Hostname des Deployment Managers (Dmgr) für den WSRR-Cluster.
WSRR_GOV_DMGR_cellname	Der WebSphere-Zellenname für den WSRR-Cluster.
WSRR_GOV_admin_user	Die Administrator-ID für die WebSphere WSRR-Governance-Zelle.
WSRR_GOV_admin_password	Das Kennwort für die Administrator-ID für die WebSphere-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.
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. Dies ist das Kennwort, das beim Exportieren dieses LTPA-Schlüssels verwendet wird.
Kennwort überprüfen (Verify password)	Überprüft die Benutzereingabe für 'LTPA_key_password'.

SOA Policy Gateway 2.0.0.0 - Konfigurationsparameter des Promotion-Scripts für das SOA Policy Gateway Basic Runtime-Muster

Erforderliche Parameter ohne Standardwert müssen konfiguriert werden, bevor das Muster implementiert werden kann.

Tabelle 24. Konfigurierbare Parameter

Parametername	Erforderlich	Standardwert	Beschreibung
WSRR_GOV_DMGR_hostname	Ja		Der Hostname des Deployment Managers (Dmgr) für den WSRR-Cluster.
WSRR_GOV_DMGR_cellname	Ja		Der WebSphere-Zellenname für den WSRR-Cluster.
WSRR_GOV_admin_user	Ja		Die Administrator-ID für die WebSphere WSRR-Governance-Zelle.
WSRR_GOV_admin_password	Ja		Das Kennwort für die Administrator-ID für die WebSphere-WSRR-Governance-Zelle.
Kennwort überprüfen (Verify password)	Ja		Überprüft die Benutzereingabe für 'WSRR_GOV_admin_password'.
Promotion_environment	Ja		Muss den Wert 'staging','production' oder 'Unset' haben. Bei diesen Werten muss die Groß-/Kleinschreibung beachtet werden und sie müssen exakt übereinstimmen.
LTPA_key_password	Ja		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. Dies ist das Kennwort, das beim Exportieren dieses LTPA-Schlüssels verwendet wird.
Kennwort überprüfen (Verify password)	Ja		Überprüft die Benutzereingabe für 'LTPA_key_password'.

SOA Policy Gateway 2.0.0.0 - Konfigurationsparameter des Promotion-Scripts für das SOA Policy Gateway Advanced Runtime-Muster

Erforderliche Parameter ohne Standardwert müssen konfiguriert werden, bevor das Muster implementiert werden kann.

Tabelle 25. Konfigurierbare Parameter

Parametername	Erforderlich	Standardwert	Beschreibung
WSRR_GOV_DMGR_hostname	Ja		Der Hostname des Deployment Managers (Dmgr) für den WSRR-Cluster.
WSRR_GOV_DMGR_cellname	Ja		Der WebSphere-Zellenname für den WSRR-Cluster.

Tabelle 25. Konfigurierbare Parameter (Forts.)

Parametername	Erforderlich	Standardwert	Beschreibung
WSRR_GOV_admin_user	Ja		Die Administrator-ID für die WebSphere WSRR-Governance-Zelle.
WSRR_GOV_admin_password	Ja		Das Kennwort für die Administrator-ID für die WebSphere-WSRR-Governance-Zelle.
Kennwort überprüfen (Verify password)	Ja		Überprüft die Benutzereingabe für 'WSRR_GOV_admin_password'.
Promotion_environment	Ja		Muss den Wert 'staging','production' oder 'Unset' haben. Bei diesen Werten muss die Groß-/Kleinschreibung beachtet werden und sie müssen exakt übereinstimmen.
LTPA_key_password	Ja		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. Dies ist das Kennwort, das beim Exportieren dieses LTPA-Schlüssels verwendet wird.
Kennwort überprüfen (Verify password)	Ja		Überprüft die Benutzereingabe für 'LTPA_key_password'.

Script: SOA Policy Gateway 2.0.0.0 - Sample

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

Parameter

Anmerkung: Bei jedem Parameter, der den Wert 'Unset' erfordert, ist die Groß-/Kleinschreibung zu beachten.

Tabelle 26. Konfigurierbare Parameter

Parametername	Beschreibung
SCP_host	Der Hostname des SCP-Servers, der die Datei `DomainZipFile.zip` enthält.
SCP_user	Der Benutzername, der zum Herstellen der Verbindung zum SCP-Server zu verwenden ist.
SCP_password	Das Kennwort, das zur Anmeldung am SCP-Server zu verwenden ist.
Kennwort überprüfen (Verify password)	Überprüft die Benutzereingabe für 'SCP_password'.
SCP_zip_location	Die URI-Position der Datei `DomainZipFile.zip`. Beispiel: `/files/DomainZipFile.zip`.

Tabelle 26. Konfigurierbare Parameter (Forts.)

Parametername	Beschreibung
CLIENT_PUBLIC_KEY_file	Der Name der PEM-Zertifikatsdatei, die für die Verbindung mit dem XML Management Interface-Port für DataPower-Geräte verwendet wird. Verwenden Sie den Wert „Unset" nur für die Serverauthentifizierung und wenn SSL nicht verwendet wird.
CLIENT_PUBLIC _KEY_password	Das Kennwort für das öffentliche Zertifikat, das für die Verbindung mit dem XML Management Interface-Port für DataPower-Geräte verwendet wird. Der Wert ist „Unset", wenn kein Kennwort verwendet wird.
Kennwort überprüfen (Verify password)	Überprüft die Benutzereingabe für CLIENT_PUBLIC_KEY_password.
CLIENT_PRIVATE_KEY_file	Der Name der PEM-Schlüsseldatei, die für die Verbindung mit dem XML Management Interface-Port für DataPower-Geräte verwendet wird. Dieser Parameter ist für die gegenseitige Authentifizierung erforderlich. Verwenden Sie den Wert „Unset" nur für die Serverauthentifizierung und wenn SSL nicht verwendet wird.
CLIENT_PRIVATE_KEY_password	Das Kennwort für die Schlüsseldatei, die für die Verbindung mit dem XML Management Interface-Port für DataPower-Geräte verwendet wird. Dieser Parameter ist für die gegenseitige Authentifizierung erforderlich. Der Wert ist „Unset", wenn kein Kennwort verwendet wird.
Kennwort überprüfen (Verify password)	Überprüft die Benutzereingabe für CLIENT_PRIVATE_KEY_password.
CLI_FILE_file	Der Name der CLI-Datei, die in der Datei `DomainZipFile.zip` enthalten ist. Diese CLI-Datei (CLI, Befehlszeilenschnittstelle) wird am Ende der Domäneninstallation und der WSRR-Serverkonfiguration ausgeführt.
Kennwort überprüfen (Verify password)	Überprüft die Benutzereingabe für LTPA_KEY_password.
DataPower_hostname	Der Hostname des DataPower-Geräts, auf dem die Beispielanwendung installiert wird.
DataPower_XML_mgmt_port	Der Port, der für DataPower XML Management Interface verwendet wird.
DataPower_admin_id	Die Administrator-ID mit den entsprechenden Berechtigungen zur Verwendung von XML Management Interface.
DataPower_admin_password	Das Kennwort für 'DataPower_admin_id'.
Kennwort überprüfen (Verify password)	Überprüft die Benutzereingabe für 'DataPower_admin_password'.
SOAPolicySample_DataPower_domain	Der Name der Beispieldomäne. Dieser Name darf mit keiner vorhandenen Domäne im DataPower-Gerät übereinstimmen.
SamplePolicySample_starting_port	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 prüft nicht, ob die Ports frei sind.
LDAP_hostname	Das Beispiel verwendet einen LDAP-Server und dieser Parameter gibt den Hostnamen dieses Servers an.
LDAP_port	Der nicht sichere Port des LDAP-Servers. In der Regel 389.
LDAP_password	Das Kennwort, das beim Binden mit dem LDAP_DN verwendet wird.
Kennwort überprüfen (Verify password)	Überprüft die Benutzereingabe für LDAP_password.
LDAP_DN	Der definierte Name, der zum Binden an das LDAP verwendet wird. Beispiel: cn=root,dc=ibm.com.

SOA Policy Gateway 2.0.0.0 - Konfigurationsparameter des Sample-Scripts für das SOA Policy Gateway Basic Runtime Sample-Muster

Erforderliche Parameter ohne Standardwert müssen konfiguriert werden, bevor das Muster implementiert werden kann.

Anmerkung: Bei jedem Parameter, der den Wert 'Unset' erfordert, ist die Groß-/Kleinschreibung zu beachten.

Tabelle 27. Konfigurierbare Parameter

Parametername	Erforderlich	Standardwert	Beschreibung
SCP_host	Ja		Der Hostname des SCP-Servers, der die Datei `DomainZipFile.zip` enthält.
SCP_user	Ja		Der Benutzername, der zum Herstellen der Verbindung zum SCP-Server zu verwenden ist.
SCP_password	Ja		Das Kennwort, das zur Anmeldung am SCP-Server zu verwenden ist.
Kennwort überprüfen (Verify password)	Ja		Überprüft die Benutzereingabe für 'SCP_password'.
SCP_zip_location	Ja		Die URI-Position der Datei `DomainZipFile.zip`. Beispiel: `/files/DomainZipFile.zip`.
CLIENT_PUBLIC_KEY_file	Ja		Der Name der PEM-Zertifikatsdatei, die für die Verbindung mit dem XML Management Interface-Port für DataPower-Geräte verwendet wird. Verwenden Sie den Wert „Unset” nur für die Serverauthentifizierung und wenn SSL nicht verwendet wird.
CLIENT_PUBLIC _KEY_password	Ja		Das Kennwort für das öffentliche Zertifikat, das für die Verbindung mit dem XML Management Interface-Port für DataPower-Geräte verwendet wird. Der Wert ist „Unset”, wenn kein Kennwort verwendet wird.
Kennwort überprüfen (Verify password)	Ja		Überprüft die Benutzereingabe für CLIENT_PUBLIC_KEY_password.
CLIENT_PRIVATE_KEY_file	Ja		Der Name der PEM-Schlüsseldatei, die für die Verbindung mit dem XML Management Interface-Port für DataPower-Geräte verwendet wird. Dieser Parameter ist für die gegenseitige Authentifizierung erforderlich. Verwenden Sie den Wert „Unset” nur für die Serverauthentifizierung und wenn SSL nicht verwendet wird.

Tabelle 27. Konfigurierbare Parameter (Forts.)

Parametername	Erforderlich	Standardwert	Beschreibung
CLIENT_PRIVATE_KEY_password	Ja		Das Kennwort für die Schlüsseldatei, die für die Verbindung mit dem XML Management Interface-Port für DataPower-Geräte verwendet wird. Dieser Parameter ist für die gegenseitige Authentifizierung erforderlich. Der Wert ist „Unset", wenn kein Kennwort verwendet wird.
Kennwort überprüfen (Verify password)	Ja		Überprüft die Benutzereingabe für CLIENT_PRIVATE_KEY_password.
DataPower_hostname	Ja		Der Hostname des DataPower-Geräts, auf dem die Beispielanwendung installiert wird.
DataPower_XML_mgmt_port	Ja	5550	Der Port, der für DataPower XML Management Interface verwendet wird.
DataPower_admin_id	Ja		Die Administrator-ID mit den entsprechenden Berechtigungen zur Verwendung von XML Management Interface.
DataPower_admin_password	Ja		Das Kennwort für 'DataPower_admin_id'.
Kennwort überprüfen (Verify password)	Ja		Überprüft die Benutzereingabe für 'DataPower_admin_password'.
SOAPolicySample_DataPower_domain	Ja	SOAPolicySample	Der Name der Beispieldomäne. Dieser Name darf mit keiner vorhandenen Domäne im DataPower-Gerät übereinstimmen.
SOAPolicySample_starting_port	Ja	62001	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 prüft nicht, ob die Ports frei sind.
LDAP_hostname	Ja		Das Beispiel verwendet einen LDAP-Server und dieser Parameter gibt den Hostnamen dieses Servers an.
LDAP_port	Ja	389	Der nicht sichere Port des LDAP-Servers. In der Regel 389.
LDAP_password	Ja		Das Kennwort, das beim Binden mit dem LDAP_DN verwendet wird.

Tabelle 27. Konfigurierbare Parameter (Forts.)

Parametername	Erforderlich	Standardwert	Beschreibung
Kennwort überprüfen (Verify password)	Ja		Überprüft die Benutzereingabe für LDAP_password.
LDAP_DN	Ja		Der definierte Name, der zum Binden an das LDAP verwendet wird. Beispiel: cn=root,dc=ibm.com.

Script: SOA Policy Gateway 2.0.0.0 - Security

Das Sicherheitsscript 'Security' kopiert Sicherheitsinformationen, die in einer ZIP-Datei enthalten und die für die Kommunikation mit einem DataPower-Gerät erforderlich sind, auf das Deployment Manager-System ('Dmgr') oder das WSRR-System. Die Daten werden von einem externen Dateiserver kopiert, der Linux Secure Copy Protocol (SCP) unterstützt.

Die Sicherheitsdatei, die kopiert wird, hat den folgenden Inhalt:

- DPC-Zugriffszertifikat (DPC Access Certificate)
- Öffentliches DPC-Zugriffszertifikat (DPC Access Public Certificate)
- Privater DPC-Schlüssel (DPC Private Key)
- DP-CLI-Script
- Ordner der Zertifikatskette

Das Befehlszeilenschnittstellenscript (CLI-Script) für DataPower ermöglicht die Konfiguration einer implementierten Domäne während der Musterimplementierungsphase.

Anmerkung: Vertrauliche Sicherheitszertifikate sollten im Anschluss an die Implementierung vom externen Dateiserver gelöscht werden.

Parameter

Tabelle 28. Konfigurierbare Parameter

Parametername	Beschreibung
SCP_host	Der Hostname des SCP-Servers, der die Datei `DomainZipFile.zip` enthält.
SCP_user	Der Benutzername, der zum Herstellen der Verbindung zum SCP-Server zu verwenden ist.
SCP_password	Das Kennwort, das zur Anmeldung am SCP-Server zu verwenden ist.
Kennwort überprüfen (Verify password)	Überprüft die Benutzereingabe für 'SCP_password'.
SCP_zip_location	Die URI-Position der Datei `DomainZipFile.zip`. Beispiel: `/files/DomainZipFile.zip`.
CLIENT_PUBLIC_KEY_file	Der Name der PEM-Zertifikatsdatei, die für die Verbindung mit dem XML Management Interface-Port für DataPower-Geräte verwendet wird.
CLIENT_PUBLIC_KEY_password	Das Kennwort für das Clientzertifikat, das für die Verbindung mit dem XML Management Interface-Port für DataPower-Geräte verwendet wird. Dieser Parameter ist, sofern verfügbar, für die gegenseitige Authentifizierung erforderlich. Der Wert kann „Unset" sein, wenn kein Kennwort verwendet wird.
CLIENT_PRIVATE_KEY_file	Der Name der PEM-Schlüsseldatei, die für die Verbindung mit dem XML Management Interface-Port für DataPower-Geräte verwendet wird. Dieser Parameter ist für die gegenseitige Authentifizierung erforderlich.

Tabelle 28. Konfigurierbare Parameter (Forts.)

Parametername	Beschreibung
CLIENT_PRIVATE_KEY_password	Das Kennwort für die Schlüsseldatei, die für die Verbindung mit dem XML Management Interface-Port für DataPower-Geräte verwendet wird. Dieser Parameter ist für die gegenseitige Authentifizierung erforderlich. Der Wert kann „Unset" sein, wenn kein Kennwort verwendet wird.
CLI_file	Der Name der CLI-Datei, die in der Datei `DomainZipFile.zip` enthalten ist. Diese CLI-Datei (CLI, Befehlszeilenschnittstelle) wird am Ende der Domäneninstallation und der WSRR-Serverkonfiguration ausgeführt.

