IBM SOA Policy Gateway Pattern

Table des matières

Chapitre 1. Présentation des règles SOA

La gestion des règles joue un rôle déterminant dans les règles de gouvernance de manière structurée et cohérente. Les règles peuvent être utilisées pour permettre une meilleure gouvernance dans un environnement orienté service.

Une règle est un élément indépendant qui peuvent être appliqué à une ou plusieurs ressources, y compris des services différents. L'affectation de la règle et toutes métadonnées associées, en particulier dans un environnement distribué, peut avoir lieu à divers points d'application et les points de décision.

Architecture de règles SOA

L'architecture de règles SOA décrit l'interaction du point d'administration de règles (PAP, Policy Administration Point), du point d'application de règles (PEP, Policy Enforcement Point), du point de décision de règles (PDP, Policy Decision Point), du point d'information de règle (PIP, Policy Information Point)et du point de contrôle de règles (PMP, Policy Monitoring Point). Dans le modèle, le PAP est fourni par WSRR, le PEP est fourni par WebSphere DataPower et le PMP est fourni par l'intermédiaire du composant de surveillance DataPower.

L'organisation de l'architecture des règles de base et la définition de ces points clés :

- **Policy Administration Point** (PAP, Point d'administration de règles). Fournit des fonctions de règle permettant la création d'une règle, sa gestion et sa gouvernance et son affectation à des ressources et l'administration des résultats de la règle pendant l'exécution. Le PAP inclut un référentiel pour stocker des règles. Il est fourni par WSRR.
- **Policy Enforcement Point** (PEP, Point d'application de règles). Un point d'application de règles est un point fonctionnel qui s'exécute sur le middleware. Il exécute les actions suivantes :
  - Applique des règles.
  - Reçoit des mises à jour de règles d'application et les met à disposition ou les traduit en vue de leur utilisation.
  - Fournit des mesures d'application au point de contrôle de règles.
  - Fournit au point d'administration de règles (PAP) et aux points de contrôle de règles (PMP), des résultats et des analyses sur les règles d'application.
  - Modifie les endroits où les règles sont appliquées et appliquées selon la phase du cycle de vie :
    - Lors de la phase de conception, WSRR constitue le point d'application.
    - Lors de la phase d'exécution, c'est le système intermédiaire sous-jacent (middleware) qui relie des fournisseurs de services à des consommateurs qui applique généralement les règles.

  Dans ce modèle, le PEP est fourni par WebSphere DataPower.
- **Policy Decision Point** (PDP, Point de décision de règles). Un point de décision de règles évalue les requêtes des participants par rapport à des règles ou des contrats et des attributs. Le PDP renvoie une décision d'autorisation, d'éligibilité ou de validation pour la fourniture de résultats calculés.

- **Policy Information Point** (PIP, Point d'information de règle). Un point d'information de règle fournit des informations externes au point de décision de règles (PDP), comme des informations d'attributs LDAP ou des résultats d'une base de données avec des informations qui doivent être évaluées pour permettre une prise de décision stratégique.
- **Policy Monitoring Point** (PMP, Point de contrôle de règle). Un composant fonctionnel qui fournit une fonction de contrôle détaillée des règles pour l'architecture globale ; par exemple, la présentation de la règle dans l'environnement distribué. Il exécute les actions suivantes :
  - La réception des mises à jour de règles de contrôle et leur mise à disposition ou leur traduction en vue de leur utilisation.
  - La capture de la collecte en temps réel et l'analyse des statistiques pour affichage.
  - La corrélation, l'analyse et la visualisation des données fournies par les différents collecteurs en temps réel, notamment les points d'application de règles.
  - Une console de gestion qui fournit une visibilité dans la gestion du réseau distribué des points d'application de règles, et le statut de ces applications.
  - La consignation et l'agrégation des mesures ainsi que la mise en évidence des événements importants, selon les spécifications de la règle de contrôle.
  - La fourniture d'une analyse des règles de contrôle pour le point d'administration de règles (PAP) et les points d'application de règles (PEP).

  Dans ce modèle, le PMP est fourni par le composant de surveillance de DataPower.

Le consommateur et le fournisseur interagissent avec le middleware qui à sa tour interagit avec le référentiel et des logiciels de surveillance.

Fonctionnement coordonné de l'architecture de règles SOA

Le flux de modèles avec des règles SOA est présenté dans figure 1, à la page 3.

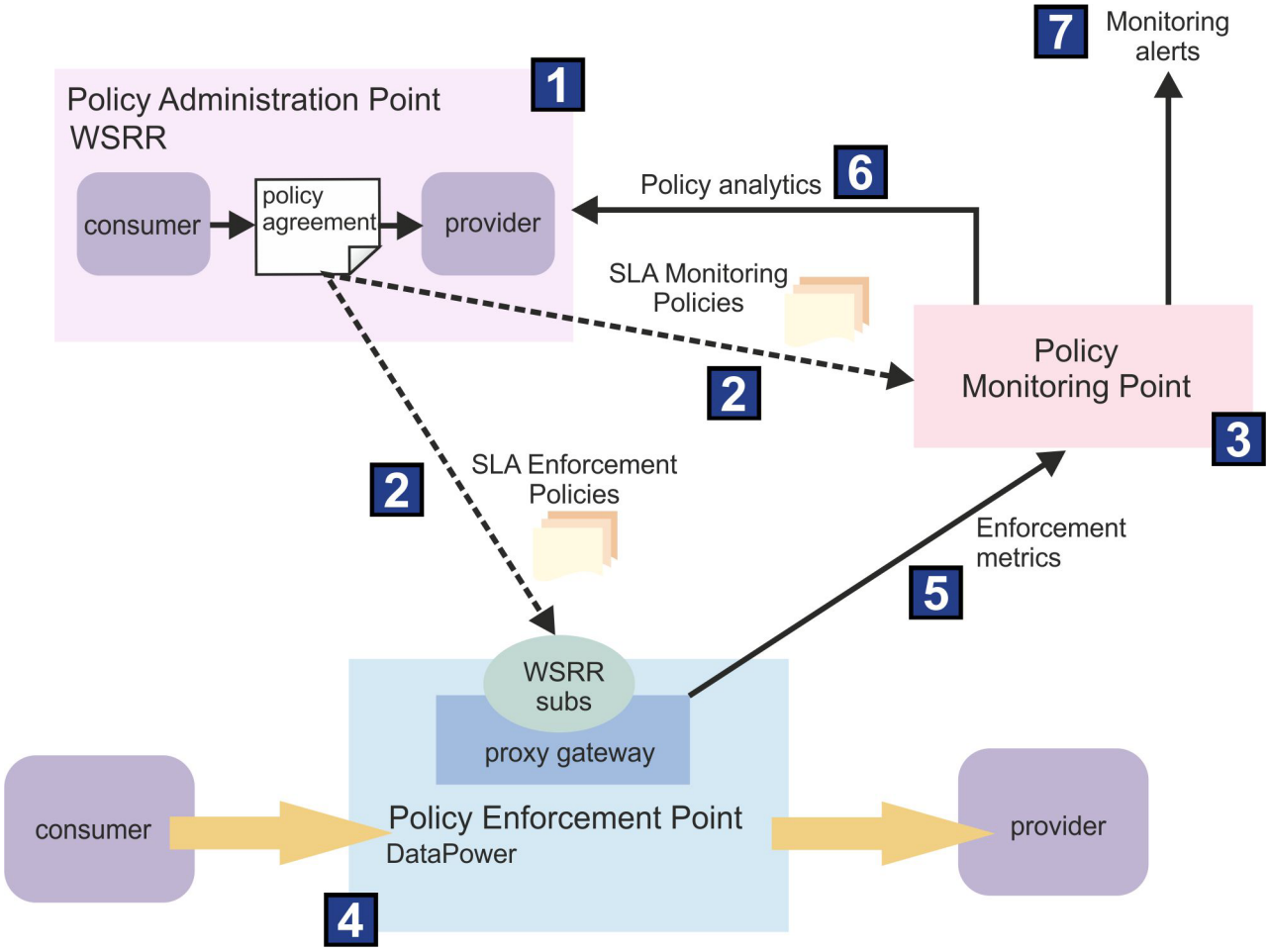


Figure 1. Règle d'accord sur les niveaux de licence (SLA) - le modèle de déploiement SOA

1 Les règles sont créées, puis associées à des services nécessitant cette règle. En général, les opérations sont menées dans l'ordre suivant :

1. Tous les services sont chargés ou créés dans le référentiel de service. Il s'agit d'un composant du point d'administration de règles (PAP).
2. Toutes les règles requises sont créées au niveau du point d'administration de règles (PAP) en utilisant le cycle de vie des règles :
   - Les règles sont attachées aux services qui nécessitent ces règles : au niveau du service, de l'exploitation ou du noeud final, selon le besoin.