SOA Policy Gateway 2.0.0.0 - Konfigurationsparameter des Security-Scripts für das SOA Policy Gateway Basic Runtime-Muster

Erforderliche Parameter ohne Standardwert müssen konfiguriert werden, bevor das Muster implementiert werden kann.

Tabelle 29. Konfigurierbare Parameter

Parametername	Erforderlich	Standardwert	Beschreibung
SCP_host	Ja		Der Hostname des SCP-Servers, der die Datei `DomainZipFile.zip` enthält.
SCP_user	Ja		Der Benutzername, der zum Herstellen der Verbindung zum SCP-Server zu verwenden ist.
SCP_password	Ja		Das Kennwort, das zur Anmeldung am SCP-Server zu verwenden ist.
Kennwort überprüfen (Verify password)	Ja		Überprüft die Benutzereingabe für 'SCP_password'.
SCP_zip_location	Ja		Die URI-Position der Datei `DomainZipFile.zip`. Beispiel: `/files/DomainZipFile.zip`.
CLIENT_PUBLIC_KEY_file	Ja		Der Name der PEM-Zertifikatsdatei, die für die Verbindung mit dem XML Management Interface-Port für DataPower-Geräte verwendet wird.
CLIENT_PUBLIC_KEY_password	Ja		Das Kennwort für das Clientzertifikat, das für die Verbindung mit dem XML Management Interface-Port für DataPower-Geräte verwendet wird. Dieser Parameter ist, sofern verfügbar, für die gegenseitige Authentifizierung erforderlich. Der Wert kann „Unset" sein, wenn kein Kennwort verwendet wird.

Tabelle 29. Konfigurierbare Parameter (Forts.)

Parametername	Erforderlich	Standardwert	Beschreibung
CLIENT_PRIVATE_KEY_file	Ja		Der Name der PEM-Schlüsseldatei, die für die Verbindung mit dem XML Management Interface-Port für DataPower-Geräte verwendet wird. Dieser Parameter ist für die gegenseitige Authentifizierung erforderlich.
CLIENT_PRIVATE_KEY_password	Ja		Das Kennwort für die Schlüsseldatei, die für die Verbindung mit dem XML Management Interface-Port für DataPower-Geräte verwendet wird. Dieser Parameter ist für die gegenseitige Authentifizierung erforderlich. Der Wert kann „Unset" sein, wenn kein Kennwort verwendet wird.
CLI_file	Ja	Unset	Der Name der CLI-Datei, die in der Datei `DomainZipFile.zip` enthalten ist. Diese CLI-Datei (CLI, Befehlszeilenschnittstelle) wird am Ende der Domäneninstallation und der WSRR-Serverkonfiguration ausgeführt.

SOA Policy Gateway 2.0.0.0 - Konfigurationsparameter des Security-Scripts für das SOA Policy Gateway Advanced Runtime-Muster

Erforderliche Parameter ohne Standardwert müssen konfiguriert werden, bevor das Muster implementiert werden kann.

Tabelle 30. Konfigurierbare Parameter

Parametername	Erforderlich	Standardwert	Beschreibung
SCP_zip_location	Ja		Die URI-Position der Datei `DomainZipFile.zip`. Beispiel: `/files/DomainZipFile.zip`.
SCP_host	Ja		Der Hostname des SCP-Servers, der die Datei `DomainZipFile.zip` enthält.
SCP_user	Ja		Der Benutzername, der zum Herstellen der Verbindung zum SCP-Server zu verwenden ist.
SCP_password	Ja		Das Kennwort, das zur Anmeldung am SCP-Server zu verwenden ist.
Kennwort überprüfen (Verify password)	Ja		Überprüft die Benutzereingabe für 'SCP_password'.

Tabelle 30. Konfigurierbare Parameter (Forts.)

Parametername	Erforderlich	Standardwert	Beschreibung
CLIENT_PUBLIC_KEY_file	Ja		Der Name der PEM-Zertifikatsdatei, die für die Verbindung mit dem XML Management Interface-Port für DataPower-Geräte verwendet wird.
CLIENT_PUBLIC_KEY_password	Ja		Das Kennwort für das Clientzertifikat, das für die Verbindung mit dem XML Management Interface-Port für DataPower-Geräte verwendet wird. Dieser Parameter ist, sofern verfügbar, für die gegenseitige Authentifizierung erforderlich. Der Wert kann „Unset" sein, wenn kein Kennwort verwendet wird.
CLIENT_PRIVATE_KEY_file	Ja		Der Name der PEM-Schlüsseldatei, die für die Verbindung mit dem XML Management Interface-Port für DataPower-Geräte verwendet wird. Dieser Parameter ist für die gegenseitige Authentifizierung erforderlich.
CLIENT_PRIVATE_KEY_password	Ja		Das Kennwort für die Schlüsseldatei, die für die Verbindung mit dem XML Management Interface-Port für DataPower-Geräte verwendet wird. Dieser Parameter ist für die gegenseitige Authentifizierung erforderlich. Der Wert kann „Unset" sein, wenn kein Kennwort verwendet wird.
CLI_file	Ja	Unset	Der Name der CLI-Datei, die in der Datei `DomainZipFile.zip` enthalten ist. Diese CLI-Datei (CLI, Befehlszeilenschnittstelle) wird am Ende der Domäneninstallation und der WSRR-Serverkonfiguration ausgeführt.

Kapitel 5. Mit IBM SOA Policy Gateway Pattern arbeiten

IBM SOA Policy Gateway Pattern stellt eine Musterdefinition für die wiederholt anwendbare Implementierung der Topologie bereit, die das Produkt ausmacht. Jedes Muster stellt eine bestimmte Funktion in IBM SOA Policy Gateway Pattern bereit und enthält mehrere Images, die die einzelnen Muster unterstützen. Die Muster müssen vor der Implementierung nach den Geschäftsanforderungen konfiguriert werden.

Im Rahmen des Implementierungsprozesses konfigurieren Sie die Parameter der Teile. Weitere Informationen finden Sie in „Muster implementieren" auf Seite 74.

Zugehörige Tasks:

Kapitel 3, „Erste Schritte mit IBM SOA Policy Gateway Pattern", auf Seite 11
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 den Komponenten dieses Szenarios vertraut zu machen, die Gründe zu verstehen, aus denen es sich für ein Unternehmen anbietet, diesem Szenario zu folgen, die beteiligten Benutzerrollen kennen zu lernen und sich eine Übersicht über die durch das Produkt gelieferte Funktionalität zu verschaffen.

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. Ermitteln Sie die erforderlichen Governance-Anforderungen und Governance-Ressourcen.

Bereiten Sie im Hinblick auf die Implementierung der Umgebung das DataPower-Gerät für die Fernverwaltung vor und stellen Sie Ressourcen zusammen, die für eine sichere Kommunikation mit dem Gerät erforderlich sind. Ein Test der Umgebung kann durch eine Implementierung von SOA Policy Gateway Basic Runtime Sample durchgeführt werden. Der Test überprüft, ob die Umgebung ordnungsgemäß für die Implementierung konfiguriert ist, und demonstriert die Durchsetzung der Richtlinien. Nach der Überprüfung der Umgebung wird die gewünschte Governance- und Laufzeitkonfiguration für IBM SOA Policy Gateway Pattern unter Verwendung bewährter WSRR-Verfahren festgelegt. Die Implementierung des Musters beginnt mit dem Governance Master. Anschließend erfolgt die Implementierung der Runtime-Muster, die der gewünschten Konfiguration entsprechen.

IBM SOA Policy Gateway Pattern vorbereiten und implementieren

Bereiten Sie DataPower vor und stellen Sie die Sicherheitsdateien zusammen:

1. Bereiten Sie das DataPower-Gerät für die Fernverwaltung vor. Weitere Informationen finden Sie in „DataPower für IBM SOA Policy Gateway Pattern konfigurieren" auf Seite 65.
2. Wenn das DataPower-Gerät geschützt wird, lesen Sie den Sicherheitsabschnitt zu DataPower. Stellen Sie anschließend die DataPower-Sicherheitsdateien zusammen, für die Kommunikation mit dem Gerät benötigt werden.

3. Stellen Sie sicher, dass eine im System implementierte DataPower-Instanz in der Cloudumgebung mit dem Gerät kommunizieren kann und dass das Gerät mit einem implementierten System kommunizieren kann.

SOA Policy Gateway Basic Runtime Sample kann dazu verwendet werden, vor einer Implementierung in der Produktionsumgebung die Funktionen des Musters zu demonstrieren. Wenn die Verwendung von Basic Runtime Sample erforderlich ist, führen Sie die folgenden Schritte aus:

1. Geben Sie einen SCP-Server unter Linux an, der von einem implementierten System in der Cloud aus zugänglich ist. SCP steht für Secure Copy Protocol. Der SCP-Server stellt eine Möglichkeit dar, die für das Muster externen Sicherheitsdateien bereitzustellen, sodass das Muster nicht für jede Sicherheitskonfiguration geändert werden muss.
2. Stellen Sie einen LDAP-Server als Host für Sicherheits-IDs bereit, die von der in DataPower implementierten Beispielanwendung verwendet werden. Weitere Informationen finden Sie in „LDAP für das Beispiel konfigurieren" auf Seite 72.
3. Implementieren Sie das SOA Policy Gateway Basic Runtime Sample-Muster, um die Infrastruktur zu validieren. Weitere Informationen finden Sie in „SOA Policy Gateway Basic Runtime Sample-Muster implementieren" auf Seite 75.
4. Wenn die Verwendung des Beispiels abgeschlossen ist, wird der LDAP-Server nicht mehr benötigt.

Bereiten Sie die Implementierung in der Produktionsumgebung vor:

1. Legen Sie die Skalierung fest, die für die Implementierung erforderlich ist. Bestimmen Sie die Clustergrößen für die Governance Master-Implementierung und die Laufzeitimplementierung.

   Anmerkung: Wenn ein Cluster implementiert ist, kann er nicht durch ein weiteres Cluster-Member erweitert werden.
2. Definieren Sie den Zellennamen sowie die Benutzer-ID mit Administratorberechtigung und das Kennwort für den Governance Master.
3. Stellen Sie die DataPower-Sicherheitsdatei `DomainZipFile.zip` auf einem SCP-Server bereit. Weitere Informationen finden Sie in „Sicherheitsdatei `DomainZipFile.zip` erstellen" auf Seite 66.

Implementieren Sie den Governance Master für die Produktionsumgebung:

1. Implementieren Sie ein SOA Policy Gateway Governance Master-Muster. Warten Sie ab, bis die Implementierung abgeschlossen ist, bevor Sie Laufzeitmuster für die Produktionsumgebung implementieren. Weitere Informationen finden Sie in „SOA Policy Gateway Governance Master-Muster implementieren" auf Seite 76.

Implementieren Sie die Laufzeitmuster für die Produktionsumgebung:

1. Bestimmen Sie, ob eine Clusterumgebung oder eine eigenständige Umgebung erforderlich ist.
2. Wenn mehrere DataPower-Domänen erforderlich sind, klonen Sie für jede benötigte Domäne das Basic Runtime-Muster oder das Advanced Runtime-Muster und fügen den einzelnen Klonen DataPower-Scriptpakete hinzu.

   Anmerkung: Nach Abschluss dieser Konfiguration können keine weiteren DataPower-Domänen hinzugefügt werden.
   Weitere Informationen finden Sie in „Mit mehreren DataPower-Domänen implementieren" auf Seite 82.

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 77.
4. Legen Sie fest, ob die Laufzeit für Bereitstellung (Staging), Produktion oder sonstige Zwecke gedacht ist.
5. Implementieren Sie das Basic Runtime- oder Advanced Runtime-Muster. Weitere Informationen finden Sie in „SOA Policy Gateway Advanced Runtime-Muster implementieren" auf Seite 79 bzw. „SOA Policy Gateway Basic Runtime-Muster implementieren" auf Seite 77.
6. Warten Sie ab, bis die Implementierung vollständig abgeschlossen ist, bevor Sie eine weitere Laufzeit implementieren.

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

1. Der SCP-Dateiserver wird nicht weiter benötigt.
2. WSRR und die WebSphere-Sicherheit können über die Standardsicherheitskonfiguration aktualisiert werden. Weitere Informationen finden Sie in „Sicherheitsmanagement" auf Seite 66.
3. Die DataPower-Domäne ist für die Gateway-Konfiguration bereit.

DataPower 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 am unterstützten DataPower-Gerät 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

Kunden benötigen unterschiedliche Sicherheitsstufen zwischen WSRR und DataPower, insbesondere im Bereich von SSL. IBM SOA Policy Gateway Pattern unterstützt drei Stufen von SSL-Kommunikation zwischen den Konfigurationsscripts und DataPower, wenn die Muster für SOA Policy Gateway Basic Runtime, SOA Policy Gateway Basic Runtime Sample und SOA Policy Gateway Advanced Runtime verwendet werden.

Wenn SSL nicht erforderlich ist

Wenn es nicht erforderlich ist, SSL zu verwenden, werden der öffentliche Schlüssel und die privaten Schlüssel für den curl-Client nicht bereitgestellt und als „Unset" angegeben.

Anmerkung: Wenn kein SSL verwendet wird, bleiben alle Daten, die an DataPower gesendet werden, unverschlüsselt. Dies gilt auch für Benutzer- und Kennwortinformationen. Dies stellt eine Sicherheitslücke dar. Für Kennwörter, die in SOMA-Aufrufen an DataPower verwendet werden, wird keine Verschlüsselung unterstützt. Diese werden infolgedessen unverschlüsselt an das DataPower-Gerät übertragen. Verwenden Sie daher mindestens die serverseitige Authentifizierung, um die Sicherheit sicherzustellen.

Gegenseitige Authentifizierung zwischen den DataPower-Anwendungen und den Scripts in den Basic- und Advanced-Mustern

Wenn es erforderlich ist, dass eine gegenseitige Authentifizierung zwischen den DataPower-Anwendungen und den Scripts in den Basic- und Advanced-Mustern erfolgt, gilt Folgendes:

- Der öffentliche Schlüssel und die privaten Schlüssel für den curl-Client müssen angegeben werden.

Sicherheitsmanagement

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

Sicherheitsdatei `DomainZipFile.zip` erstellen

Erstellen Sie die Sicherheitsdatei `DomainZipFile.zip` für das SOA Policy Gateway Basic Runtime-Muster, das SOA Policy Gateway Advanced Runtime-Muster und SOA Policy Gateway Basic Runtime Sample-Muster.

Vorgehensweise

Erstellen Sie die Datei `DomainZipFile.zip` nach den folgenden Regeln:

1. Die Struktur der Datei `DomainZipFile.zip` muss wie folgt aussehen:

   Anmerkung: Nur die Verzeichnisstruktur ist erforderlich, einzelne Dateinamen können einer beliebigen Benennungskonvention entsprechen. Allerdings müssen alle Zertifikats- und Schlüsseldateien das PEM-Format haben.

Anmerkung: Die Verwendung des DataPower-Hostnamens im Pfad ermöglicht die Verwendung verschiedener Zertifikate für verschiedene DataPower-Geräte.

Tabelle 31. Für die Basic- und Advanced-Muster erforderliche Dateien

Dateiname, Position relativ zum Stammverzeichnis	Anmerkungen
`CurlClientPublicKeyFile.crt`	Nur erforderlich, wenn die gegenseitige Authentifizierung verwendet wird. Nur PEM-Format.
`CurlClientPrivateKeyFile.key`	Nur erforderlich, wenn die gegenseitige Authentifizierung verwendet wird.
`/dataPowerHostName/certificate1.crt`	Die DataPower-Zertifikate, die in WSRR hochzuladen sind. Es ist erforderlich, dass die gesamte Zertifikatskette das PEM-Format hat. Die Datei darf nur die DataPower-Zertifikate zwischen den folgenden Zeilen enthalten: `------BEGINCERTIFICATE---- bis -----END CERTIFICATE-----` Die Dateierweiterung muss `.crt` oder `.pem` sein.
`/dataPowerHostName/certificate2.crt`	Die Dateierweiterung muss `.crt` oder `.pem` sein.
`/dataPowerHostName/certificate3.crt`	Die Dateierweiterung muss `.crt` oder `.pem` sein.

2. Nur für das SOA Policy Gateway Advanced Runtime-Muster: Fügen Sie die auszuführende Datei `cli` hinzu (optional):

Tabelle 32. Zusätzliche, für das Advanced-Muster erforderliche Dateien

Dateiname, Position relativ zum Stammverzeichnis	Anmerkungen
`/cli.cli`	Eine einzelne CLI-Datei, die am Ende der DataPower-Domänenkonfiguration ausgeführt wird.

3. Speichern Sie die Datei `DomainZipFile.zip` an Ihrer SCP-Serverposition. Aufgrund des sensiblen Inhalts dieser Datei wird empfohlen, diese Datei nach der Konfiguration wieder zu löschen. Die Musterkonfigurationsscripts löschen alle Dateien, die aus der Datei `DomainZipFile.zip` abgerufen wurden, sowie die Kopie der Datei `DomainZipFile.zip`, die über SCP in Ihrer SCP-Umgebung erstellt wird.
4. Notieren Sie sich die folgenden Informationen zum SCP-Server:
   - Den SCP-Hostnamen
   - Den SCP-Pfad zur Datei `DomainZipFile.zip`
   - Den SCP-Benutzer und das zugehörige Kennwort

Datei `DomainZipFile` verwenden

Nachfolgend werden Anwendungsfälle für die Datei `DomainZipFile` für verschiedene Sicherheitsstufen in Mustern beschrieben.

Die Datei `DomainZipFile.zip` kann im Basic Runtime-, Basic Runtime Sample- und Advanced Runtime-Muster verwendet werden.

Für die Herstellung der Verbindung der Musterscriptpakete zum DataPower-Gerät ist SSL nicht erforderlich. Wenn Sie SSL nicht verwenden, brauchen Sie keine Datei `DomainZipFile.zip` zu erstellen, sofern Sie kein CLI-Script benötigen, um die durch das Muster erstellte DataPower-Domäne anzupassen. In diesem Fall werden die Daten nicht verschlüsselt, wenn Sie nicht mindestens die Serverauthentifizierung verwenden. Dies stellt ein Sicherheitsrisiko dar, da Benutzer- und Kennwortinformationen während der Kommunikation mit dem Scripting-Client

über eine HTTP-Verbindung an DataPower übertragen werden und diese Übertragung ansonsten durch die Zertifikate in der Datei `DomainZipFile.zip` geschützt wird.

Wenn der DataPower-Host nicht so konfiguriert ist, dass er das Clientzertifikat überprüft, müssen Sie die gegenseitige Authentifizierung zwischen dem Scripting-Client und dem DataPower-Gerät nicht verwenden. Es wird empfohlen, mindestens die Serverauthentifizierung zu verwenden.

Die Fallszenarios in diesem Abschnitt beschreiben unterschiedliche Sicherheitsstufen.

Das Produkt unterstützt die folgenden Fallszenarios:

Fall 1: SSL ist nicht erforderlich

Fall 2: SSL ist nicht erforderlich, jedoch wird das CLI-Script zur Anpassung der Domäne benötigt

Fall 3: Serverauthentifizierung des DataPower-Zertifikats durch den Scripting-Client ist erforderlich

Fall 4: Gegenseitige Authentifizierung mit dem DataPower-Gerät ist erforderlich

Fall 1: SSL ist nicht erforderlich

Aus den erwähnten Sicherheitsgründen wird empfohlen, diese Option nur für Entwicklungsszenarios zu verwenden. Wenn Sie SSL nicht verwenden wollen, gehen Sie wie folgt vor:

1. Setzen Sie den Parameter für 'SCP_host' auf den Wert „Unset". Wenn Sie das Basic Runtime- oder Advanced Runtime-Muster verwenden, ist dies der Parameter 'SCP_host' im Script des Pakets 'SOA Policy Gateway 2.0.0.0 - Security'. Wenn Sie das Basic Runtime Sample-Muster verwenden, ist dies der Parameter 'SCP_host' im Script des Pakets 'SOA Policy Gateway 2.0.0.0'. Dadurch wird das Script im betreffenden Muster so eingestellt, dass es die Datei `DomainZipFile.zip` über SCP nicht abruft.
2. Setzen Sie die folgenden Parameter in denselben Scriptpaketen wie in Schritt 1 auf den Wert „Unset":
   - CLIENT_PUBLIC_KEY_file
   - CLIENT_PUBLIC_KEY_password
   - Kennwort überprüfen (Verify password)
   - CLIENT_PRIVATE_KEY_file
   - CLIENT_PRIVATE_KEY_password
   - Kennwort überprüfen (Verify password)

Fall 2: SSL ist nicht erforderlich, jedoch wird das CLI-Script zur Anpassung der Domäne benötigt

Aus den erwähnten Sicherheitsgründen wird empfohlen, diese Option nur für Entwicklungsszenarios zu verwenden. Gehen Sie wie folgt vor, wenn SSL nicht verwendet werden soll, jedoch ein CLI-Script erforderlich ist:

1. Setzen Sie den Parameter für 'SCP_host' auf den Wert „Unset". Wenn Sie das Basic Runtime- oder Advanced Runtime-Muster verwenden, ist dies der Parameter 'SCP_host' im Script des Pakets 'SOA Policy Gateway 2.0.0.0 - Security'. Wenn Sie das Basic Runtime Sample-Muster verwenden, ist dies der Parameter 'SCP_host' im Script des Pakets 'SOA Policy Gateway 2.0.0.0'.

Dadurch wird das Script im betreffenden Muster so eingestellt, dass es die Datei `DomainZipFile.zip` über SCP nicht abruft.

2. Setzen Sie die folgenden Parameter in denselben Scriptpaketen wie in Schritt 1 auf den Wert Unset:
   - CLIENT_PUBLIC_KEY_file
   - CLIENT_PUBLIC_KEY_password
   - Kennwort überprüfen (Verify password)
   - CLIENT_PRIVATE_KEY_file
   - CLIENT_PRIVATE_KEY_password
   - Kennwort überprüfen (Verify password)

   Anmerkung: Wenn der Parameter 'SCP_host' den Wert „Unset" hat, ist eine Datei `DomainZipFile.zip` nur erforderlich, wenn Sie ein CLI-Script haben, das Sie im Basic Runtime- bzw. Advanced Runtime-Muster ausführen möchten.
3. Stellen Sie die CLI-Scriptdatei, die Sie verwenden wollen, in das Stammverzeichnis der Datei `DomainZipFile.zip`. Ein Beispiel für die Struktur der Datei `DomainZipFile.zip` sieht wie folgt aus:

   ```
   /cli.cli
   ```

   Diese Datei wird am Ende des DataPower Domain-Scriptpakets ausgeführt. Der Name `cli.cli` ist ein Beispieldateiname. Der Dateiname darf keine Leerzeichen enthalten.

Fall 3: Serverauthentifizierung des DataPower-Zertifikats durch den Scripting-Client ist erforderlich

Sie müssen alle Zertifikate der DataPower-Zertifikatskette bereitstellen, durch die die XML-Managementschnittstelle (XML Management Interface) geschützt wird. Führen Sie die folgenden Schritte aus, um diese Zertifikate zu finden:

1. Suchen Sie im SSL-Proxy-Profil nach 'XML Management Interface' und suchen Sie das Kryptoprofil (CryptoProfile). Das Kryptoprofil enthält die Berechtigungsnachweise zur Identifikation, die die Zertifikate enthalten, die zum Schutz der XML-Managementschnittstelle verwendet werden.
2. Fügen Sie diese Zertifikate der Datei `DomainZipFile.zip` hinzu.

   Das Format sieht wie folgt aus:
   - dataPowerHostName/certificateChainMember1.crt
   - dataPowerHostName/certificateChainMember2.pem
   - dataPowerHostName/certificateChainMember(n).crt

   Wenn Sie das Szenario mit mehreren Domänen verwenden, kann die Datei zwei verschiedene Verzeichnisse `dataPowerHostName` enthalten, die jeweils die folgenden Dateien für die DataPower-Zertifikatskette enthalten:
   - clientCertificate.crt clientKeyFile.key
   - dataPowerHostName/certificateChainMember1.crt
   - dataPowerHostName/certificateChainMember2.pem
   - dataPowerHostName/certificateChainMember(n).crt
   - dataPowerHostName2/certificateChainMember1a.crt
   - dataPowerHostName2/certificateChainMember2a.pem
   - dataPowerHostName2/certificateChainMember2(n).crt

   Anmerkung: Die DataPower-Zertifikatskettendateien müssen den Typ `.crt` oder `.pem` haben und dürfen nur das Zertifikat selbst enthalten. Die hier

verwendeten Namen der .crt- oder .pem-Dateien sind Beispiele. Der Dateiname darf keine Leerzeichen enthalten.

3. Optional: Wenn Sie nur die Serverauthentifizierung für das Script aus dem Paket 'SOA Policy Gateway 2.0.0.0 - Security', das von dem Basic Runtime- und dem Advanced Runtime-Muster verwendet wird, oder nur das Script 'SOA Policy Gateway 2.0.0.0 - Sample' im Basic Runtime Sample-Muster benötigen, verwenden Sie „Unset" als Wert für die folgenden Parameter in diesen Scripts:
   - CLIENT_PUBLIC_KEY_file
   - CLIENT_PUBLIC_KEY_password
   - Kennwort überprüfen (Verify password)
   - CLIENT_PRIVATE_KEY_file
   - CLIENT_PRIVATE_KEY_password
   - Kennwort überprüfen (Verify password)
4. Optional: Wenn ein CLI-Script erforderlich ist:

   Stellen Sie die CLI-Scriptdatei, die Sie verwenden wollen, in das Stammverzeichnis der Datei DomainZipFile.zip. Ein Beispiel für die Struktur der Datei DomainZipFile.zip sieht wie folgt aus:

   ```
   /cli.cli
   ```

   Diese Datei wird am Ende des DataPower Domain-Scriptpakets ausgeführt. Der Name cli.cli ist ein Beispieldateiname. Der Dateiname darf keine Leerzeichen enthalten.

Fall 4: Gegenseitige Authentifizierung mit dem DataPower-Gerät ist erforderlich

In diesem Fall erfordern der Client und der DataPower-Server eine Überprüfung der Zertifikate des jeweils anderen. Dies ist nur erforderlich, wenn der DataPower-Host im SSL-Proxy-Profil für die XML-Managementschnittstelle (XML Management Interface) zur Überprüfung der Zertifikate des Clients konfiguriert ist.

1. Fügen Sie diese Zertifikate der Datei DomainZipFile.zip hinzu.

   Das Format sieht wie folgt aus:
   - clientCertificate.crt
   - clientKeyFile.key
   - dataPowerHostName/certificateChainMember1.crt
   - dataPowerHostName/certificateChainMember2.pem
   - dataPowerHostName/certificateChainMember(n).crt
   - dataPowerHostName2/certificateChainMember1a.crt
   - dataPowerHostName2/certificateChainMember2a.pem
   - dataPowerHostName2/certificateChainMember2(n).crt

   Anmerkung: Die DataPower-Zertifikatskettendateien müssen den Typ .crt oder .pem haben und dürfen nur das Zertifikat selbst enthalten. Die hier verwendeten Namen der .crt- oder .pem-Dateien sind Beispiele. Der Dateiname darf keine Leerzeichen enthalten.

   Die Clientzertifikatdatei und die Clientschlüsseldatei können die Daten in der Zertifikats- bzw. Schlüsseldatei vor der Zeile enthalten, die wie folgt aussieht: -----BEGIN CERTIFICATE-----.
2. Optional: Wenn Sie die Serverauthentifizierung für das Script aus dem Paket 'SOA Policy Gateway 2.0.0.0 - Security', das von dem Basic Runtime- und dem Advanced Runtime-Muster verwendet wird, oder das Script 'SOA Policy

Gateway 2.0.0.0 - Sample' im Basic Runtime Sample-Muster benötigen, verwenden Sie „Unset" als Wert für die folgenden Parameter in diesen Scripts:

- CLIENT_PUBLIC_KEY_file
- CLIENT_PRIVATE_KEY_file
- CLIENT_PRIVATE_KEY_password
- Kennwort überprüfen (Verify password)

3. Wenn kein Kennwort für die Datei mit dem öffentlichen Schlüssel vorhanden ist, kann der Wert für die folgenden Parameter „Unset" sein:
   - CLIENT_PUBLIC_KEY_password
   - Kennwort überprüfen (Verify password)
4. Die curl-Befehle, die von den Scriptpaketen verwendet werden, gehen von der Annahme aus, dass der Dateityp `.pem` ist, sodass die Parameter **--key-type** und **--cert-type** standardmäßig auf PEM eingestellt sind. Die Zertifikats- und Schlüsseldateien können diesen Inhalt vor `-----BEGIN CERTIFICATE-----` in der jeweiligen Zertifikats- bzw. Schlüsseldatei enthalten.
5. Optional: Wenn ein CLI-Script bei Verwendung des Basic Runtime- oder Advanced Runtime-Musters erforderlich ist:

   Stellen Sie die CLI-Scriptdatei, die Sie verwenden wollen, in das Stammverzeichnis der Datei `DomainZipFile.zip`. Ein Beispiel für die Struktur der Datei `DomainZipFile.zip` sieht wie folgt aus:

   ```
   /cli.cli
   ```

   Diese Datei wird am Ende des DataPower Domain-Scriptpakets ausgeführt. Der Name `cli.cli` ist ein Beispieldateiname. Der Dateiname darf keine Leerzeichen enthalten.

Durch die Auswahl eines Falls haben Sie die entsprechende Sicherheitsstufe mit oder ohne Verwendung der Datei `DomainZipFile.zip` konfiguriert.

DataPower-Zertifikate zum Hochladen in WSRR

Sie können ein Verzeichnis von Zertifikaten im Verzeichnis `dataPowerHostName` der Datei `DomainZipFile.zip` bereitstellen. Dieses kann auf den WSRR-Dmgr-Server oder auf den eigenständigen WSRR-Server hochgeladen werden.

Eigenen Mechanismus zum Herunterladen der Datei `DomainZipFile.zip` bereitstellen

Sie können eine eigene Datei `DomainZipFile.zip` bereitstellen, ohne den SCP-Server im Sicherheitsscriptpaket (Security Script Package) zu verwenden.

Vorgehensweise

Sie müssen die folgenden Schritte ausführen, um andere Methoden zur Bereitstellung der Datei in Ihrer Umgebung zu verwenden:

1. Der Parameter **`SCP_host`** muss auf den Wert 'Unset' (nicht festgelegt) gesetzt werden.
2. Sie müssen ein angepasstes Scriptpaket erstellen, um die Datei `DomainZipFile.zip` im Verzeichnis `/tmp` zu erstellen, bevor Sie eines der Scripts für SOA-Gateway-Muster ausführen.
3. Für Advanced-Muster erstellen Sie die Datei `DomainZipFile.zip` im Verzeichnis `/tmp/security/RetrieveDomainFiles`.
4. Für Basic-Muster mit Sample erstellen Sie die Datei `DomainZipFile.zip` im Verzeichnis `/installSample/Retrieve_Domain_Files`.

Anmerkung: Wenn die Datei `DomainZipFile.zip` nicht vorhanden ist, schlägt die Ausführung des Scripts möglicherweise fehl, wenn die Parameter angeben, dass Zertifikate oder Schlüssel verwendet werden.

CN-Werte in Zertifikaten

Die Zertifikate, die als Teil der Datei `DomainZipFile.zip` bereitgestellt werden, müssen den CN-Wert im Zertifikat berücksichtigen.