2 Publication/soumission automatique de règles issue du point d'administration de règles (PAP) pour le point d'application de règles (PEP) et le point de contrôle des règles (PMP) :

1. Lors de la configuration, le service de surveillance souscrit à la règle de surveillance issue de WSRR. Cette action ne se produit qu'une seule fois.
2. Lors de la configuration, des passerelles de proxy sont créées dans chaque dispositif WebSphere DataPower disposant de transactions de service avec une application de règles. Cette action ne se produit qu'une seule fois, et elle est ajoutée ou modifiée, le cas échéant.

3. Lors de la configuration, chaque passerelle de proxy du dispositif souscrit à des règles de WSRR pour les services dont elle a la responsabilité. Cette action ne se produit qu'une seule fois, et elle est ajoutée ou modifiée, le cas échéant.
4. Lors de la configuration, WebSphere DataPower est configuré pour permettre le partage des règles par d'autres dispositifs au sein d'un cluster. Cette action ne se produit qu'une seule fois, et elle est ajoutée ou modifiée, le cas échéant.
5. Le PMP télécharge les règles de contrôle à mesure de leur publication.
6. Le PMP convertit les règles en une présentation interne appelée règles de situation.
7. WebSphere DataPower télécharge les WSDL pour des services dont il a la responsabilité des transactions.
8. WebSphere DataPower télécharge les règles pour des services dont il a la responsabilité en cas de notification par WSRR.
9. WebSphereDataPower convertit les règles en une représentation WebSphere DataPower interne sous la forme d'objets SLM.

 Contrôle des règles SOA avec génération de rapports et notification des opérations :

1. Les règles de contrôle sont actives dans la règle de situation PMP.
2. Le PMP reçoit des informations de contrôle et place ces informations dans des espaces de travail.

 Application des règles SOA :

1. Les règles d'application sont actives dans les différents dispositifs de WebSphere DataPower.
2. WebSphereDataPower reçoit des transactions de service et applique des règles pour ce service consommateur ou service fournisseur.

 Le point d'application de règles (PEP) envoie des statistiques de mise en application des règles SOA au point de contrôle des règles (PMP).

 Le point de contrôle de règles (PMP) envoie des événements de contrôle au point d'administration de règles (PAP) :

1. Des événements sont configurés au niveau du point d'administration de règles (PAP) pour être contrôlés depuis le point de contrôle de règles (PMP). Cette action ne se produit qu'une seule fois, et elle est ajoutée ou modifiée, le cas échéant.
2. A mesure que les règles de situation sont évaluées à true (vrai), les événements sont poussés du point de contrôle de règles (PMP) vers le point de création de règles (PAP).

 Contrôle des alertes :

- Les règles de situation sont exécutées périodiquement et mènent des actions opérationnelles comme spécifié dans la règle. La valeur par défaut est toutes les 5 minutes.

Cycle de vie de règles SOA

Les règles sont régies par le cycle de vie de règles SOA. Ce cycle de vie prend la règle depuis son identification initiale jusqu'à ce qu'elle soit plus requise et considérée comme obsolète, en passant par son déploiement en production.

Pour plus d'informations sur les transitions et états de cycle de vie du cycle de vie de règles SOA, voir Centre de documentation d'IBM® WebSphere Service Registry and Repository version 8.0 - Cycle de vie des règles SOA.

Normes associées à des règles

Les groupes du comité technique du Web, W3C et OASIS, ont créé des normes pour définir les règles applicables aux services du Web.

- **WS-Policy** : Le domaine Web Services Mediation Policy 1.0 définit un ensemble d'assertions de règles permettant de décrire les exigences de médiation relatives à un service.
- **Web Services Policy 1.5 - Framework** : définit un cadre et un modèle pour exprimer des règles qui font référence à des fonctionnalités, exigences et caractéristiques générales et spécifiques du domaine d'entités d'un système basé sur des services Web.

Exemples de spécifications qui définissent des assertions de règles spécifiques de domaine :

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

Pour plus d'informations sur WS-MediationPolicy, voir ftp://public.dhe.ibm.com/software/solutions/soa/pdfs/WSMediationPolicy1.7-20130506.pdf.

Le modèle de données WS-Policy inclut les entités suivantes :

- **Policy** : un ensemble non ordonné d'alternatives de règles «Policy Alternative».
- **Policy Alternative** : une alternative de règle est un ensemble d'assertions de règles «Policy Assertion».
- **Policy Assertion** : représente une préférence individuelle ; par exemple, une exigence ou une fonctionnalité.
- **Policy Parameters** : le contenu opaque d'une assertion de règle «Policy Assertion».
- **Policy Subject** : une entité à laquelle une expression de règles peut être liée. Cette entité est utilisée dans un document WS-PolicyAttachment.

Pour l'exemple suivant, figure 2, à la page 6, présente une expression de règle de sécurité définie dans WS-Security et WS-SecurityPolicy :

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

Les lignes (03) à (07) représentent une alternative de règle pour la signature d'un corps du message.

Les lignes (08) à (12) représentent une deuxième alternative de règle destinée au chiffrement d'un corps de message.

Les lignes (02) à (13) présentent l'opérateur de règle `ExactlyOne`. Les opérateurs de règles regroupent des assertions de règles dans des alternatives de règles. Une interprétation valide de la règle ci-dessus est qu'un appel d'un service Web doit signer ou chiffrer le corps du message, mais pas les deux en même temps.

Figure 2. Utilisation d'une règle de service Web avec des assertions de règles de sécurité.

La figure 3 affiche une définition de règle d'administration.

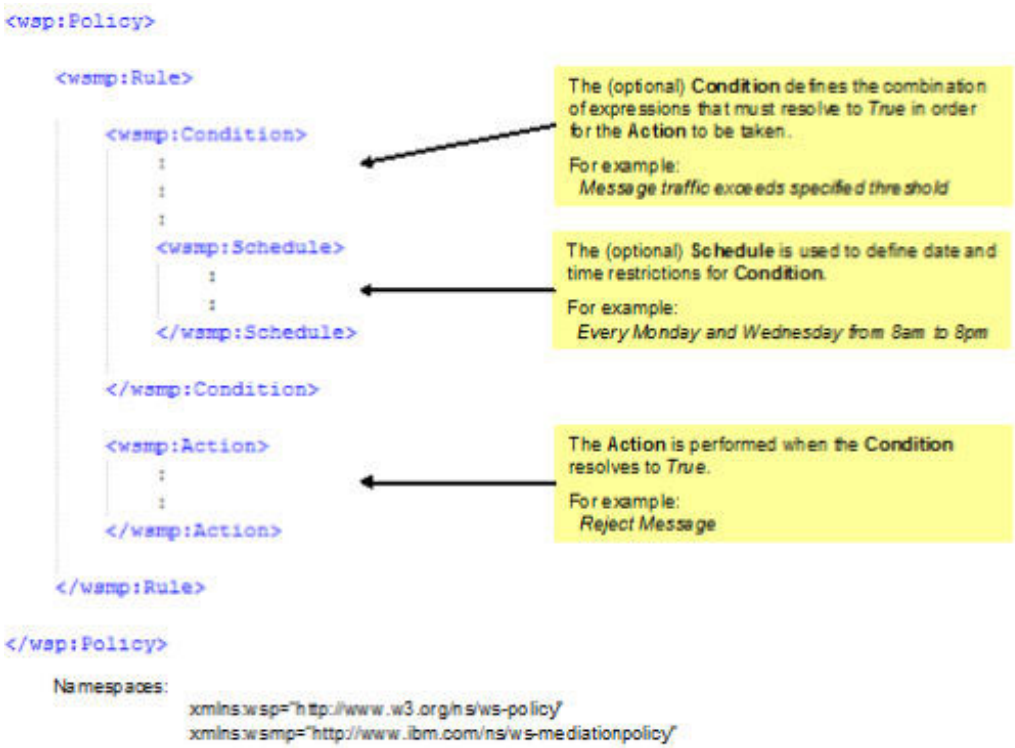


Figure 3. Présentation d'une structure de règle

PolicyAttachment

Le rôle du document PolicyAttachment consiste à associer un ensemble de règles WS-Policy à un point de connexion de service spécifique pour une application comme un point de connexion de services Web.

Par exemple, les plateformes de services Web peuvent prendre en charge des points de connexion basés sur des :

- éléments WSDL Element URI 1.1
- éléments WS-Addressing

La syntaxe est définie dans la spécification WS-PolicyAttachment :

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


    </wsp:AppliesTo>
    <wsp:Policy>


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

Figure 4. Spécification WS-PolicyAttachment

WSRR expose des interfaces REST pour acquérir des pièces jointes de règles appropriées dans un modèle SLA. Les informations sur la paire consommateur-fournisseur à laquelle la règle s'applique sont transmises au bus de services d'entreprise (ESB) au format de WS-PolicyAttachment. La syntaxe est définie dans WS-PolicyAttachment : spécification des filtres de contenu de message.