Die Hostnamensprüfung ist immer aktiv, wenn Sie die Verwendung von SSL auswählen. Daher müssen Sie die folgenden Punkte berücksichtigen, wenn das Zertifikat im Scriptpaket verwendet wird:

- Für Clientzertifikate (öffentlicher und privater Schlüssel) gibt es keine Möglichkeit, den genauen Host zu kennen, auf dem sich der WSRR-Server oder der WSRR-Dmgr-Server befinden wird, der das Script ausführt. Daher muss der CN-Wert generisch genug sein, um auf einem beliebigen potenziellen Client-Host in der IBM Workload Deployer-Umgebung ausführbar zu sein. Beispiel: `*clientname*.ihrunternehmen.com`.
- Die Zertifikate für die DataPower-Maschinen befinden sich in einzelnen Verzeichnissen in der Datei `DomainZipFile.zip`. Beispiele:

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

- Der CN-Wert für das Zertifikat (im Endzertifikat in der Kette für den DataPower-Host) muss für den betreffenden Hostnamen gültig sein. Beispiel: `dp1.ihrunternehmen.com` oder `*dp*.ihrunternehmen.com`.

LDAP für das Beispiel konfigurieren

Für das Beispiel ist Lightweight Directory Access Protocol (LDAP) mit einigen speziellen Einträgen erforderlich.

Informationen zu diesem Vorgang

Die Elemente und Eigenschaften müssen bei der Konfiguration von LDAP definiert werden.

Anmerkung: Ändern Sie diese Kennwörter nicht.

Alternativ zu den manuellen Konfigurationsschritten können Sie den Inhalt der folgenden `.zip`-Datei extrahieren, die zwei LDIF-Dateien mit den Konfigurationsdetails enthält, die in dieser Task bereitgestellt werden, und diese Dateien zum Aktualisieren des LDAP-Servers verwenden: soaSamples.zip.

Vorgehensweise

Erstellen Sie ein LDAP mit den folgenden Elementen:

1. Definieren Sie das Suffix:

```
dc=ibm.com
```

2. Definieren Sie die Domäne `dc=ibm.com` mit den folgenden Eigenschaften:

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

3. Definieren Sie die Container:
   a. Definieren Sie die Containergruppen:

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

b. Definieren Sie die Containerbenutzer:

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

4. Definieren Sie die folgenden Benutzer:
   a. Benutzer 'ConsumerA' mit den folgenden Eigenschaften:

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

   b. Benutzer 'ConsumerB' mit den folgenden Eigenschaften:

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

   c. Benutzer 'ConsumerX' mit den folgenden Eigenschaften:

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

5. Definieren Sie die folgenden Gruppen:
   a. Definieren Sie die Gruppe MANAGER mit den folgenden Eigenschaften:

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

   b. Definieren Sie die Gruppe 'Clerk' mit den folgenden Eigenschaften:

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

   c. Definieren Sie die Gruppe 'Customer' mit den folgenden Eigenschaften:

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

6. Stellen Sie sicher, dass Sie die folgenden Informationen zum LDAP vor der Ausführung des Beispiels sammeln:
   - Den definierten Name (DN). Beispiel: `cn=root`.
   - Das Kennwort. Beispiel: `passw0rd`.
   - Den nicht sicheren Port. Beispiel: 389.
   - Den LDAP-Hostnamen. Beispiel: `ldap.customer.com`.

Muster implementieren

Durch die Implementierung von Mustern mit IBM Workload Deployer 3.1.0.2 oder IBM SOA Policy Gateway Pattern in der Cloud wird eine aktive IBM PureApplication System-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.

Informationen zu diesem Vorgang

Durch die Implementierung eines Musters wird ein virtuelles System bzw. eine neu bereitgestellte Laufzeitumgebung für IBM SOA Policy Gateway Pattern erstellt, das bzw. die in der Cloud ausgeführt wird.

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 Workload Deployer: Virtuelle Systemmuster verwalten

IBM PureApplication System: Virtuelle Systemmuster verwalten

SOA Policy Gateway Basic Runtime Sample-Muster implementieren

Durch die Implementierung des SOA Policy Gateway Basic Runtime Sample-Musters wird eine aktive virtuelle Systeminstanz des Musters erstellt.

Vorbereitende Schritte

Die folgenden Voraussetzungen müssen vor der Implementierung des Musters erfüllt werden:

- Konfigurieren Sie DataPower für das Muster (siehe „DataPower für IBM SOA Policy Gateway Pattern konfigurieren" auf Seite 65).
- Konfigurieren Sie die Sicherheit für das Muster (siehe „Sicherheit für die IBM SOA Policy Gateway Pattern-Muster" auf Seite 65).
- Konfigurieren Sie den SCP-Server als Host für die Bereitstellung der Sicherheitsdateien.
- Konfigurieren Sie den LDAP-Server für das Muster (siehe „LDAP für das Beispiel konfigurieren" auf Seite 72).

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 auf **Patterns** > **Virtual Systems**.
2. Wählen Sie in der Liste 'Virtual System Patterns' den Eintrag **SOA Policy Gateway 2.0.0.0 - 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. Konfigurieren Sie die virtuellen Muster. Klicken Sie auf **Configure virtual parts** und anschließend auf den Namen des Teils, um den Editor für die Teile und das Script zu öffnen:

Anmerkung: Für alle Kennwörter in diesem Muster wird mit Ausnahme des Parameters 'DataPower_admin_id' der Standardwert `password` verwendet.

- „Konfigurationsparameter des DB2 Enterprise-Teils für das SOA Policy Gateway Basic Runtime Sample-Muster" auf Seite 30.
- „Konfigurationsparameter des Teils für den eigenständigen WSRR-Server für das SOA Policy Gateway Basic Runtime Sample-Muster" auf Seite 42
- „SOA Policy Gateway 2.0.0.0 - Konfigurationsparameter des Sample-Scripts für das SOA Policy Gateway Basic Runtime Sample-Muster" auf Seite 55

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

Nächste Schritte

Informationen zur Überprüfung der Implementierung finden Sie in „Implementierung überprüfen" auf Seite 80.

SOA Policy Gateway Governance Master-Muster implementieren

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

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 Governance Master-Muster zu implementieren:

1. Klicken Sie auf **Patterns** > **Virtual Systems**.
2. Wählen Sie in der Liste 'Virtual System Patterns' den Eintrag **SOA Policy Gateway 2.0.0.0 - Governance Master** 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. Konfigurieren Sie die virtuellen Muster. Klicken Sie auf **Configure virtual parts** und anschließend auf den Namen des Teils, um den Editor für den Teil zu öffnen.
      - „Konfigurationsparameter des Teils für die DB2 Enterprise-HADR-Primärdatenbank für das SOA Policy Gateway Governance Master-Muster" auf Seite 35
      - „Konfigurationsparameter des WSRR-Deployment Manager-Teils für das SOA Policy Gateway Governance Master-Muster" auf Seite 45
      - „Konfigurationsparameter des Teils für angepasste WSRR-Knoten für das SOA Policy Gateway Governance Master-Muster" auf Seite 48

- „Konfigurationsparameter des Teils für die DB2 Enterprise-HADR-Bereitschaftsdatenbank für das SOA Policy Gateway Governance Master-Muster" auf Seite 39

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

Nächste Schritte

Informationen zur Überprüfung der Implementierung finden Sie in „Implementierung überprüfen" auf Seite 80.

Implementierungsinformationen zum SOA Policy Gateway Governance Master

Der Governance Master muss vor der Implementierung des SOA Policy Gateway Basic Runtime-Musters oder des SOA Policy Gateway Advanced Runtime-Musters 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. Notieren Sie die folgenden Informationen:
   - 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**.

   Anmerkung: 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 SOA Policy Gateway Basic Runtime-Muster bzw. im SOA Policy Gateway Advanced Runtime-Muster:
   - WSRR_GOV_DMGR_hostname
   - WSRR_GOV_DMGR_cellname
   - WSRR_GOV_admin_user
   - WSRR_GOV_admin_password

SOA Policy Gateway Basic Runtime-Muster implementieren

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

Vorbereitende Schritte

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

- Konfigurieren Sie DataPower für IBM SOA Policy Gateway Pattern (siehe „DataPower für IBM SOA Policy Gateway Pattern konfigurieren" auf Seite 65).
- Konfigurieren Sie die Sicherheit für IBM SOA Policy Gateway Pattern (siehe „Sicherheit für die IBM SOA Policy Gateway Pattern-Muster" auf Seite 65).
- Konfigurieren Sie den SCP-Server als Host für die Bereitstellung der Sicherheitsdateien.
- Stellen Sie die Implementierungsinformationen zum Governance Master zusammen (siehe „Implementierungsinformationen zum SOA Policy Gateway Governance Master" auf Seite 77).

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 im SOA Policy Gateway Basic Runtime-Muster oder SOA Policy Gateway Advanced Runtime-Muster implementieren. Dies 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 das SOA Policy Gateway 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 Basic Runtime 2.0.0.0** 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. 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:
      - „Konfigurationsparameter des DB2 Enterprise-Teils für das SOA Policy Gateway Basic Runtime-Muster" auf Seite 28
      - „Konfigurationsparameter des Teils für den eigenständigen WSRR-Server für das SOA Policy Gateway Basic Runtime-Muster" auf Seite 42
      - „SOA Policy Gateway 2.0.0.0 - Konfigurationsparameter des Security-Scripts für das SOA Policy Gateway Basic Runtime-Muster" auf Seite 59
      - „SOA Policy Gateway 2.0.0.0 - Konfigurationsparameter des Promotion-Scripts für das SOA Policy Gateway Basic Runtime-Muster" auf Seite 52

- „SOA Policy Gateway 2.0.0.0 - Konfigurationsparameter des DataPower Domain-Scripts für das SOA Policy Gateway Basic Runtime-Muster" auf Seite 50

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

Nächste Schritte

Informationen zur Überprüfung der Implementierung finden Sie in „Implementierung überprüfen" auf Seite 80.

SOA Policy Gateway Advanced Runtime-Muster implementieren

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

Vorbereitende Schritte

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

- Konfigurieren Sie DataPower für IBM SOA Policy Gateway Pattern (siehe „DataPower für IBM SOA Policy Gateway Pattern konfigurieren" auf Seite 65).
- Konfigurieren Sie die Sicherheit für IBM SOA Policy Gateway Pattern (siehe „Sicherheit für die IBM SOA Policy Gateway Pattern-Muster" auf Seite 65).
- Konfigurieren Sie den SCP-Server als Host für die Bereitstellung der Sicherheitsdateien.
- Stellen Sie die Implementierungsinformationen zum Governance Master zusammen (siehe „Implementierungsinformationen zum SOA Policy Gateway Governance Master" auf Seite 77).

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 im SOA Policy Gateway Basic Runtime-Muster oder SOA Policy Gateway Advanced Runtime-Muster implementieren. Dies 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 das SOA Policy Gateway 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 2.0.0.0 - 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. Optional: Wählen Sie die Umgebung und den Zeitplan für die Implementierung aus.
   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:
      - „Konfigurationsparameter des Teils für die DB2 Enterprise-HADR-Primärdatenbank für das SOA Policy Gateway Advanced Runtime-Muster" auf Seite 33
      - „Konfigurationsparameter des WSRR-Deployment Manager-Teils für das SOA Policy Gateway Advanced Runtime-Muster" auf Seite 44
      - „SOA Policy Gateway 2.0.0.0 - Konfigurationsparameter des Security-Scripts für das SOA Policy Gateway Advanced Runtime-Muster" auf Seite 60
      - „SOA Policy Gateway 2.0.0.0 - Konfigurationsparameter des Promotion-Scripts für das SOA Policy Gateway Advanced Runtime-Muster" auf Seite 53
      - „SOA Policy Gateway 2.0.0.0 - Konfigurationsparameter des DataPower Domain-Scripts für das SOA Policy Gateway Advanced Runtime-Muster" auf Seite 51
      - „Konfigurationsparameter des Teils für angepasste WSRR-Knoten für das SOA Policy Gateway Advanced Runtime-Muster" auf Seite 47
      - „Konfigurationsparameter des Teils für die DB2 Enterprise-HADR-Bereitschaftsdatenbank für das SOA Policy Gateway Advanced Runtime-Muster" auf Seite 38
5. Klicken Sie auf **OK**, um die Implementierung auszuführen.

Nächste Schritte

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

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 129.
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 85.

Szenario: Zusätzliche Laufzeit dem Muster 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. Dies bedeutet, dass Zustände (Status) und Übergänge vorhanden sind, die für die Bereitstellungs- und die Produktionsumgebung spezifisch sind, sodass eine kontrollierte Umstufung (Promotion) in diese Laufzeiten durch Definieren der Zielsysteme in der Promotionskonfigurationsdatei ermöglicht wird. Dies 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 zusätzliche 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 63.

Vorgehensweise

1. Implementieren Sie den SOA Policy Gateway Governance Master. Weitere Informationen finden Sie in „SOA Policy Gateway Governance Master-Muster implementieren" auf Seite 76.
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 das SOA Policy Gateway Basic Runtime-Muster bzw. das SOA Policy Gateway Advanced Runtime-Muster mit den Governance Master-Details. Weitere Informationen finden Sie in „Implementierungsinformationen zum SOA Policy Gateway Governance Master" auf Seite 77.

   Anmerkung: Der Wert für die Umstufungsumgebung (Promotionsumgebung) muss auf „Unset" gesetzt werden.
4. Implementieren Sie das vordefinierte SOA Policy Gateway Basic Runtime- oder SOA Policy Gateway Advanced Runtime-Muster. Weitere Informationen finden Sie in „SOA Policy Gateway Basic Runtime-Muster implementieren" auf Seite 77 und „SOA Policy Gateway Advanced Runtime-Muster implementieren" auf Seite 79.

IBM SOA Policy Gateway Pattern klonen und anpassen

IBM SOA Policy Gateway Pattern kann nicht bearbeitet werden. Wenn die Topologie, die in den Mustern für virtuelle Systeme von IBM SOA Policy Gateway Pattern nicht die erforderliche Funktion bereitstellen, kann das Muster geklont und anschließend bearbeitet werden, um neue Muster zu erstellen.

Informationen zu diesem Vorgang

Sie können die Muster auf folgende Weisen anpassen:

- Zusätzliche DataPower-Domänen hinzufügen. Weitere Informationen finden Sie in „Mit mehreren DataPower-Domänen implementieren".
- Standardclustergröße erhöhen. Weitere Informationen finden Sie im Information Center von IBM Workload Deployer Version 3.1.

  Anmerkung: Wenn Sie die Clustergröße erhöhen, erhöhen auch Sie die Speicherkapazität für den WSRR-Deployment Manager.
- Methode zum Abrufen der komprimierten Sicherheitsdatei auf dem Server auswählen. Weitere Informationen finden Sie in „Sicherheitsmanagement" auf Seite 66.
- Eigene Standardwerte definieren und sperren (z. B. die DataPower-Administrator-ID). Weitere Informationen zum Sperren von Parametern finden Sie im Information Center von IBM Workload Deployer Version 3.1.
- Eigenen Mechanismus zum Herunterladen der Datei `DomainZipFile.zip` verwenden. Weitere Informationen finden Sie in „Eigenen Mechanismus zum Herunterladen der Datei `DomainZipFile.zip` bereitstellen" auf Seite 71.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um die Muster zu klonen und zu bearbeiten und neue Muster zu erstellen:

1. Wählen Sie im linken Teilfenster des Fensters 'Pattern' das zu klonende Muster aus.
2. Klicken Sie auf das Symbol zum Klonen ('Clone') und geben Sie einen Namen für das neue Muster an. Sie können auch zusätzliche Informationen, zum Beispiel eine Beschreibung, angeben.
3. Wählen Sie das neue Muster aus und klicken Sie auf das Symbol zum Bearbeiten ('Edit'), um die Konfiguration zu ändern. Sie können Teile hinzufügen und entfernen, Teile konfigurieren, die Anzahl einiger Teile erhöhen oder verringern oder die Reihenfolge ändern, in der einige Teile implementiert werden.

Nächste Schritte

Stellen Sie sicher, dass alle erforderlichen Teile für den Typ von Muster, das Sie erstellt haben, ordnungsgemäß konfiguriert sind. Sie können das Muster implementieren, wenn Ihre Konfiguration abgeschlossen ist.

Zugehörige Informationen:

IBM Workload Deployer: Virtuelle Systemmuster verwalten

IBM PureApplication System: Virtuelle Systemmuster verwalten

Mit mehreren DataPower-Domänen implementieren

Das SOA Policy Gateway Basic Runtime-Muster und das SOA Policy Gateway Advanced Runtime-Muster können geklont und angepasst werden, um mehrere DataPower-Domänen einzubeziehen.

Vorgehensweise

1. Klonen Sie das SOA Policy Gateway Basic Runtime-Muster oder das SOA Policy Gateway Advanced Runtime-Muster. Weitere Informationen finden Sie in „IBM SOA Policy Gateway Pattern klonen und anpassen" auf Seite 81.
2. Zum Bearbeiten des Musters klicken Sie auf **Edit**.
3. Erweitern Sie den Abschnitt **Scripts**.
4. Für jede zusätzliche Domäne, die hinzugefügt werden soll, ziehen Sie das Scriptpaket **SOA Policy Gateway 2.0.0.0 DataPower Domain** auf den WSRR-Deployment Manager-Teil des Advanced Runtime-Musters bzw. auf den Teil für den eigenständigen WSRR-Server für das Basic Runtime-Muster.
5. Klicken Sie auf **Done editing**.
6. Implementieren Sie das Muster, indem Sie die folgenden Informationen für jede hinzugefügte Domäne eingeben:
   - DataPower_hostname
   - DataPower_XML_mgmt_port
   - DataPower_admin_id
   - DataPower_admin_password
   - Kennwort überprüfen (Verify password)
   - New_DataPower_domain
   - securityFileCleanUp

   Anmerkung: Bei Verwendung mehrerer Domänen muss für die letzte Domäne der Parameter 'securityFileCleanUp' auf den Wert **`true`** gesetzt werden. Für alle anderen Domänen muss der Parameter auf den Wert **`false`** gesetzt werden.

   Weitere Informationen zur Implementierung von Mustern finden Sie in „SOA Policy Gateway Basic Runtime-Muster implementieren" auf Seite 77 oder „SOA Policy Gateway Advanced Runtime-Muster implementieren" auf Seite 79.

Beispielanwendung

Die Beispielanwendung besteht aus einer konfigurierbaren DataPower-Domäne und einer Gruppe von WSRR-Artefakten, die zur Demonstration der Funktionen des Musters verwendet werden können.

Das Grundszenario in der Beispielanwendung ist eine Anwendung zur Warenbestandsführung für ein Geschäft ('Warehouse'). Es gibt einen Web-Service 'Store', der drei Operationen besitzt:

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

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

- Überprüfung anhand der Datei 'Store.wsdl'. Dies basiert auf der Annahme, dass die DataPower-Validierung inaktiviert ist.
- Zurückweisung, wenn mehr als fünf Nachrichten in 90 Sekunden eingehen. Dies ist ein niedriger Schwellenwert für einfache Demonstrationen.

Die Konsumenten dieses Service haben gegenwärtig zwei Service-Level-Agreements (SLAs): 'Gold SLA' und 'Anonymous SLA'. Wenn der Kundenkontext im HTTP-Header 'Gold' ausweist, werden Kunden unverzüglich an den

alternativen Endpunkt weitergeleitet. Wenn sie anonym sind, was gegenwärtig äquivalent zu 'Nicht Gold' ist, werden sie an den StoreMockService-Endpunkt geleitet, der einen anderen Wert für den Preis des Artikels hat.

Das Szenario führt außerdem eine Autorisierung für die Operation 'findInventory' auf der Basis der Gruppenzugehörigkeit aus. Abb. 5 zeigt den Ablauf der Anwendung, wobei jedes Feld ein anderes DataPower-Gateway darstellt.

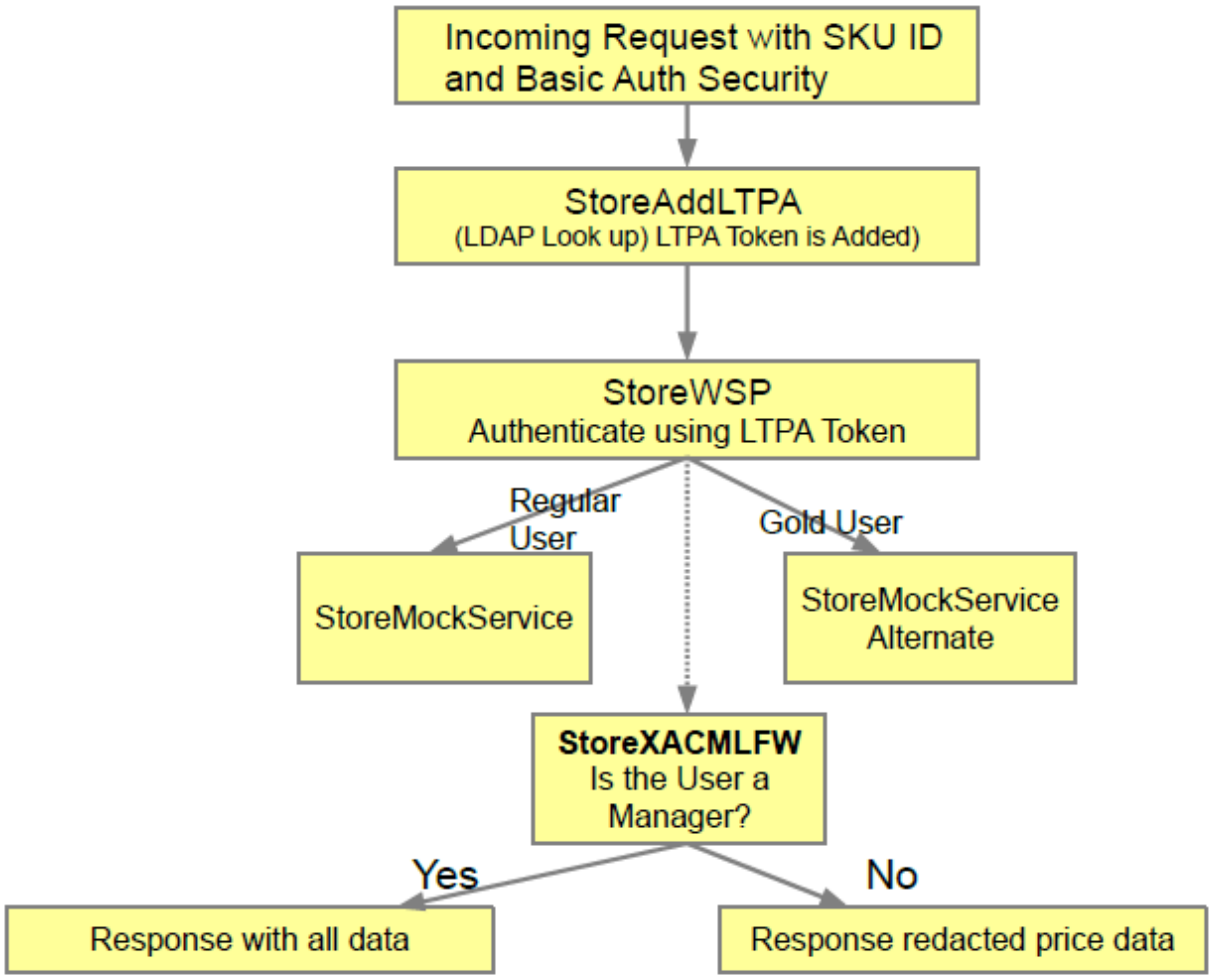


Abbildung 5. Ablaufdiagramm der Beispielanwendung

Zugehörige Tasks:

„IBM SOA Policy Gateway Pattern klonen und anpassen" auf Seite 81
IBM SOA Policy Gateway Pattern kann nicht bearbeitet werden. Wenn die Topologie, die in den Mustern für virtuelle Systeme von IBM SOA Policy Gateway Pattern nicht die erforderliche Funktion bereitstellen, kann das Muster geklont und anschließend bearbeitet werden, um neue Muster zu erstellen.

Übersicht über die WSRR-Artefakte im Beispiel

Die WSRR-Artefakte beschreiben den Warenhausbetrieb.

Es gibt grundlegende Geschäftsfunktionen (Business Capabilities) für das Warenhaus ('Warehouse'), das zur größeren Organisation mit dem Namen 'Bob's Warehouse' gehört. Die Serviceversion Store V1.0 stellt den Geschäftsservice dar. Die Service-Level-Definition 'Store SLD' hat zwei Service-Level-Agreements (SLAs): Das SLA 'Gold SLA' für Gold-Kunden, das diese an einen alternativen, bevorzugten Service weiterleitet, und das SLA 'Anonymous SLA' für anonyme Benutzer, das für alle anderen Benutzer verwendet wird und einfach eine Benachrichtigung in DataPower protokolliert, dass die Anforderung erfolgt ist. Der Service-Level-Definition 'Store SLD' sind außerdem zwei weitere Beispielrichtlinien 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.

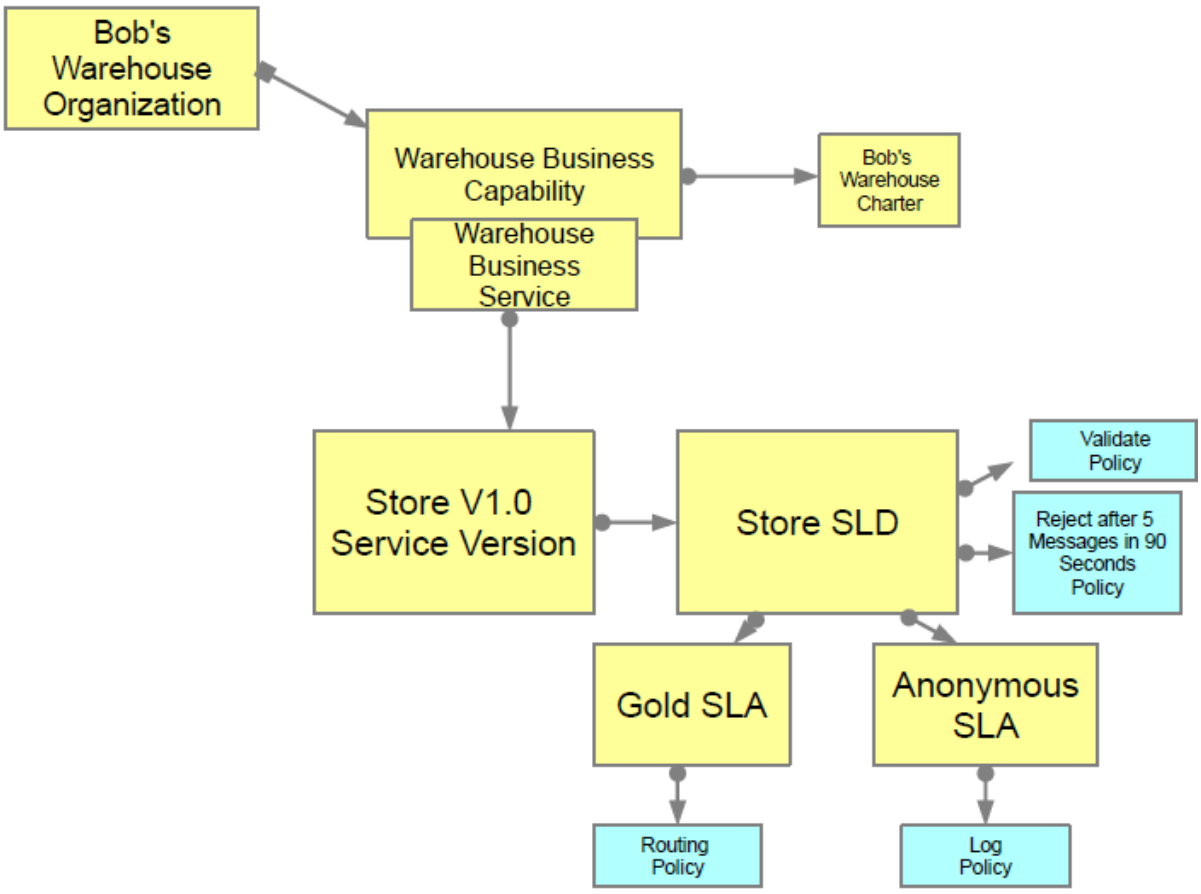


Abbildung 6. Beispieldomäne

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 „SOA Policy Gateway Basic Runtime Sample-Muster implementieren" auf Seite 75.

Anmerkung: Der Wert von `SamplePolicySample_starting_port`, der in den folgenden XML-Beispielen verwendet wird, ist in den Protokollen für SOA Policy Gateway Basic Runtime Sample zu finden.

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. Erweitern Sie dazu 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. Die Testanzeige für die in DataPower implementierte Beispielanwendung wird angezeigt.
4. Die folgenden Optionen sind verfügbar:
   - **Send Standard** - Sendet eine Anforderung 'findInventory' an den Service 'Store'. Die Kontext-ID gibt einen Benutzer der Kategorie „Silver" an. Ein erfolgreiches Ergebnis ist `Part: SKU10 Price: 461.73`.
   - **Send Routed** - Sendet eine Anforderung 'findInventory' an den Service 'Store'. Die Kontext-ID gibt einen Benutzer der Kategorie „Gold" an, sodass die Anforderung an eine Gold-Implementierung des Service geleitet wird. Ein erfolgreiches Ergebnis ist `Part: GOLDSKU10 Price: 461.73`.
   - **Send Invalid** - Sendet eine Anforderung mit ungültigen Nutzdaten. Die Prüfrichtlinie erfordert, dass DataPower die Anforderung überprüft. Ein erfolgreiches Ergebnis ist in diesem Fall eine Antwortnachricht von DataPower: `"Internal Error (from client)"`.
   - **User ID = ConsumerA** - Für Aufrufe mit der Benutzer-ID (UserID) 'ConsumerA' wird die XACML-Richtlinie durchgesetzt, sodass die Preisinformationen nur für Manager zurückgegeben werden. Der Wert von 'Price' in der Antwortnachricht wird überarbeitet. Ein erfolgreiches Ergebnis enthält die Angabe `Price: 0.0`.
   - **Many Standard Requests** - Wenn mehr als fünf Anforderungen innerhalb von 90 Sekunden ausgeführt werden, wird die Zurückweisungsrichtlinie durchgesetzt. Eine erfolgreiche Antwort, die die Durchsetzung der Richtlinie demonstriert, ist: `Rejected: "Rejected (from client)"`.
5. Öffnen Sie die WSRR-Konsole und untersuchen Sie den Service und die Richtlinien. Weitere Informationen finden Sie in .