La règle peut être spécifiée pour un service de fournisseurs uniquement, pour une paire consommateur-fournisseur spécifique ou pour des consommateurs anonymes. Les consommateurs anonymes fournissent un moyen de définir une règle par défaut qui ne s'applique qu'à des consommateurs pour lesquels aucune autre règle ne s'applique.

Dans la figure 4, l'objet de règle spécifique du domaine auquel la règle s'applique (le fournisseur) est contenu dans la section `<wsp:AppliesTo>`. Elle est suivie par le filtre de contexte consommateur auquel la règle s'applique (consommateur). Ensuite, dans la section `<wsp:Policy>`, la ou les règles sont déclarées ou référencées.

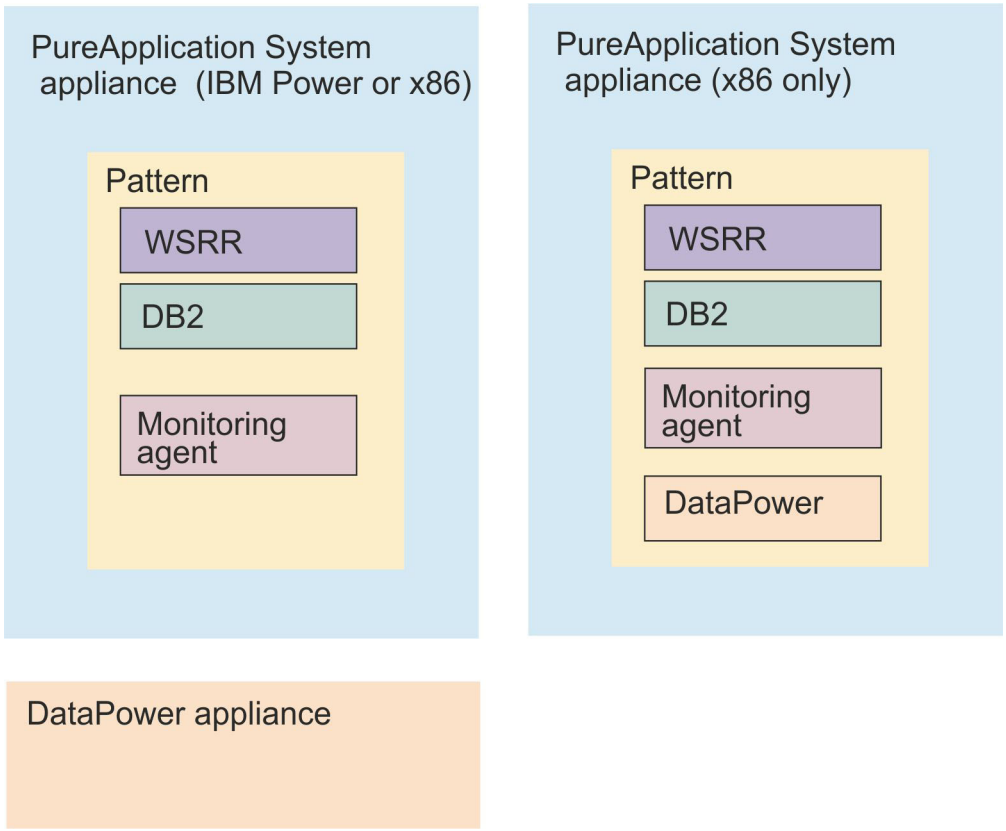
Chapitre 2. Présentation du modèle

Le modèle IBM SOA Policy Gateway Pattern est un ensemble de modèles de système virtuel fournissant un point d'application de règles, un point d'administration de règles et un point de surveillance de règles.

Vous pouvez installer le modèle IBM SOA Policy Gateway Pattern sur un dispositif IBM PureApplication dans une architecture de type IBM Power ou x86.

Le point d'administration des règles est fourni par des canevas de système virtuel qui mettent à disposition WSRR dans une architecture multiniveau, en fournissant un environnement de production et de transfert. Le point d'application de règles peut être fourni par un dispositif WebSphere DataPower. Sur plateforme x86, en revanche, votre système PureApplication peut déployer une image DataPower virtuelle. Dans l'un ou l'autre cas, un domaine est créé durant le déploiement du modèle de système virtuel. Le point de contrôle de règles est fourni par une extension de surveillance du service de surveillance PureApplication System.

Le diagramme suivant illustre les fonctionnalités dérivées du modèle IBM SOA Policy Gateway Pattern



Il existe des exemples de règles dans de nombreux, si ce n'est pas dans tous les environnements avec des architectures orientées vers le service (SOA, Services Oriented Architecture). Les producteurs et consommateurs de services s'accordent sur les fonctions, les performances et les caractéristiques du service pendant la

phase de conception. Pour implémenter ces accords, vous pouvez utiliser des définitions de niveau de service (SLD) et des accords sur les niveaux de service (SLA). A l'aide du modèle, définissez efficacement des règles pour des SLD et des SLA par un moyen administré, défini et gouverné. Les types de règles utilisés dans ce modèle inclut les règles suivantes :

- **Règles de médiation** -
  - Rejection (Rejet) - Rejette ou régule des requêtes qui arrivent à un rythme supérieur à celui défini.
  - Logging (Consignation) - Crée un message de journal avec le point d'application de règles lorsqu'un service est appelé.
  - Transformation.
  - Validation - Valide l'appel de service par rapport à la définition de service.
  - Routing (Routage) - Basé sur le message, achemine vers un noeud final spécifique.
- **Règles de sécurité** : L'exemple illustre l'application de règles de sécurité des contrôles d'accès XACML. Ces règles ne sont pas gouvernées au sein du point d'administration des règles pour le moment.
- **Règles de surveillance** : Vous pouvez définir des règles de surveillance sur les déploiements PureApplication System.

IBM SOA Policy Gateway Pattern contient les canevas de système virtuel suivants :

- SOA Policy Gateway Basic Runtime Sample (x86 uniquement)
- SOA Policy Gateway Governance Master
- SOA Policy Gateway Basic Runtime
- SOA Policy Gateway Basic Runtime External DataPower
- SOA Policy Gateway Advanced Runtime
- SOA Policy Gateway Advanced Runtime External DataPower
- Surveillance du système pour SOA Policy Gateway Pattern 2.5 (service partagé)

Les canevas de système virtuel s'associent pour fournir un environnement de gouvernance de services multi-étapes. IBM SOA Policy Gateway Pattern offre également la possibilité de mettre à disposition plusieurs domaines DataPower configurés pour l'environnement de gouvernance au cours du déploiement du modèle.

Pour plus d'informations sur la règle SOA, voir Chapitre 1, «Présentation des règles SOA», à la page 1.

Concepts associés:

Chapitre 1, «Présentation des règles SOA», à la page 1
La gestion des règles joue un rôle déterminant dans les règles de gouvernance de manière structurée et cohérente. Les règles peuvent être utilisées pour permettre une meilleure gouvernance dans un environnement orienté service.

«SOA Policy Gateway Basic Runtime External DataPower», à la page 23
Le modèle SOA Policy Gateway Basic Runtime External DataPower est similaire au modèle Basic Runtime, mais requiert la spécification des DataPower externes lors du déploiement.

«SOA Policy Gateway Basic Runtime Sample (x86)», à la page 19
SOA Policy Gateway Basic Runtime Sample met à disposition un modèle d'exécution basique avec un exemple d'interface et d'application qui illustre les règles actuellement prises en charge dans cette version.

«SOA Policy Gateway Governance Master», à la page 20
Le modèle SOA Policy Gateway Governance Master fournit un environnement de gouvernance en cluster pour la création et la gestion de services et de règles. L'environnement est mis à disposition avec le profil d'activation de gouvernance (Governance Enablement Profile) WSRR par défaut configuré. Le profil prend en charge deux cibles de promotion : Staging et Production.

«SOA Policy Gateway Advanced Runtime External DataPower», à la page 26
Le modèle SOA Policy Gateway Advanced Runtime External DataPower est similaire au modèle Advanced Runtime, mais requiert la spécification des DataPower externes lors du déploiement.

«Surveillance du système pour SOA Policy Gateway», à la page 28
Le service partagé Surveillance du système pour SOA Policy Gateway fournit les composants de surveillance pour la passerelle SOA Policy Gateway.