Gehen Sie wie folgt vor, um die Testfälle für die Beispielanwendung über die Befehlszeile auszuführen:

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 obige Beispiel für das Anforderungs-XML in einer Datei mit dem Namen `silver.xml` enthalten ist, können Sie den folgenden curl-Befehl ausführen:

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

In diesem Beispiel ist ConsumerX ein Manager, sodass die vollständigen Preisinformationen als Antwort zurückgegeben 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. Führen Sie den curl-Befehl aus:

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

Die Kontext-ID ('ContextIdentifier') des SLA wird verwendet, um die Routing-Richtlinie auszulösen. In diesem Fall hat das SLA für Gold-Kunden den Wert „Gold" im SLA. Der Inhalt einer Beispielanforderung mit dem Wert "Gold" im Element 'ContextIdentifier' sieht zum Beispiel wie folgt aus:

```
<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 obige Beispiel für das Anforderungs-XML in einer Datei mit dem Namen `gold.xml` enthalten ist, können Sie den folgenden curl-Befehl ausführen:

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

Jetzt wird die folgende curl-Anforderung ausgeführt:

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

Diese Anforderung generiert den folgenden Fehler:

```
<?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://<ihrDataPowerHostName>.com:<SamplePolicySample_starting_port+4>/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 wie unten gezeigt 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

Falls 'ContextIdentifier' nicht den Wert „Gold" hat, wird kein SLA zugeordnet und das anonyme SLA wird verwendet. Die Mediationsrichtlinie für das anonyme SLA gibt Protokollieren oder Benachrichtigen an. Dies erfordert, dass der Debugmodus für die Sample-Domäne aktiviert wird. Führen Sie den folgenden Befehl aus:

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

In diesem Fall ist ConsumerX ein Manager, sodass die vollständigen Preisinformationen zurückgegeben 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">AFIAAgAkZmExODgzNTQtY2Q1ZC0zYjU0L
WEyMzItZGM3MmEzNWY0MTAzACRmYWVjYjA1Mi1jMWUxLTMyODEtOWY3Ni0wY2IxNm
RhMDc4MjkAAw==</KD4NS:KD4SoapHeaderV2></soapenv:Header><soapenv:Body><b:fin
dInventoryResponse xmlns:a="http://company.ibm.com/"
xmlns:b="http://company.ibm.com/store">
<findInventoryRes>
<sku>SKU10</sku>
<price>461.73</price>
<inventory>460</inventory>
<msrp>923.46</msrp>
```

```
<supplierID>IBM</supplierID>
</findInventoryRes>
</b:findInventoryResponse>
</soapenv:Body>
</soapenv:Envelope>
```

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-a255-9187e20cddb0_05aec6ec-3674-4165-85de-a0f7be48a938'
```

Anmerkung: Die Protokollierung muss auf 'debug' 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 „debug" und klicken Sie auf **Set Log Level** (Protokollierungsstufe festlegen).

Das Protokoll finden Sie, indem Sie **Files** und **File Administration** > **File Management** auswählen. Das Protokoll befindet sich im Ordner `logtemp` und hat den Namen `default-log`. Wegen der zyklischen Wiederverwendung des Protokolls kann es erforderlich sein, die Protokolldatei vor der Ausführung des Tests in einem Web-Browser-Fenster zu öffnen und die Registerkarte im Browser nach der Ausführung des Tests zu aktualisieren.

Zugehörige Tasks:

„SOA Policy Gateway Basic Runtime Sample-Muster implementieren" auf Seite 75
Durch die Implementierung des SOA Policy Gateway Basic Runtime Sample-Musters wird eine aktive virtuelle Systeminstanz des Musters erstellt.

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. Wäre es gewünscht gewesen, den Richtlinienentscheidungspunkt (PDP) in eine andere DataPower-Box zu versetzen, hätte ein SSL-Proxy-Profil erstellt und mit dem url-open-Aufruf verwendet werden können.

```
<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="$incoming_resource" />
</xsl:message>
-->
- <!--
Erstellung der XACML-Anforderung für Maskierung
-->
<xsl:variable name="customized-request">
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
<soapenv:Header />
<soapenv:Body>
<xacml-context:Request xmlns:wsa="http://www.w3.org/2005/08/addressing"
  xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:xacml-context="urn:oasis:names:tc:xacml:2.0:context:schema:os"
  xmlns:ws="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
- <!--
Kopieren in Subjects, die aus der AAA-Anforderungsverarbeitung gespeichert wurden
-->
<xsl:copy-of select="dp:variable('var://context/snip/xacml/xacmlSubjects')/*" />
<xacml-context:Resource>
<xacml-context:ResourceContent>
<xsl:copy-of select="./soap:Envelope/soap:Body" />
</xacml-context:ResourceContent>
<xacml-context:Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#string">
<xacml-context:AttributeValue>PriceInfo</xacml-context:AttributeValue>
</xacml-context:Attribute>
</xacml-context:Resource>
<xacml-context:Action>
<xacml-context:Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
DataType="http://www.w3.org/2001/XMLSchema#string">
<xacml-context:AttributeValue>View</xacml-context:AttributeValue>
</xacml-context:Attribute>
</xacml-context:Action>
<xacml-context:Environment>
<xacml-context:Attribute AttributeId="ContextId" DataType="http://www.w3.org/2001/XMLSchema#string"
Issuer="http://security.tivoli.ibm.com/policy/distribution">
<xacml-context:AttributeValue>StorePriceData</xacml-context:AttributeValue>
</xacml-context:Attribute>
</xacml-context:Environment>
</xacml-context:Request>
</soapenv:Body>
</soapenv:Envelope>
</xsl:variable>
- <!--
Verwenden von 'set-variable', sodass sie im Testmonitor (Probe) sichtbar ist, was nützlich ist.
-->
<dp:set-variable name="'var://context/snip/xacml/BacksideXacmlRequest'" value="$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>
```

Bei der Untersuchung der Datei `sendToPDP.xsl` sind die folgenden Elemente zu beachten:

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 konstruiert eine SOAP-Anforderung:
   - 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.

Sehen Sie sich das Richtlinien-Style-Sheet für die Überarbeitung (Redaktion) an.

StorePrivateDataXACML.xml

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

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

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

Es gibt verschiedene Punkte, an denen Sie die `.xsl`-Scripts ändern können, die in der Anwendung verwendet werden.

Vorgehensweise

Sie haben die folgenden Möglichkeiten, die Beispiel-XSL-Style-Sheets zu ändern:

1. Ändern des Credential-Mappings für AZ.

   Öffnen Sie das Style-Sheet `rgxacml.xsl` und vervollständigen Sie die folgenden XSL-Anweisungen:

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

   Die folgenden Variablen werden im Style-Sheet `soavars.xsl` definiert:

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

Das Beispiel enthält ein unverschlüsseltes Kennwort für den LDAP-Server. Es kann wünschenswert sein, das bereitgestellte Style-Sheet in der Weise anzupassen, dass das unverschlüsselte Kennwort verschlüsselt wird.

```
<!-- Angabe des Basis-DN für den Beginn der Suche -->
<xsl:variable name="baseDN">dc=ibm.com</xsl:variable>
```

Der Wert für `baseDN` ist mit `dc=ibm.com` fest codiert. Wenn Sie Ihr LDAP mit einem anderen Suffix (baseDN) konfiguriert haben, ändern Sie diese Zeile, um das Beispiel anzupassen.

2. Ändern Sie das Überarbeitungs-Style-Sheet (Redaktion).

   Das Style-Sheet `noPriceInfo.xsl` enthält den folgenden Code, durch den alle Werte für den Preis mit Nullen überschrieben 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.

Richtliniendokumente bearbeiten

Verwenden Sie die Business Space-Benutzerschnittstelle zur Bearbeitung von Richtliniendokumenten.

Vorbereitende Schritte

Konfigurieren Sie den SOA-Governance-Space. Weitere Informationen finden Sie in „Business Space für die Erstverwendung konfigurieren” auf Seite 110.

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 Richtlinien erstellen” auf Seite 124.
2. Klicken Sie auf **Finish**. Die Sicht 'Browse' wird angezeigt.
3. Legen Sie Governance-Regeln für die Richtlinie fest. Weitere Informationen zur Governance eines Richtliniendokuments finden Sie in „Lebenszyklus der Richtlinie verwalten” auf Seite 126.
   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.

Zugehörige Tasks:

„Neue Richtlinien erstellen” auf Seite 124
Wenn Sie Mediationsrichtlinien in der Business Space-Benutzerschnittstelle erstellen (Authoring), geben Sie die Bedingungen und Aktionen für die Richtlinie an.

„Lebenszyklus der Richtlinie verwalten” auf Seite 126
Richtlinien können in der Business Space-Benutzerschnittstelle durch Übergänge von einem Governance-Zustand in einen anderen versetzt werden.

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 zusätzliche 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 84.
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. Dies 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) oder Ähnliches) aufrufen können. Die Regel zur Anforderungsverarbeitung führt folgende Aktionen aus:

1. Sie identifiziert durch Basisauthentifizierung.
2. Sie authentifiziert durch eine sehr 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 Operationen aus:

1. Sie führt AAA mit den SSL-Informationen für die Authentifizierung aus.
2. Sie 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: Diese Verarbeitung mit der Antwort 'Zulassung/Verweigerung/Unbestimmt' ist lediglich ein Beispiel. In einen kundenspezifischen 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 manuellen 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 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, stellen Sie fest, dass ähnliche Zuordnungen für Customer und Clerk vorhanden sind. Sie werden bemerken, 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'. Dies ist das Style-Sheet mit der 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. Bei einer Untersuchung des XACML-Dokuments für die Überarbeitung (Redaktion) mit dem Namen 'storePrivateDataXACML.xml' ist zu erkennen, dass die Struktur mit der Struktur im StoreWSP-Szenario annähernd identisch ist. 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/extens
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']/*[
        response']/*[local-name()='Envelope']/*[local-name()='Body']/*[local-name()='Response']/*[local-name()='Result']/
        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 33. Für das SOA Policy Gateway Basic Runtime Sample-Muster erstellte WSRR-Artefakte

Objekt	**Beschreibung**
Organisation	Bob's Warehouse.
Geschäftsfunktion (Business Capability)	'Warehouse', die zur Organisation 'Bob's Warehouse' gehört.
Serviceversion	Store 1.0 verwendet den Web-Service 'Store', die Service-Level-Definition 'Store SLD' und die Geschäftsfunktion 'Warehouse'.
WSDL	Store.wsdl.
XSD	Company.xsd.
Richtlinie	• Validate.xml • RouteForGold.xml • LogEveryTime.xml • RejectAfter5MsgIn90Seconds.xml

Tabelle 33. Für das SOA Policy Gateway Basic Runtime Sample-Muster erstellte WSRR-Artefakte (Forts.)

Objekt	Beschreibung
Richtlinienzuordnungen	• Anonymous Users_GenericObject_Anonymous Users_LogEveryTime.xml - Ordnet die Richtlinie 'LogEveryTime' dem Service-Level-Agreement (SLA) für anonyme Benutzer zu. • Gold SLA_GenericObject_Gold SLA_RouteForGold.xml - Ordnet die Richtlinie 'RouteForGold' dem SLA für Gold-Benutzer (Gold SLA) zu. • Store_GenericObject_Store_urn :RejectAfter5MsgIn90Seconds.xml - Ordnet die Richtlinie 'RejectAfter5MsgIn90Seconds' der SLD 'Store SLD' zu. • Store_GenericObject_Store_urn:Validate.xml - Ordnet die Richtlinie 'Validate' der SLD 'Store SLD' zu.
SLD	Store SLD - Wird von der Serviceversion Store 1.0 verwendet.
SLA	Gold SLA - Leitet an den Gold-Endpunkt weiter, wenn die Kontext-ID (ContextIdentifier) den Wert „Gold" hat.
Anonymes SLA	Anonymous Users - Verwendet die Benachrichtigung der Richtlinie 'LogEveryTime', die ausgeführt wird, wenn die Kontext-ID nicht den Wert „Gold" hat.

Verwendung von WSRR-Artefakten durch die Beispielanwendung

Das Gateway 'StoreWSP' verwendet eine WSRR-Subskription zum Abrufen der WSDL und der Richtlinienartefakte. Wenn eine Anforderung durch StoreWSP verarbeitet wird, werden die folgenden Aktionen ausgeführt:

1. Die Serviceversion Store 1.0 wird mit der Service-Level-Definition 'Store SLD' verbunden, der zwei Richtlinien zugeordnet sind: 'Validate' und 'RejectAfter5MsgIn90Seconds'. Die Reihenfolge, in der die Richtlinien ausgeführt werden, ist unbestimmt.
   a. Wenn fünf Anforderungen in den letzten 90 Sekunden stattgefunden haben, wird die Anforderung zurückgewiesen.
   b. Die Anforderung wird anhand der Datei 'Store.wsdl' und der ihr zugeordneten Datei 'Company.xsd' überprüft.
2. Der Service Store 1.0 verwendet die Service-Level-Definition 'Store SLD', die zwei SLAs hat: 'Gold SLA' zur Verwendung mit Gold-Benutzern und 'Anonymous Users' für alle anderen Benutzer. Wenn das Kontext-ID-Attribut ('ContextIdentifier') den Wert „Gold" hat, wird die Anforderung an die XML-Firewall 'StoreMockServiceAlternate' weitergeleitet. Wenn es den Wert „Silver" oder irgendeinen anderen Wert hat, übernimmt das SLA 'Anonymous Users' und die Richtlinie 'LogEveryTime' wird ausgeführt. Diese Richtlinie fügt eine Benachrichtigung in die Protokolldatei `default.log` der Sample-Domäne ein. Diese Benachrichtigung kann nur angezeigt werden, wenn der Debugmodus für die Domäne aktiviert ist. Die Nachricht wird anschließend an die XML-Firewall 'StoreMockService' weitergeleitet.

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 34. 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.
WSRR-Subskription	StoreSub	Stellt Suchinformationen zu WSRR-Namensbereich, WSRR-Objekt usw. bereit.
AAA-Richtlinie	StoreAddLTPA	Identifikation durch Basisauthentifizierung 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. Dies 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 35. 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.

Tabelle 35. Style-Sheets in der Beispielanwendung (Forts.)

Style-Sheet	Zweck
`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.
`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 36. 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.

Tabelle 36. DataPower-Objekte, die die XSL-Style-Sheets verwenden (Forts.)

Style-Sheet	Zweck
`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

Wenn das IBM SOA Policy Gateway Pattern-Image implementiert wurde, können Sie eigene Servicedefinitionen registrieren und den Definitionen eigene Richtlinien zuordnen. Sie können darüber hinaus Ihre implementierten Systeme anzeigen und verwalten. Zum Anzeigen der Liste der implementierten Instanzen klicken Sie auf **Instances** > **Virtual system**.

Instanzdetails anzeigen

Die Details einer implementierten Instanz können durch Auswählen einer Instanz in der Instanzliste im Fenster 'Virtual System Instances' angezeigt werden. Die Details zu einer virtuellen Systeminstanz werden auf der rechten Seite angezeigt. Zu den Details gehören eine Liste der virtuellen Maschinen, die in der Cloudinfrastruktur für die betreffende Implementierung bereitgestellt wurden, die IP-Adresse, der Status der virtuellen Maschine und der Rollenstatus. Die Rolle ist eine Funktionseinheit, die durch die Middleware der virtuellen Anwendung auf einer virtuellen Maschine ausgeführt wird. Sie können auch die Informationen zum Allgemeinzustand der Rolle der virtuellen Maschine anzeigen. Zum Beispiel wird ein rotes Häkchen auf dem grünen Statuspfeil angezeigt, wenn die CPU auf der virtuellen Maschine einen kritischen Status hat.

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**. Erweitern Sie eine aktive virtuelle Maschine, um die Scriptprotokolle im Abschnitt **Script Packages** sowie Links für den Zugriff auf die virtuelle Maschine im Abschnitt **Consoles** anzuzeigen.

Implementierte Instanzen verwalten

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

Vorbereitende Schritte

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

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. Es können zum Beispiel folgende Möglichkeiten zur Verfügung stehen:
   - Sie könnten die Administrationskonsole für den Deployment Manager starten, sich dort anmelden und die erstellten Cluster anzeigen.
   - Sie könnten die Prozesszentrale starten und den Prozessdesigner herunterladen, um Prozessanwendungen zu erstellen.
   - Sie könnten IBM Integration Designer einrichten und eine Verbindung zur Prozesszentrale für die Prozesserstellung herstellen.

Verbindung zu WSRR herstellen - Business Space

Verwenden Sie die Business Space-Benutzerschnittstelle zur Verwaltung von Richtlinien.

Informationen zu diesem Vorgang

Sie können auf die Business Space-Benutzerschnittstelle über die Hostadresse des WSRR-Systems zugreifen.