Chapitre 3. Guide d'initiation à IBM SOA Policy Gateway Pattern

Ce modèle utilise WebSphere DataPower pour contrôler des messages utilisant des règles gouvernées et des définitions de service dans WSRR. Lisez les rubriques de cette section pour comprendre comment télécharger et installer le modèle, comment vérifier le modèle après l'installation, accepter les licences et les rôles utilisateur impliqués.

Téléchargement et installation des modèles

IBM SOA Policy Gateway Pattern à utiliser avec IBM PureApplication System est assemblé pour être téléchargé depuis Passport Advantage.

Avant de commencer

Vous téléchargez le modèle IBM SOA Policy Gateway Pattern vers un système temporaire, qui peut être un système Linux ou Microsoft Windows. Vous exécutez ensuite le programme d'installation sur le système temporaire afin d'installer les modèles sur IBM PureApplication System.

Assurez-vous de disposer de 16 Go d'espace disponible pour le fichier `CIQ1LML.tar.gz` (cible Power) ou `CIQ1VML.tar.gz` file (cible x86), et de 40 Go supplémentaires pour les fichiers extraits. Java™ Runtime Environment (JRE) version 6 doit également être installé avant de lancer l'installation du modèle. Vous pouvez télécharger le JRE pour Linux à partir de l'adresse suivante : http://www.ibm.com/developerworks/java/jdk/linux/download.html.

Pourquoi et quand exécuter cette tâche

IBM SOA Policy Gateway Pattern est compressé dans le fichier `CIQ1LML.tar.gz` si le système cible est de type Power, ou dans le fichier `CIQ1VML.tar.gz` si le système cible est de type x86. Cet archivage contient les fichiers d'archive virtuel ouvert (OVA), les fichiers du package de script et les fichiers de définition de modèle.

Procédure

Pour télécharger les images IBM SOA Policy Gateway Pattern à partir de Passport Advantage, procédez comme suit :

1. Accédez au site Web Passport Advantage : Passport Advantage.
2. Téléchargez le fichier archive contenant les images, les packages de script et les modèles à utiliser. Le fichier est dénommé `CIQ1LML.tar.gz` (cible Power) ou `CIQ1VML.tar.gz` (cible x86).
3. Ouvrez un terminal sous Linux ou une fenêtre d'invite de commande sous Windows pour accéder au répertoire dans lequel le fichier d'archive a été téléchargé.
4. Extrayez le contenu du fichier d'archive vers votre système de fichier local. Sous Linux, la commande d'extraction est utilisée :

```
tar xvzf fichier_archive
```

Sous Windows, utilisez un logiciel d'extraction supplémentaire pour extraire le contenu du fichier d'archive.

5. Changez pour le répertoire `installer` :

```
cd installer
```

6. Pour installer IBM SOA Policy Gateway Pattern dans le système IBM PureApplication System, exécutez le programme d'installation. Le nom de la commande est `installer.bat` sous Microsoft Windows ou `installer` sous Linux. Entrez la commande suivante : `installer -h <hôte> -u <nom_utilisateur> -p <mot_de_passe>` où `<hôte>` représente le dispositif IBM PureApplication System, et nom_utilisateur et mot_de_passe sont les données d'identification de l'administrateur cloud. Par exemple :

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

7. A l'invite du système, acceptez la licence IBM SOA Policy Gateway Pattern.
   a. Sous Microsoft Windows : après avoir accepté le contrat de licence, si une nouvelle ligne du terminal affiche `>>>`, entrez `quit()`, puis appuyez sur la touche Entrée. Répétez l'étape 7.
8. Les modèles sont importés. A mesure que chaque modèle est installé, un message s'affiche dans le programme d'installation pour indiquer que son installation s'est effectuée correctement. Par exemple :

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

Résultats

Le système charge les modèles et les scripts et créé les modèles du système virtuel.

Remarque : Si un modèle de système virtuel au niveau de version correct utilisé dans IBM SOA Policy Gateway Pattern existe déjà dans le catalogue, il n'est pas remplacé.

Que faire ensuite

Acceptez les licences dans IBM PureApplication System. Voir .

Pour valider l'installation, voir «Vérification du modèle installé».

Vérification du modèle installé

Vous pouvez vérifier que le modèle est installé correctement.

Avant de commencer

Vérifiez que toutes les étapes de «Téléchargement et installation des modèles», à la page 13 sont terminées.

Pourquoi et quand exécuter cette tâche

Après avoir installé le modèle, vous pouvez vérifier l'installation de celui-ci pour vous assurer que tous les composants sont opérants.

Procédure

Pour vérifier l'installation du modèle IBM SOA Policy Gateway Pattern, procédez comme suit :

1. Ouvrez Workload Console sur le dispositif où le modèle a été installé.
2. Vérifiez les images virtuelles en accédant à **Catalogue** > **Images virtuelles** et recherchez les éléments suivants :
   - DB2 Enterprise 10.1.0.2
   - WebSphere Service Registry and Repository 8.0.0.2
   - WebSphere DataPower X152 Virtual Edition (systèmes x86 uniquement)
3. Accédez à **Catalogue** > **Packages de script**, puis recherchez :
   - SOA Policy Gateway 2.5.0.0 - domaine DataPower
   - SOA Policy Gateway 2.5.0.0 - DataPower Monitoring (x86 uniquement)
   - SOA Policy Gateway 2.5.0.0 - External DataPower Monitoring
   - SOA Policy Gateway 2.5.0.0 - Promotion
   - SOA Policy Gateway 2.5.0.0 - Sample (x86 uniquement)
   - SOA Policy Gateway 2.5.0.0 - Security
   - SOA Policy Gateway 2.5.0.0 - Add_Named_Queries
   - SOA Policy Gateway 2.5.0.0 - Tear Down

   Ces packages de script sont tous présents dans une installation qui s'est correctement effectuée.
4. Accédez à **Modèles** > **Systèmes virtuels**. Sur les systèmes x86, recherchez :
   - SOA Policy Gateway 2.5.0.0 - Advanced Runtime
   - SOA Policy Gateway 2.5.0.0 - Advanced Runtime External DataPower
   - SOA Policy Gateway 2.5.0.0 - Basic Runtime
   - SOA Policy Gateway 2.5.0.0 - Basic Runtime External DataPower
   - SOA Policy Gateway 2.5.0.0 - Basic Runtime Sample
   - SOA Policy Gateway 2.5.0.0 - Governance Master

   Sur les systèmes Power, recherchez :
   - SOA Policy Gateway 2.5.0.0 - Advanced Runtime
   - SOA Policy Gateway 2.5.0.0 - Basic Runtime
   - SOA Policy Gateway 2.5.0.0 - Governance Master

   Ces modèles sont tous présents dans une installation qui s'est correctement effectuée.
5. Accédez à **Cloud** > **Types de modèle** et recherchez l'élément suivant :
   - Surveillance du système pour SOA Policy Gateway Pattern 2.5.0.0

   Ce modèle est présent dans une installation qui s'est correctement effectuée.

Résultats

Vous avez vérifié l'installation du modèle IBM SOA Policy Gateway Pattern.

Que faire ensuite

Si votre installation est correcte, vous pouvez poursuivre en acceptant les licences (voir «Acceptation des licences»). Sinon, répétez à partir de l'étape 7 de la rubrique «Téléchargement et installation des modèles», à la page 13.

Acceptation des licences

Pour pouvoir utiliser les modèles, vous devez accepter les licences des composants nouvellement installés.

Avant de commencer

Vérifiez que toutes les étapes de «Téléchargement et installation des modèles», à la page 13 sont terminées.

Pourquoi et quand exécuter cette tâche

Avant de pouvoir utiliser une image virtuelle, vous devez accepter la licence requise pour celle-ci.

Procédure

Pour accepter les licences, procédez comme suit :

1. Ouvrez Workload Console sur le dispositif où le modèle a été installé.
2. Sélectionnez **Catalogue** > **Images virtuelles**.
3. Localisez les images suivantes dans la liste **Images virtuelles** et confirmez l'acceptation de la licence dans la sous-fenêtre des détails si vous n'avez pas cliqué sur 'Accepter' pour consulter la licence et l'accepter. Pour les systèmes x86 :
   - WebSphere DataPower XI52 Virtual Edition, Version 6.0.0.0 - Numéro de référence de l'image : XI52.6.0.0.0231528 (2013/06/16 14:14:19)
   - WebSphere Service Registry and Repository 8.0.0.2 - Numéro de référence de l'image : 201309062038
   - DB2 Enterprise 10.1.0.2 - Numéro de référence de l'image : 39
   - IBM OS Image for Red Hat Linux Systems, version 2.0.0.3 - Numéro de référence de l'image : 136

   Pour les systèmes Power :
   - WebSphere Service Registry and Repository 8.0.0.2 - Numéro de référence de l'image : 201309080001
   - DB2 Enterprise 10.1.0.2 - Numéro de référence de l'image : 50
   - IBM OS Image for AIX Systems version 2.0.0.2 - Numéro de référence de l'image : 126
4. Pour accepter une licence, cliquez sur l'image pour afficher ses détails. L'état est affiché. Cliquez sur **accept** pour le contrat de licence, puis cliquez sur l'une des licences qui doit être acceptée pour permettre l'utilisation de l'image virtuelle. L'état indique **En lecture seule** et le contrat de licence indique **Accepté** à la fin. Si une licence n'est pas acceptée, l'icône de l'image contient une case rouge barrée d'une croix.