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. Greifen Sie auf das WSRR-System über die Business Space-Benutzerschnittstelle zu:
   - Klicken Sie im Abschnitt **Consoles** auf **WSRR Business Space**, um eine Verbindung zu dem Business Space herzustellen, der auf dem WSRR-System aktiv ist.
   - Alternativ haben Sie in einem externen Web-Browser die folgende Möglichkeit:
     a. Ermitteln Sie den Hostnamen und die Portnummern für WSRR. 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**.
     b. Geben Sie die Business Space-URL ein:
        – Für den eigenständigen WSRR-Server mit aktivierter Sicherheit: `https://<hostname>:port/BusinessSpace`
        – Für den Cluster: `http://<hostname>/BusinessSpace`

Dabei sind *<hostname>* und *port* die Werte für den Hostnamen und den Port des WSRR-Servers.

Ergebnisse

Business Space wird angezeigt und kann zum Hinzufügen, Bearbeiten oder Entfernen von Richtlinien 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" auf Seite 110. Führen Sie die Schritte zur Erstellung des Space für Operationen aus.

Zugehörige Informationen:

Information Center von IBM WebSphere Service Registry and Repository Version 8.0

Verbindung zu WSRR herstellen - Service-Registry-Konsole

Verwenden Sie die Service-Registry-Konsole, um Serviceversionen zu klassifizieren.

Informationen zu diesem Vorgang

Sie können auf die Benutzerschnittstelle der Service-Registry-Konsole über die Hostadresse des WSRR-Systems zugreifen.

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. Greifen Sie auf das WSRR-System zu:
   - Klicken Sie im Abschnitt **Consoles** auf **WSRR_Web_UI**, um eine Verbindung zu dem Business Space herzustellen, der auf dem WSRR-System aktiv ist.
   - Alternativ haben Sie in einem externen Web-Browser die folgende Möglichkeit:
     a. Ermitteln Sie den Hostnamen und die Portnummern für WSRR. 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**.
     b. Geben Sie die URL für die Service-Registry-Konsole ein: http://*hostname*/ServiceRegistry

        Dabei ist *hostname* der Hostname des WSRR-Servers.

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 108.

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**.

Musterkonfiguration nach der Implementierung

Nach der Implementierung der Muster müssen Sicherheitseinstellungen und andere Einstellungen konfiguriert werden.

Änderungen von LDAP-Einstellungen für die Beispielanwendung

Wenn Sie SOA Policy Gateway Basic Runtime Sample verwenden und die Sicherheitseinstellungen für Ihren LDAP-Server (z. B. das Kennwort oder den Benutzernamen) ändern müssen, müssen Sie diese Werte an zwei Stellen ändern.

Die Änderungen müssen an den folgenden Stellen vorgenommen werden:

- Der Abschnitt der AAA-Richtlinienauthentifizierung (AAA Policy Authentication) für die AAA-Richtlinie 'StoreAddLTPA' - Verwenden Sie zum Auffinden dieser Richtlinie das Suchfenster der DataPower Administration-Webbenutzerschnittstelle und suchen Sie nach `AAA`. Wählen Sie die betreffende AAA-Richtlinie aus und ändern Sie den Wert auf der Registerkarte 'Authentication'.
- Die Datei `soavars.xsl` - Verwenden Sie den Abschnitt für Dateimanagement (File Management) in der DataPower Administration-Webbenutzerschnittstelle. Öffnen Sie die vom SOA Policy Gateway Basic Runtime Sample-Muster erstellte Domäne auf dem DataPower-Gerät und durchsuchen Sie das lokale Verzeichnis nach der Datei `soavars.xsl`. Ändern Sie die Variablen LDAPHost, LDAPPort, LDAPCN und LDAPPassword in der erforderlichen Weise.

  Anmerkung: Sie müssen die Domäne möglicherweise erneut starten, damit diese Änderungen wirksam werden.

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.

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 sehr spezielles Zertifikat, das zwischen dem Standard-WebSphere Application Server und DataPower funktioniert, funktioniert möglicherweise für das Scriptpaket „SOA Policy Gateway 2.0.0.0 - Security" oder das Scriptpaket „SOA Policy Gateway 2.0.0.0 - Sample" nicht, 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" auf Seite 112.

LTPA-Schlüssel ändern

In dieser Prozedur wird beschrieben, wie der LTPA-Schlüssel geändert wird. Der LTPA-Schlüssel wird von allen Zellen im Basic-Muster 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', 'production' oder 'Unset' importiert.

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. Handelt es sich bei der Laufzeitinstanz um eine Advanced-ND-Umgebung (ND - Network Deployment), 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 es sich um eine Advanced-Umgebung handelt, muss sie in umgekehrter Reihenfolge erneut gestartet werden:
   a. Starten Sie den Dmgr.
   b. Starten Sie die Knotenagenten.
   c. Starten Sie den WSRR-Cluster.
5. Wenn der WSRR-Server ein eigenständiger Server ist, muss er gestoppt und erneut gestartet werden, damit die Änderung des LTPA-Schlüssels wirksam wird.

DataPower-Zertifikate im WSRR-Truststore entfernen oder hinzufügen

In dieser Task wird beschrieben, wie DataPower-Zertifikate hinzugefügt oder entfernt werden. Die Ausführung dieser Task hat u. a. den Vorteil, dass sie die zukünftige Einrichtung der Synchronisationsaktualisierungsfunktion zwischen WSRR und DataPower für Richtlinienaktualisierungen vereinfacht.

Informationen zu diesem Vorgang

Die DataPower-Zertifikate werden als Teil der Muster, die von den mit dem curl-Tool ausgeführten DataPower-Aufrufen verwendet werden, in den Standardtruststore des Knotens bzw. der Zelle hochgeladen. Dies vereinfacht die Einrichtung zukünftiger Verwendungen der Synchronisationsaktualisierungsfunktion zwischen WSRR und DataPower für Richtlinienaktualisierungen. Wenn diese Funktion nicht benötigt wird, beschreibt diese Prozedur, wie DataPower-Zertifikate entfernt werden. Darüber hinaus beschreibt diese Prozedur, wie neue DataPower-Zertifikate hinzugefügt werden, wenn die Zertifikate geändert werden müssen.

Vorgehensweise

1. Melden Sie sich am WSRR-Dmgr-Server bzw. am eigenständigen WSRR-Server mit folgender Adressangabe an: `http://hostname:9060/admin`. Geben Sie den Benutzer und das zugehörige Kennwort ein.

2. Navigieren Sie zu **Security, SSL certficates and key management**.
3. Klicken Sie auf **Key Stores and Certificates**.
4. Klicken Sie auf **NodeDefaultTrustStore**, wenn Sie ein Basic-Muster ausgewählt haben, oder auf **CellDefaultTruststore**, wenn Sie ein Advanced-Muster ausgewählt haben.
5. Klicken Sie auf **Signer Certificates**.
6. Wählen Sie die Kontrollkästchen für die Zertifikate aus, die entfernt werden sollen.
7. Klicken Sie auf **Delete**.
8. Klicken Sie auf **Save**.
9. Optional: Wenn Sie neue DataPower-Zertifikate hinzufügen müssen, klicken Sie auf **Add**, um die neuen Zertifikate hinzuzufügen.

Richtliniendurchsetzungspunkt konfigurieren

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

Vorgehensweise

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 bereitgestellten Beispiel wurden 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 Authentifizierung ist der Schritt, in dem der Benutzer als ein Benutzer bestätigt wird, der dem System bekannt ist. Es stehen viele Optionen zur Auswahl. Im Beispiel wurden zwei Optionen gezeigt: 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 95.
  - 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.

Nächste Schritte

Neben der Erstellung einer Domäne und der Einrichtung einer WSRR-Serverkonfiguration im SOA Policy Gateway Advanced Runtime- und SOA Policy Gateway Basic Runtime-Muster ist es möglich, die Domäne durch Ausführen eines angepassten CLI-Scripts zu erweitern. Das CLI-Script muss sich im Stammverzeichnis der Struktur in der Datei `DomainZipFile.zip` befinden. Beispiel: `/cli.cli`. Die CLI (Befehlszeilenschnittstelle) kann CLI-Standardbefehle ausführen. Alle Artefakte, auf die CLI verweist, müssen jedoch vorhanden sein bzw. für die DataPower-Domäne, die von dem Muster erstellt wird, zugänglich sein. Wenn Sie eine Instanz des SOA Policy Gateway Advanced Runtime- oder SOA Policy Gateway Basic Runtime-Musters implementieren, werden Sie aufgefordert, den CLI-Dateinamen in den Parametern des Sicherheitspakets ('Security') anzugeben.

Mit dem SOA Policy Gateway Basic Runtime-Muster arbeiten

Das SOA Policy Gateway Basic Runtime-Muster besteht aus drei wesentlichen Funktionsabschnitten: Die Dateien, die für die Sicherheit zwischen DataPower und den WSRR-Musterscripts erforderlich sind, werden abgerufen, eine Domäne wird in DataPower konfiguriert und schließlich wird die Umstufung (Promotion) konfiguriert.

Nach Abschluss der Konfiguration haben die folgenden Aktionen stattgefunden:

1. Die neue Domäne wurde auf dem angegebenen DataPower-Gerät erstellt.
2. Eine WSRR-Serverdefinition wurde in der Domäne erstellt.
3. Das angepasste CLI-Script wurde für die DataPower-Domäne ausgeführt.
4. Ein WSRR-Server wurde konfiguriert.
5. Alle DataPower-Unterzeichnerzertifikate, die vom Kunden bereitgestellt wurden, wurden in den Standardtrustore der WSRR-Zelle ('NodeDefaultTruststore') hochgeladen.
6. Die Umstufung (Promotion) zwischen der WSRR-Zelle des SOA Policy Gateway Basic Runtime-Musters und der SOA Policy Gateway Governance Master-Zelle wurde konfiguriert.
7. Unterzeichnerzertifikate wurden ausgetauscht. Das Unterzeichnerzertifikat des Governance-Dmgr wurde im Standardtruststore 'NodeDefaultTrustStore' der Basic-Zelle abgelegt und das Unterzeichnerzertifikat des Dmgr der Basic-Zelle wurde im Standardtruststore 'CellDefaultTrustStore' der Governance-Zelle abgelegt.
8. LTPA-Schlüssel wurden ausgetauscht. Der LTPA-Schlüssel der Governance-Zelle wurde in die Basic-Zelle importiert.
9. Jeder Host des WSRR-Clusters mit dem Governance Master wurde den vertrauenswürdigen Realms der Basic-Zelle hinzugefügt. Jeder Host des WSRR-Clusters der Basic-Zelle wurde den vertrauenswürdigen Realms des Governance Masters hinzugefügt.
10. Die Promotionseigenschaftendatei wurde konfiguriert, wenn die Zelle entweder als Stagingumgebung oder als Produktionsumgebung in den gegebenen Eingaben vorgesehen war.

Obwohl noch weitere Schritte erforderlich sind, um eine vollständig sichere Produktionsumgebung herzustellen, lässt die bis zu diesem Punkt ausgeführte Konfiguration die Ausführung der folgenden Aktionen zu:

1. Mithilfe des Standard-Governance-Realisierungsprofils (GEP) können Sie Services und Richtlinien erstellen und durch den SOA-Lebenszyklus in WSRR regeln (wenn eine Staging- und eine Produktionsumgebung bereitgestellt wurden).
2. Sie können Web-Service-Proxys erstellen, die die vorab erstellte WSRR-Serverdefinition zum Erstellen von Subskriptionen verwenden können.

Mit dem SOA Policy Gateway Advanced Runtime-Muster arbeiten

Das SOA Policy Gateway Advanced Runtime-Muster besteht aus drei wesentlichen Funktionsabschnitten: Die Dateien, die für die Sicherheit zwischen DataPower und den WSRR-Musterscripts erforderlich sind, werden abgerufen, eine Domäne wird in DataPower konfiguriert und schließlich wird die Umstufung (Promotion) konfiguriert.

Nach Abschluss der Konfiguration haben die folgenden Aktionen stattgefunden:

1. Eine neue Domäne wurde auf dem angegebenen DataPower-Gerät erstellt.
2. Eine WSRR-Serverdefinition wurde in der Domäne erstellt.
3. Das angepasste CLI-Script wurde für die DataPower-Domäne ausgeführt.
4. Eine WSRR-Clusterumgebung mit 'n' Knoten wurde erstellt und konfiguriert.
5. Alle DataPower-Unterzeichnerzertifikate, die vom Kunden bereitgestellt wurden, wurden in den Standardtrustore der WSRR-Zelle (CellDefaultTruststore) hochgeladen.
6. Die Umstufung (Promotion) zwischen der WSRR-Zelle des SOA Policy Gateway Advanced Runtime-Musters und der SOA Policy Gateway Governance Master-Zelle wurde konfiguriert:
   a. Unterzeichnerzertifikate wurden ausgetauscht. Das Unterzeichnerzertifikat des Governance-Dmgr wurde im Standardtruststore 'CellDefaultTrustStore' der Advanced-Zelle abgelegt und das Unterzeichnerzertifikat des Dmgr der Advanced-Zelle wurde im Standardtruststore 'CellDefaultTrustStore' der Governance-Zelle abgelegt.
   b. LTPA-Schlüssel wurden ausgetauscht. Der LTPA-Schlüssel der Governance-Zelle wurde in die Advanced-Zelle importiert.
   c. Jeder Host des WSRR-Clusters mit dem Governance Master wurde den vertrauenswürdigen Realms der Advanced-Zelle hinzugefügt. Jeder Host des WSRR-Clusters der Advanced-Zelle wurde den vertrauenswürdigen Realms des Governance Masters hinzugefügt.
   d. Die Promotionseigenschaftendatei wurde konfiguriert, wenn die Zelle entweder als Stagingumgebung oder als Produktionsumgebung in den gegebenen Eingaben vorgesehen war.

Die aktuelle Konfiguration ermöglicht die folgenden Aktionen:

1. Mithilfe des Standard-Governance-Realisierungsprofils (GEP, Governance Enablement Profile) können Sie Services und Richtlinien erstellen und durch den SOA-Lebenszyklus in WSRR regeln (wenn eine Staging- und eine Produktionsumgebung bereitgestellt wurden).
2. Sie können Web-Service-Proxys erstellen, die die vorab erstellte WSRR-Serverdefinition zum Erstellen von Subskriptionen verwenden können.

Als Nächstes müssen Sie weitere Schritte ausführen, um eine vollständig sichere Produktionsumgebung herzustellen. Weitere Informationen finden Sie in „Sicherheit für die IBM SOA Policy Gateway Pattern-Muster" auf Seite 65.

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

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

Tabelle 37. Objekte des DataPower-Musters

Objekt	Beschreibung
Domäne	Eine Domäne, die für die Benutzeranwendung verwendet werden kann.
WSRR-Server	Hat den Namen WSRRSVR. Die SOAP-URL, der Benutzer und das Kennwort sowie ein SSL-Proxy-Profil mit Berechtigungsnachweisen zur Überprüfung werden konfiguriert.

Tabelle 37. Objekte des DataPower-Musters (Forts.)

Objekt	Beschreibung
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.

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 erstellt wurde, finden Sie Informationen in „Business Space für die Erstverwendung konfigurieren" auf Seite 110. 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 108
Verwenden Sie die Business Space-Benutzerschnittstelle zur Verwaltung von Richtlinien.

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 Verfassen (Authoring) aller SOA-Richtlinien verwendet werden. Dazu gehören SLA-Richtlinien (SLA, Service-Level-Agreement), Mediationsrichtlinien, angepasste Richtlinien und andere Richtliniendomänen, deren Unterstützung für die Zukunft vorgesehen ist. 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 Richtlinien erstellen" auf Seite 124.

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 sollten im Rahmen der Analyse und des Entwurfs dieses Service nicht funktionale Anforderungen definiert werden, 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 das SLA nicht erfüllt wird, 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 normalerweise 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 dieser Art 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 angegebene 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.

  Anmerkung: Klicken Sie auf den Hyperlink 'xs:date', 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. (Anmerkung: 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 erforderliche Parameter, die aus Attribut, Operator und Wert bestehen, sowie zwei optionale Parameter für ein Intervall und eine Begrenzung ('Limit'). 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 38. 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 39. 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 39. 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.