Résultats

Vous avez accepté les licences correspondant à IBM SOA Policy Gateway Pattern.

Que faire ensuite

Si votre installation réussit et que vous avez accepté toutes les licences, vous pouvez poursuivre avec le modèle (voir la rubrique Chapitre 5, «Utilisation du IBM SOA Policy Gateway Pattern», à la page 45). Sinon, répétez-la à partir de l'étape 7 de la rubrique «Téléchargement et installation des modèles», à la page 13.

Configuration de l'accès utilisateur

Pour permettre aux utilisateurs d'accéder aux images et aux modèles du dispositif, l'administrateur du dispositif doit d'abord autoriser l'accès utilisateur. Vous pouvez soit commencer par créer les utilisateurs et ajouter les utilisateurs au groupe ou créer le premier groupe, puis créer les utilisateurs et les ajouter au groupe.

Pourquoi et quand exécuter cette tâche

Les utilisateurs administratifs, généralement l'administrateur du dispositif, peut ajouter d'autres utilisateurs pour accéder aux modèles et les administrer. Pour ce faire, ils emploient la console système.

Procédure

Pour configurer l'accès utilisateur, procédez comme suit :

1. Choisissez l'une des options suivantes pour configurer les utilisateurs et, le cas échéant, les groupes d'utilisateurs :
   - Ajoutez et configurez un utilisateur dans la fenêtre Utilisateurs de la console.
     a. Dans le menu, cliquez sur **Système** > **Utilisateurs**.
     b. Cliquez sur l'icône **Add** (Ajouter).
     c. Fournissez un nom d'utilisateur abrégé ainsi que le nom, l'adresse électronique et les mots de passe actuels de l'utilisateur et cliquez sur **OK**.
     d. Sélectionnez l'utilisateur que vous avez ajouté dans le panneau Utilisateurs pour configurer l'accès. Configurez l'accès et les actions de l'utilisateur que vous avez sélectionné.
     e. Ajoutez l'utilisateur à un ou plusieurs groupes d'utilisateurs dans la zone **Groupes d'utilisateurs**.
   - Créez un groupe d'utilisateurs.
     a. Dans le menu, cliquez sur **Système** > **Groupes d'utilisateurs**.
     b. Cliquez sur l'icône **Add** (Ajouter). Indiquez un nom et une description pour le groupe.
     c. Sélectionnez le groupe que vous avez ajouté dans le panneau Groupes d'utilisateurs pour configurer l'accès.
     d. Ajoutez des membres dans la zone **Membres du groupe** et fournissez les autorisations à appliquer au groupe.
2. Facultatif : Si vous avez déjà ajouté les images virtuelles, fournissez l'accès à celles-ci aux utilisateurs ou au groupe. Dans la console Workload Console, cliquez sur **Modèles** > **Systèmes virtuels** pour ouvrir la fenêtre des modèles de système virtuel. Sélectionnez une image virtuelle IBM SOA Policy Gateway Pattern pour afficher ses informations détaillées. Ajoutez les utilisateurs ou le groupe dans la zone **Access granted to**.

Que faire ensuite

Si vous n'avez pas encore ajouté les images virtuelles, ajoutez les images et fournissez l'accès à celles-ci aux utilisateurs ou au groupe.

Information associée:

IBM PureApplication System : Gestion des utilisateurs et des groupes

Chapitre 4. Modèles, composant et packages de script

Un modèle fournit une définition de topologie pour un déploiement reproductible pouvant être partagé. Les composants du modèle IBM SOA Policy Gateway Pattern sont les composants fonctionnels du modèle. Chaque élément représente une machine virtuelle unique.

Les modèles décrivent la fonction fournie par chaque machine virtuelle dans un système virtuel. Chaque fonction est identifiée comme un élément du modèle. Les modèles adoptent les caractéristiques des éléments auxquels ils sont associés. Par exemple, lorsqu'un composant WSRR est placé dans un modèle, qui est ensuite déployé, le résultat est une machine virtuelle comportant une instance WSRR d'exécution.

Modèles

Une fois que les images virtuelles sont chargées dans IBM PureApplication System et que l'accès est affecté aux utilisateurs, ceux-ci commencent à utiliser les modèles.

Les modèles fournissent une topologie reproductible qui peut être déployée sur un cloud. Les modèles déployés sont des systèmes virtuels exécutés dans le cloud. Les modèles, qu'ils soient prédéfinis ou créés, contiennent des composants. Certains composants sont requis pour que le modèle fonctionne lorsqu'il est déployé sur le cloud sous la forme d'un système virtuel.

SOA Policy Gateway Basic Runtime Sample (x86)

SOA Policy Gateway Basic Runtime Sample met à disposition un modèle d'exécution basique avec un exemple d'interface et d'application qui illustre les règles actuellement prises en charge dans cette version.

Le modèle SOA Policy Gateway Basic Runtime Sample est disponible uniquement sur les systèmes x86.

Le modèle SOA Policy Gateway Basic Runtime Sample comporte les composants suivants :

- Serveur autonome WSRR
- DB2 Enterprise
- DataPower

Le modèle SOA Policy Gateway Basic Runtime Sample installe un modèle d'application dans l'environnement déployé. Le modèle installe l'exemple de domaine au sein de DataPower qui implémente un service exemple, installe un exemple de WSDL et des règles jointes dans WSRR pour le service ; en outre, il fournit une application de test pour présenter la mise en application des règles. Pour plus d'informations sur le modèle d'application, voir «Modèle d'application», à la page 58. Il installe un exemple de domaine dans DataPower, installe un exemple de langage WSDL et des règles dans WSRR et présente plusieurs règles en regard d'un service.

Le diagramme suivant affiche l'exemple d'exécution basique.

Figure 5. Configuration PureApplication Server avec machine virtuelle DataPower (x86 uniquement)

Les règles mises en oeuvre incluent :

Tableau 1. Des règles incluses dans Basic Runtime avec le modèle Sample

Type de règle	**Description**
Consignation	Basée sur un ID de contexte des demandes, elle consigne la demande dans DataPower.
Acheminement	Basé sur un ID de contexte demande, il achemine la demande vers un noeud final spécifié.
Validation	Valide la requête par rapport aux implémentations de service WSDL.
Rejet	Contrôle les demandes à un service en fonction du nombre de messages avec des actions : rejet, file d'attente, etc.
Sécurité AAA	Contrôle l'accès au service à l'aide d'une autorisation d'utilisateur basée sur XACML. XACML n'est pas enregistré dans WSRR.
Réécriture de sécurité	Réécrit des éléments du message de réponse basés sur XACML. XACML n'est pas enregistré dans WSRR.

Scripts et options avancées

Le modèle requiert les scripts suivants.

Sur le composant Serveur autonome WSRR :
- SOA Policy Gateway 2.5.0.0 - Sample

Afficher les paramètres des composants et des scripts :
- «Composant DB2 Enterprise», à la page 28
- «Composant Serveur autonome WSRR», à la page 34
- «Composant DataPower», à la page 37
- «Script : SOA Policy Gateway 2.5.0.0 - Sample», à la page 40