  Anmerkung: 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 WebSphere 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 sollen. Nachrichten sollen zurückgewiesen werden, 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 40. 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 'Stylesheet' 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 Richtlinien erstellen

Wenn Sie Mediationsrichtlinien in der Business Space-Benutzerschnittstelle erstellen (Authoring), geben Sie die Bedingungen und Aktionen für die Richtlinie an.

Vorbereitende Schritte

Informationen zum Zugriff auf Business Space finden Sie in „Verbindung zu WSRR herstellen - Business Space” auf Seite 108.

Der SOA Governance-Space muss erstellt werden, bevor Richtlinien erstellt werden können. Wenn der SOA-Governance-Space noch nicht erstellt wurde, finden Sie Informationen in „Business Space für die Erstverwendung konfigurieren” auf Seite 110. Führen Sie die beschriebenen Schritte aus, um den Space zu erstellen.

Informationen zu diesem Vorgang

Erstellen Sie neue Richtlinien im 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 118 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 soeben erstellt haben, 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.

Zugehörige Konzepte:

„Richtlinien" auf Seite 118
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

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 110.

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.

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' in der linken unteren Ecke der Anzeige auswählen. 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. 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
Mediationsrichtlinien 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 zu DataPower 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 DataPower, 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.
- Prüfen Sie die unten beschriebenen Schritte zur Fehlerbehebung bei einem SSL-Verbindungsfehler, um sicherzustellen, dass die Zertifikate sowohl in der Datei `DomainZipFile.zip` als auch im DataPower-Gerät ordnungsgemäß installiert sind.

Fehlerbehebung bei fehlgeschlagener Clientauthentifizierung für die gegenseitige Authentifizierung

Versuchen Sie die folgenden Lösungen:

- Überprüfen Sie, ob sich die richtigen Zertifikate in der Datei `DomainZipFile.zip` befanden.
- Überprüfen Sie, ob das Kryptoprofil für den XML Management Interface-Port Berechtigungsnachweise zur Überprüfung für alle Zertifikate in der Kette enthält.
- Überprüfen Sie, ob die Kennwörter für den öffentlichen Clientschlüssel und das öffentliche Clientzertifikat korrekt sind.

Fehlerbehebung bei fehlgeschlagener Serverauthentifizierung

Versuchen Sie die folgenden Lösungen:

- Überprüfen Sie, ob alle Zertifikate in der Kette im Verzeichnis *ihrDataPowerHostName* der von Ihnen verwendeten Datei `DominZipFile.zip` vorhanden sind.
- Überprüfen Sie, ob das SSL-Proxy-Profil ein Umkehrkryptoprofil hat, das die Berechtigungsnachweise zur Identifikation bei der Zertifikatskette enthält.

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 fehlschlagender Verbindung zu einem SCP

Versuchen Sie die folgenden Lösungen:

- Überprüfen Sie, ob der SCP-Hostname korrekt ist.
- Überprüfen Sie, ob der SCP-Benutzer korrekt ist.
- Überprüfen Sie, ob das SCP-Kennwort korrekt ist.
- Führen Sie einen manuellen SCP-Test von einem Knoten in der IBM Workload Deployer- oder IBM PureApplication System-Umgebung mit den angegeben Informationen durch.

Fehlerbehebung bei fehlschlagendem Abrufen der Datei `DomainZipFile.zip` über SCP oder bei fehlschlagendem Debugging fehlender Artefakte

Versuchen Sie die folgenden Lösungen:

- Überprüfen Sie, ob die Datei `DomainZipFile.zip` an der URI-Position vorhanden ist.
- Überprüfen Sie, ob die in der Protokollfehlernachricht genannte Datei an der richtigen Position in der Datei `DomainZipFile.zip` vorhanden ist. Stellen Sie insbesondere sicher, dass sich die erforderlichen Zertifikate im richtigen Verzeichnis befinden.

Fehlerbehebung bei einem Umstufungsfehler (Promotionsfehler)

Es gibt zahlreiche Probleme, die bei einer Umstufung (Promotion) auftreten können. 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 (SOA Policy Gateway Basic Runtime oder SOA Policy Gateway Advanced Runtime) vorhanden ist.
  - Prüfen Sie in jeder Laufzeitumgebung (SOA Policy Gateway Basic Runtime oder SOA Policy Gateway Advanced Runtime) 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 SSL-Fehlern wegen fehlender DataPower-Zertifikate

Wenn nicht der korrekte Hostname für Ihr DataPower-Zertifikatsverzeichnis in der Datei `DomainZipFile.zip` angegeben wurde, können die Scriptpakete keine Verbindung zum WSRR-Server herstellen, wenn die gegenseitige Authentifizierung oder die Serverauthentifizierung auf dem DataPower-Host aktiviert ist.

Fehlerbehebung bei WSRR/DataPower-Verbindungsproblemen

Wenn Sie erkennen, dass sich die WSDL in einem Web-Service-Proxy in einem Status 'inaktiv' (Down) oder 'wird synchronisiert' (Synchronizing) befindet, der sich nie in OK ändert, überprüfen Sie die folgenden Punkte:

1. Überprüfen Sie, ob das Kryptozertifikat für den WSRR-Server (WSRRSVR) gültig ist.
2. Überprüfen Sie, ob für DataPower die richtige DNS-Konfiguration zur Erkennung des Hostnamens des WSRR-Servers oder des Dmgr eingerichtet ist.
3. Wenn das DNS (Domain Name System) nicht richtig ist, besteht eine vorläufige Fehlerumgehung darin, die URL in der WSRR-Serverdefinition so zu ändern, dass sie direkt die IP-Adresse angibt. Dazu muss die IP-Adresse anstelle des Hostnamens (HostName) in der URL eingesetzt werden.
4. Navigieren Sie zur WSRR-Subskription und führen Sie eine manuelle Synchronisation aus:
   a. Überprüfen Sie die Datei `default.log` auf Fehler in Bezug auf die Konnektivität des WSRR-Servers.
5. Stellen Sie sicher, dass die erforderlichen Zertifikate den Zertifikaten in den Berechtigungsnachweisen zur Identifikation für das Kryptoprofil des SSL-Proxy-Profils der XML-Managementschnittstelle (XML Management Interface) des DataPower-Geräts entsprechen.

Fehlerbehebung bei Problemen in der implementierten Instanz

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

Verbindung zu LDAP wird nicht hergestellt

Versuchen Sie zur Diagnose von LDAP-Fehlern im Beispiel die folgenden Lösungen:

- Stellen Sie unter 'Troubleshooting' der DataPower Control Panel-Anzeige sicher, dass die Tracefunktion im Debugmodus arbeitet.
- Navigieren Sie zu 'StoreAddLTPA', öffnen Sie die Details für den Testmonitor ('Probe') und aktivieren Sie den Testmonitor.
- Führen Sie einen Clienttest durch.
- Prüfen Sie die Protokolle im Testmonitor. Suchen Sie nach 'LDAP Bind'-Fehlernachrichten.
- Überprüfen Sie den LDAP-Hostnamen.
- Überprüfen Sie den definierten LDAP-Namen (DN). Beispiel: cn=root,dc=ibm.com.
- Überprüfen Sie das LDAP-Kennwort. Beispiel: passw0rd.

- Überprüfen Sie, ob der LDAP-Port die Nummer 389 hat und nicht gesichert ist.
- Überprüfen Sie, ob die Eingabekennwörter für ConsumerX, ConsumerA, ConsumerB alle 'passw0rd' lauten. Stellen Sie sicher, dass der LDIF-Dateiimport die richtigen Kennwörter transkribiert hat.

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.

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.

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 neue 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.

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

Bemerkungen

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden.

Möglicherweise bietet IBM die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim zuständigen IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, dass nur Programme, Produkte oder Services von IBM verwendet werden können. An Stelle der IBM Produkte, Programme oder Services können auch andere, ihnen äquivalente Produkte, Programme oder Services verwendet werden, solange diese keine gewerblichen oder anderen Schutzrechte der IBM verletzen. Die Verantwortung für den Betrieb von Produkten, Programmen und Services anderer Anbieter liegt beim Kunden.

Für in diesem Handbuch beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanforderungen sind schriftlich an folgende Adresse zu richten (Anfragen an diese Adresse müssen auf Englisch formuliert werden):

IBM Director of Licensing
IBM Europe, Middle East & Africa
Tour Descartes
2, avenue Gambetta, 92066 Paris La Defense
France

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die Angaben in diesem Handbuch werden in regelmäßigen Zeitabständen aktualisiert. Die Änderungen werden in Überarbeitungen oder in Technical News Letters (TNLs) bekannt gegeben. IBM kann ohne weitere Mitteilung jederzeit Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Verweise in diesen Informationen auf Websites anderer Anbieter dienen lediglich als Benutzerinformationen und stellen keinerlei Billigung des Inhalts dieser Websites dar. Das über diese Websites verfügbare Material ist nicht Bestandteil des Materials für dieses IBM Produkt. Die Verwendung dieser Websites geschieht auf eigene Verantwortung.

Werden an IBM Informationen eingesandt, können diese beliebig verwendet werden, ohne dass eine Verpflichtung gegenüber dem Einsender entsteht.

Lizenznehmer des Programms, die Informationen zu diesem Produkt wünschen mit der Zielsetzung: (i) den Austausch von Informationen zwischen unabhängig voneinander erstellten Programmen und anderen Programmen (einschließlich des vorliegenden Programms) sowie (ii) die gemeinsame Nutzung der ausgetauschten Informationen zu ermöglichen, wenden sich an folgende Adresse:

IBM Europe, Middle East & Africa
Software Interoperability Coordinator, Department 49XA
3605 Highway 52 N
Rochester, MN 55901
France

Die Bereitstellung dieser Informationen kann unter Umständen von bestimmten Bedingungen - in einigen Fällen auch von der Zahlung einer Gebühr - abhängig sein.

Die Lieferung des in diesen Informationen aufgeführten Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt auf der Basis der IBM Rahmenvereinbarung bzw. der Allgemeinen Geschäftsbedingungen von IBM, der IBM Internationalen Nutzungsbedingungen für Programmpakete oder einer äquivalenten Vereinbarung.

Alle in diesem Dokument enthaltenen Leistungsdaten stammen aus einer kontrollierten Umgebung. Die Ergebnisse, die in anderen Betriebsumgebungen erzielt werden, können daher erheblich von den hier erzielten Ergebnissen abweichen. Einige Daten stammen möglicherweise von Systemen, deren Entwicklung noch nicht abgeschlossen ist. Eine Gewährleistung, dass diese Daten auch in allgemein verfügbaren Systemen erzielt werden, kann nicht gegeben werden. Darüber hinaus wurden einige Daten unter Umständen durch Extrapolation berechnet. Die tatsächlichen Ergebnisse können abweichen. Benutzer dieses Dokuments sollten die entsprechenden Daten in ihrer spezifischen Umgebung prüfen.

Alle Informationen zu Produkten anderer Anbieter stammen von den Anbietern der aufgeführten Produkte, deren veröffentlichten Ankündigungen oder anderen allgemein verfügbaren Quellen. IBM hat diese Produkte nicht getestet und kann daher keine Aussagen zu Leistung, Kompatibilität oder anderen Merkmalen machen. Fragen zu den Leistungsmerkmalen von Produkten anderer Anbieter sind an den jeweiligen Anbieter zu richten.

Die oben genannten Erklärungen bezüglich der Produktstrategien und Absichtserklärungen von IBM stellen die gegenwärtige Absicht von IBM dar, unterliegen Änderungen oder können zurückgenommen werden, und repräsentieren nur die Ziele von IBM.

Diese Veröffentlichung enthält Beispiele für Daten und Berichte des alltäglichen Geschäftsablaufes. Sie sollen nur die Funktionen des Lizenzprogrammes illustrieren; sie können Namen von Personen, Firmen, Marken oder Produkten enthalten. Alle diese Namen sind frei erfunden; Ähnlichkeiten mit tatsächlichen Namen und Adressen sind rein zufällig.

COPYRIGHTLIZENZ:

Diese Veröffentlichung enthält Musteranwendungsprogramme, die in Quellensprache geschrieben sind und Programmiertechniken in verschiedenen Betriebsumgebungen veranschaulichen. Sie dürfen diese Musterprogramme kostenlos kopieren, ändern und verteilen, wenn dies zu dem Zweck geschieht, Anwendungsprogramme zu entwickeln, verwenden, vermarkten oder zu verteilen, die mit der Anwendungsprogrammierschnittstelle konform sind, für die diese Musterprogramme geschrieben werden. Diese Beispiele wurden nicht unter allen

denkbaren Bedingungen getestet. Daher kann IBM die Zuverlässigkeit, Wartungsfreundlichkeit oder Funktion dieser Programme weder zusagen noch gewährleisten.

Werden diese Informationen als Softcopy angezeigt, erscheinen keine Fotografien oder Farbabbildungen.

Informationen zu Programmierschnittstellen

Bereitgestellte Informationen zur Programmierschnittstelle sind als Unterstützung für die Erstellung von Anwendungssoftware mit diesem Programm gedacht.

Diese Informationen können jedoch auch Angaben über Diagnose, Bearbeitung und Optimierung enthalten. Die Informationen zu Diagnose, Bearbeitung und Optimierung sollten Ihnen bei der Fehlerbehebung für die Anwendungssoftware helfen.

Wichtig: Verwenden Sie diese Informationen zu Diagnose, Änderung und Optimierung nicht als Programmierschnittstelle, da sie jederzeit geändert werden können.

Marken

IBM, das IBM Logo und ibm.com sind Marken der IBM Corporation. Eine aktuelle Liste der IBM Marken finden Sie auf der Webseite „Copyright and trademark information“ unter ibm.com/legal/copytrade.shtml. Weitere Produkt- und Servicenamen können Marken von IBM oder anderen Unternehmen sein.

Dieses Produkt enthält Software, die vom Eclipse-Projekt entwickelt wurde (http://www.eclipse.org/).

Java und alle auf Java basierenden Marken und Logos sind Marken oder eingetragene Marken der Oracle Corporation und/oder ihrer verbundenen Unternehmen.

Senden Ihrer Kommentare an IBM

Wenn Ihnen an diesem Handbuch etwas besonders gefällt oder missfällt, dann lassen Sie IBM über einen der folgenden Wege Ihre Kommentare zukommen.

Halten Sie nichts zurück, was Sie als besonderen Fehler oder als Versäumnis in Bezug auf die Genauigkeit, die Struktur, den Inhalt oder die Vollständigkeit der Dokumentation ansehen.

Beschränken Sie aber bitte Ihre Kommentare auf die Informationen in diesem Handbuch und die Art, in der die Informationen präsentiert werden.

Kommentare zu den Funktionen von Produkten oder Systemen von IBM richten Sie bitte an Ihren IBM Ansprechpartner oder an Ihren autorisierten IBM Vertriebsbeauftragten.

Werden an IBM Kommentare eingesendet, dann erhält IBM das nicht ausschließliche Recht, diese beliebig und nach eigenem Ermessen zu verwenden oder weiterzugeben, ohne dass eine Verpflichtung gegenüber dem Einsender entsteht.

Für die Einsendung von Kommentaren an IBM stehen Ihnen die folgenden Möglichkeiten zur Verfügung:

- Per Post an die folgende Adresse:

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

- Per Fax:
  - Außerhalb von GB verwenden Sie hinter Ihrem internationalen Zugriffscode die Nummer 44–1962–816151
  - In GB verwenden Sie die Nummer 01962–816151
- Auf elektronischen Wege mit der entsprechenden Netz-ID:
  - IBM Mail Exchange: GBIBM2Q9 bei IBMMAIL
  - IBMLink: HURSLEY(IDRCF)
  - Internet: idrcf@hursley.ibm.com

In jedem Fall sollten Sie die folgenden Informationen angeben:

- Den Titel und die Bestellnummer der Veröffentlichung
- Den Abschnitt, auf den sich Ihr Kommentar bezieht
- Ihren Namen und Ihre Adresse, Telefonnummer, Faxnummer oder Netz-ID.