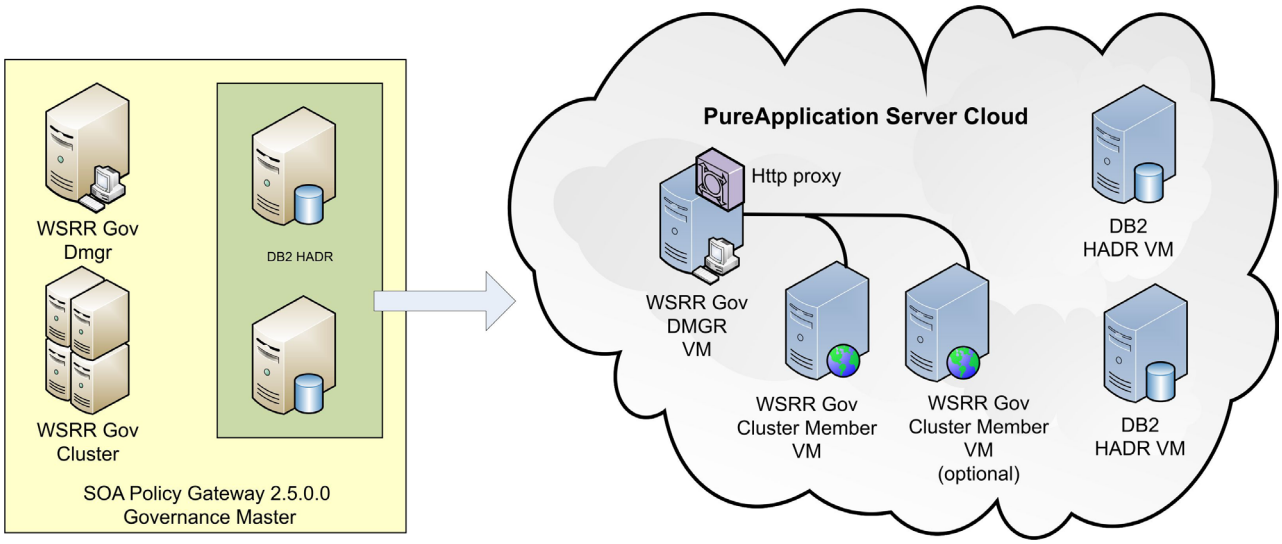
SOA Policy Gateway Governance Master

Le modèle SOA Policy Gateway Governance Master fournit un environnement de gouvernance en cluster pour la création et la gestion de services et de règles. L'environnement est mis à disposition avec le profil d'activation de gouvernance (Governance Enablement Profile) WSRR par défaut configuré. Le profil prend en charge deux cibles de promotion : Staging et Production.

Le modèle SOA Policy Gateway Governance Master requiert les composants suivants :
- HADR principal DB2
- HADR de secours DB2
- Gestionnaire de déploiement WSRR
- Noeuds personnalisés WSRR

Remarque : Le modèle Governance Master doit être déployé avant le déploiement des modèles de l'environnement d'exécution. Les paramètres utilisés pour configurer le modèle Governance Master sont utilisés par les modèles de

l'environnement d'exécution pour de configurer eux-même avec Governance Master.



Paramètres des composants

Affichez les paramètres des composants :

- «Composant principal HADR DB2 Enterprise», à la page 30
- «Composant de secours HADR DB2 Enterprise», à la page 32
- «Composant Gestionnaire de déploiement WSRR», à la page 35
- «Composant Noeuds personnalisés WSRR», à la page 36
- «Script : SOA Policy Gateway 2.5.0.0 - Security», à la page 41
- «Script : SOA Policy Gateway 2.5.0.0 - Promotion», à la page 39

Utilisation du modèle Governance comme maître de gouvernance

Le modèle SOA Policy Gateway Governance Master est déployé avec le profil GEP (Governance Enablement Profile) WSRR par défaut qui inclut deux étapes de promotion : Staging et Production. Pour plus d'informations sur le profil d'activation de gouvernance dans WSRR, voir Centre de documentation d'IBM WebSphere Service Registry and Repository version 8.0 - Profil d'activation de gouvernance. Les modèles d'exécution basique ou d'exécution avancée peuvent être déployés dans cette intégration en tant que cibles de promotion. Pour plus d'informations sur la procédure de configuration des cibles de promotion, voir «Ajout d'un environnement d'exécution supplémentaire», à la page 55.

Information associée:

Centre de documentation d'IBM WebSphere Service Registry and Repository version 8.0 - Profil d'activation de gouvernance

SOA Policy Gateway Basic Runtime

Le modèle SOA Policy Gateway Basic Runtime constitue le moyen le plus simple de fournir un environnement d'exécution SOA Policy Gateway. Il comprend deux instances DataPower (x86 uniquement), une instance WSRR autonome, une instance DB2 autonome et une instance Base OS (pour l'hébergement d'agents de surveillance DataPower).

Remarque : Cette rubrique décrit le modèle disponible sur x86. Pour le modèle IBM Power, voir «SOA Policy Gateway Basic Runtime External DataPower», à la page 23.

Le modèle SOA Policy Gateway Basic Runtime requiert les composants suivants :

- Serveur autonome WSRR
- DB2 Enterprise
- WebSphere DataPower X152 Virtual Edition
- Surveillance SOA pour DataPower (dans un composant Core OS)

Le diagramme suivant affiche la configuration du modèle SOA Policy Gateway Basic Runtime.

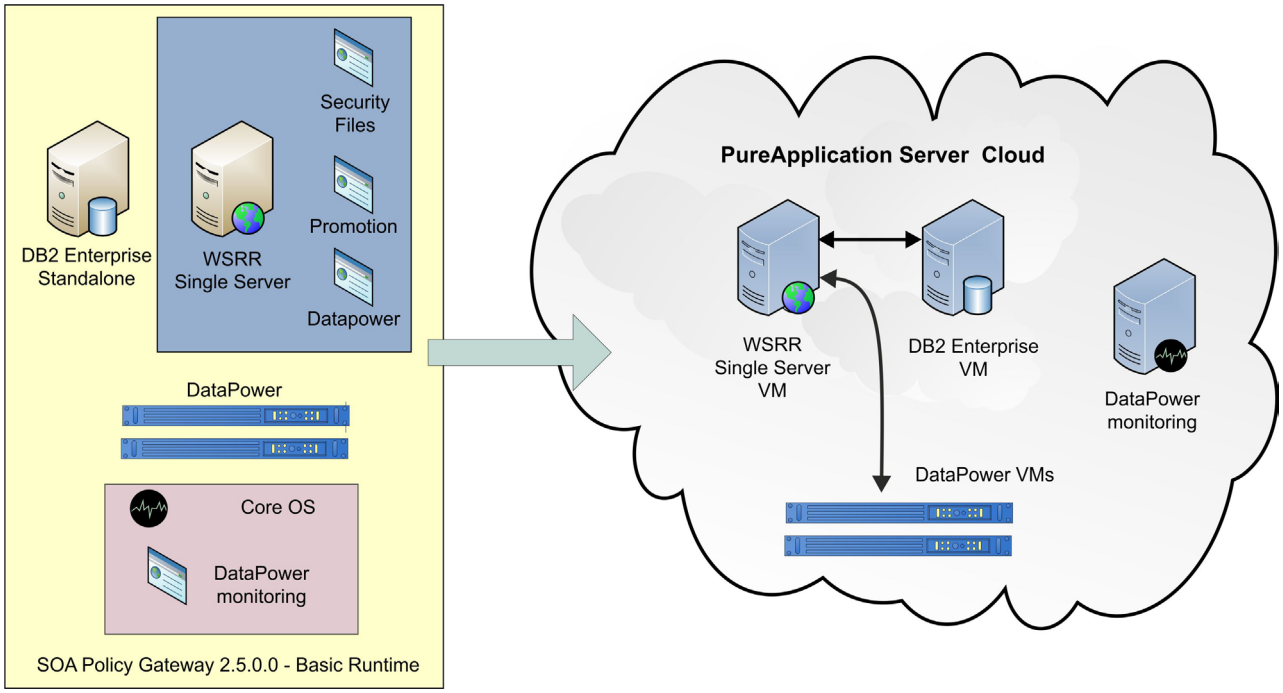


Figure 6. Configuration PureApplication Server avec machine virtuelle DataPower

Scripts et options avancées

Le modèle requiert la saisie de l'utilisateur dans les scripts suivants durant le déploiement.

Sur le composant Serveur autonome WSRR :

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

Sur le composant Core OS :

- SOA Policy Gateway 2.5.0.0 - surveillance DataPower

Afficher les paramètres des composants et des scripts :

- «Composant Serveur autonome WSRR», à la page 34
- «Composant DB2 Enterprise», à la page 28

- «Composant DataPower», à la page 37
- «Script : SOA Policy Gateway 2.5.0.0 - Security», à la page 41
- «Script : SOA Policy Gateway 2.5.0.0 - Promotion», à la page 39
- «Script : SOA Policy Gateway 2.5.0.0 - DataPower Domain», à la page 38
- «Script : SOA Policy Gateway 2.5.0.0 - DataPower Monitoring (x86 uniquement)» , à la page 41

Configuration de l'exécution basique avec le maître de gouvernance

Lorsqu'un modèle d'exécution basique est configuré avec un modèle de maître de gouvernance, les actions suivantes se produisent :

- La sécurité inter-cellule est configurée
- Le fichier `promotion.xml` du maître de gouvernance est mis à jour avec les données de déploiement issues du déploiement d'exécution basique.

Pour configurer une promotion, vous devez choisir l'une des options d'étape suivantes :

- production
- staging

Ces options s'alignent avec les niveaux fournis par le profil d'activation de gouvernance (Governance Enablement Profile) dans WSRR. Pour plus d'informations sur le profil d'activation de gouvernance dans WSRR, voir Centre de documentation d'IBM WebSphere Service Registry and Repository version 8.0 - Profil d'activation de gouvernance.

Remarque : Vous pouvez employer ce modèle pour configurer un système autonome, sans le maître de gouvernance. Pour ce faire, vous réglez les paramètres du maître de gouvernance sur «Unset» lors du déploiement du modèle. Avec ces paramètres, le script de promotion génère une erreur durant le déploiement, et le déploiement indique **failed** ; cependant, vous pouvez ignorer l'erreur.

SOA Policy Gateway Basic Runtime External DataPower

Le modèle SOA Policy Gateway Basic Runtime External DataPower est similaire au modèle Basic Runtime, mais requiert la spécification des DataPower externes lors du déploiement.

Remarque : Cette description s'applique au modèle sur les systèmes IBM Power.

Le modèle SOA Policy Gateway Basic Runtime External DataPower comporte les composants suivants :

- Serveur autonome WSRR
- DB2 Enterprise
- Surveillance SOA pour DataPower (dans un composant Core OS)

Le diagramme suivant affiche la configuration du modèle SOA Policy Gateway Basic Runtime External DataPower.

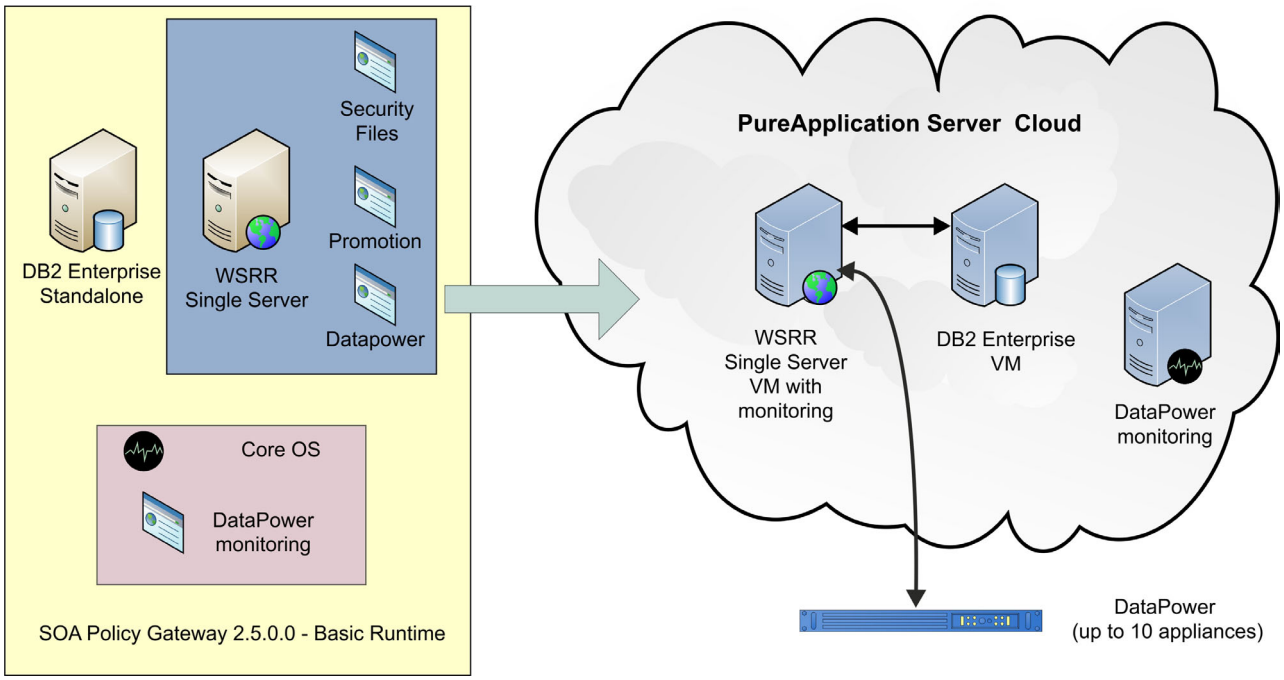


Figure 7. Configuration PureApplication Server avec dispositif DataPower

Scripts et options avancées

Le modèle requiert la saisie de l'utilisateur dans les scripts suivants durant le déploiement.

Sur le composant Serveur autonome WSRR :

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

Sur le composant Core OS :

- SOA Policy Gateway 2.5.0.0 - surveillance DataPower

Afficher les paramètres des composants et des scripts :

- «Composant Serveur autonome WSRR», à la page 34
- «Composant DB2 Enterprise», à la page 28
- «Script : SOA Policy Gateway 2.5.0.0 - Security», à la page 41
- «Script : SOA Policy Gateway 2.5.0.0 - Promotion», à la page 39
- «Script : SOA Policy Gateway 2.5.0.0 - DataPower Domain», à la page 38
- «Script : SOA Policy Gateway 2.5.0.0 - DataPower Monitoring (x86 uniquement)» , à la page 41

Configuration de l'exécution basique avec le maître de gouvernance

Lorsqu'un modèle d'exécution basique est configuré avec un modèle de maître de gouvernance, les actions suivantes se produisent :

- La sécurité inter-cellule est configurée

- Le fichier `promotion.xml` du maître de gouvernance est mis à jour avec les données de déploiement issues du déploiement d'exécution basique.

Pour configurer une promotion, vous devez choisir l'une des options d'étape suivantes :

- production
- staging

Ces options s'alignent avec les niveaux fournis par le profil d'activation de gouvernance (Governance Enablement Profile) dans WSRR. Si le profil de gouvernance est différent, «other» est alors choisi lors du changement de profil de gouvernance des maîtres de gouvernance (Governance masters). Pour plus d'informations sur le profil d'activation de gouvernance dans WSRR, voir Centre de documentation d'IBM WebSphere Service Registry and Repository version 8.0 - Profil d'activation de gouvernance.

Remarque : Vous pouvez employer ce modèle pour configurer un système autonome, sans le maître de gouvernance. Pour ce faire, vous réglez les paramètres du maître de gouvernance sur «Unset» lors du déploiement du modèle. Avec ces paramètres, le script de promotion génère une erreur durant le déploiement, et le déploiement indique **failed** ; cependant, vous pouvez ignorer l'erreur.

SOA Policy Gateway Advanced Runtime

SOA Policy Gateway Advanced Runtime inclut deux instances de serveur DB2 dans une configuration HADR, et un cluster WSRR avec un unique gestionnaire de déploiement et deux noeuds personnalisés.

Remarque : Cette rubrique décrit le modèle disponible sur x86. Pour le modèle IBM Power, voir «SOA Policy Gateway Advanced Runtime External DataPower», à la page 26.

Le modèle nécessite les pièces suivantes :

- Gestionnaire de déploiement WSRR
- Noeuds personnalisés WSRR
- HADR principal DB2
- HADR de secours DB2
- WebSphere DataPower X152 Virtual Edition
- Surveillance SOA pour DataPower (dans un composant Core OS)

Le diagramme suivant affiche la configuration d'un système d'exécution avancé.

Figure 8. Configuration PureApplication Server avec machines virtuelles DataPower

Scripts et options avancées

Le modèle requiert la saisie de l'utilisateur dans les scripts suivants durant le déploiement :

Sur le composant du gestionnaire de déploiement WSRR :

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

Sur le composant Core OS :

- SOA Policy Gateway 2.5.0.0 - surveillance DataPower

Afficher les paramètres des composants et des scripts :

- «Composant principal HADR DB2 Enterprise», à la page 30
- «Composant de secours HADR DB2 Enterprise», à la page 32
- «Composant Gestionnaire de déploiement WSRR», à la page 35
- «Composant Noeuds personnalisés WSRR», à la page 36
- «Script : SOA Policy Gateway 2.5.0.0 - Promotion», à la page 39
- «Script : SOA Policy Gateway 2.5.0.0 - DataPower Domain», à la page 38
- «Script : SOA Policy Gateway 2.5.0.0 - DataPower Monitoring (x86 uniquement)» , à la page 41

Configuration de l'exécution avancée avec un maître de gouvernance

Lorsqu'un modèle d'exécution avancée est configuré avec un modèle de maître de gouvernance, les actions suivantes se produisent :

- La sécurité inter-cellule est configurée
- Le fichier `promotion.xml` du maître de gouvernance est mis à jour avec les données issues du déploiement d'exécution avancée.

Pour configurer une promotion, vous devez choisir l'une des options d'étape suivantes :

- production
- staging

Ces options s'alignent avec les niveaux fournis par le profil d'activation de gouvernance (Governance Enablement Profile) dans WSRR. Pour plus d'informations sur le profil d'activation de gouvernance dans WSRR, voir Centre de documentation d'IBM WebSphere Service Registry and Repository version 8.0 - Profil d'activation de gouvernance.

SOA Policy Gateway Advanced Runtime External DataPower

Le modèle SOA Policy Gateway Advanced Runtime External DataPower est similaire au modèle Advanced Runtime, mais requiert la spécification des DataPower externes lors du déploiement.

Remarque : Cette description s'applique au modèle SOA Policy Gateway Advanced Runtime sur les systèmes IBM Power.

Le modèle SOA Policy Gateway Advanced Runtime External DataPower requiert les composants suivants :

- Gestionnaire de déploiement WSRR
- Noeuds personnalisés WSRR
- HADR principal DB2
- HADR de secours DB2
- Surveillance SOA pour DataPower (dans un composant Core OS)

Le diagramme suivant affiche la configuration d'un système d'exécution avancé.

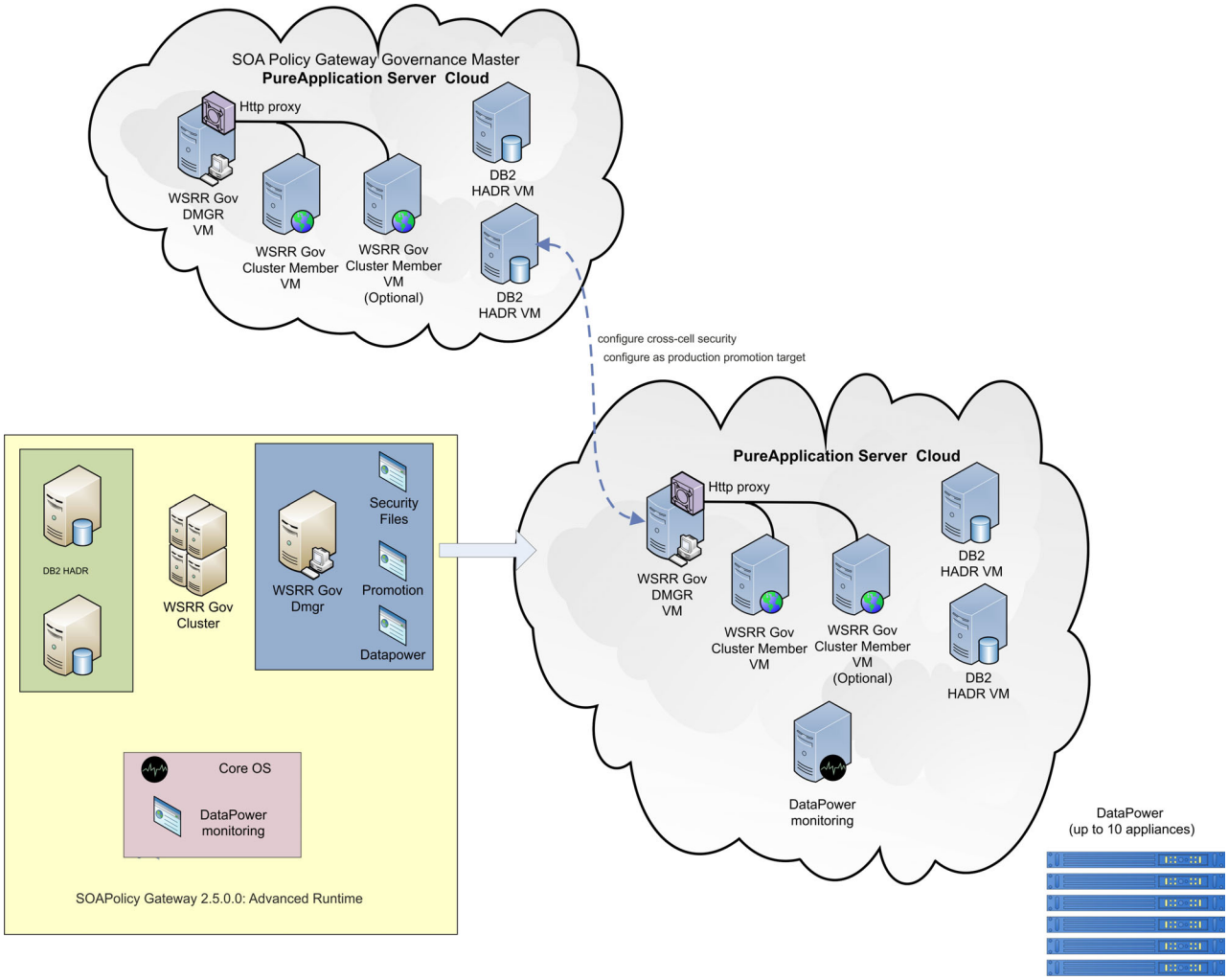


Figure 9. Configuration PureApplication Server avec dispositifs DataPower

Scripts et options avancées

Le modèle requiert la saisie de l'utilisateur dans les scripts suivants durant le déploiement.

Sur le composant du gestionnaire de déploiement WSRR :

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

Sur le composant Core OS :

- SOA Policy Gateway 2.5.0.0 - surveillance DataPower

Afficher les paramètres des composants et des scripts :

- «Composant principal HADR DB2 Enterprise», à la page 30
- «Composant de secours HADR DB2 Enterprise», à la page 32
- «Composant Gestionnaire de déploiement WSRR», à la page 35
- «Composant Noeuds personnalisés WSRR», à la page 36
- «Script : SOA Policy Gateway 2.5.0.0 - Promotion», à la page 39

- «Script : SOA Policy Gateway 2.5.0.0 - DataPower Domain», à la page 38
- «Script : SOA Policy Gateway 2.5.0.0 - DataPower Monitoring (x86 uniquement)» , à la page 41

Configuration de l'exécution avancée avec un maître de gouvernance

Lorsqu'un modèle d'exécution avancée est configuré avec un modèle de maître de gouvernance, les actions suivantes se produisent :

- La sécurité inter-cellule est configurée
- Le fichier `promotion.xml` du maître de gouvernance est mis à jour avec les données issues du déploiement d'exécution avancée.

Pour configurer une promotion, vous devez choisir l'une des options d'étape suivantes :

- production
- staging

Ces options s'alignent avec les niveaux fournis par le profil d'activation de gouvernance (Governance Enablement Profile) dans WSRR. Pour plus d'informations sur le profil d'activation de gouvernance dans WSRR, voir Centre de documentation d'IBM WebSphere Service Registry and Repository version 8.0 - Profil d'activation de gouvernance.

Service partagé

Le modèle comprend un service partagé utilisé par les modèles déployés pour fournir la surveillance.

Surveillance du système pour SOA Policy Gateway

Le service partagé Surveillance du système pour SOA Policy Gateway fournit les composants de surveillance pour la passerelle SOA Policy Gateway.

Dans les modèles d'exécution basique et d'exécution avancée, la surveillance est assurée par le service de surveillance DataPower qui s'exécute sur un composant Core OS. Le service de surveillance lui-même utilise des composants ITCAM pour SOA contenus dans le modèle System Monitoring for SOA Policy Gateway. La surveillance des instances WSRR nécessite également l'exécution du service partagé System Monitoring for WebSphere Application Server.

Suivez le lien connexe de la documentation détaillée ITCAM pour SOA.

Information associée:

Documentation ITCAM for SOA 7.2.1 (de Fix Central)

Composants

Les composants suivants comprennent le modèle IBM SOA Policy Gateway Pattern.

Composant DB2 Enterprise

Le composant DB2 Enterprise fournit certaines options de configuration.

Les paramètres configurables de l'image de système virtuel DB2 Enterprise 10.1.0.2 sont décrits dans le tableau suivant :

Tableau 2. Paramètres configurables

Nom du paramètre	Valeur par défaut	Description
Unités centrales virtuelles	1	Nombre de processeurs virtuels alloués pour la machine virtuelle représentée par cet élément.
Taille de mémoire (Mo)	2048	Taille de la mémoire allouée à cette machine virtuelle, en mégaoctets.
Groupe du propriétaire d'instance	db2iadm1	Groupe auquel le propriétaire de l'instance DB2 appartient.
Propriétaire de l'instance	db2inst1	ID du propriétaire de l'instance DB2. Cet ID utilisateur est utilisé en tant que propriétaire de l'installation de l'instance DB2 et en tant que propriétaire des bases de données et des schémas.
Mot de passe (propriétaire de l'instance)	mot de passe	Le mot de passe de l'ID utilisateur db2inst1 du système d'exploitation.
Confirmation du mot de passe	mot de passe	Vérifie le mot de passe du propriétaire de l'instance.
Groupe d'utilisateurs isolés	db2fadm1	Groupe auquel le propriétaire isolé DB2 appartient.
Utilisateur isolé	db2fenc1	ID de l'utilisateur isolé DB2. L'ID de l'utilisateur isolé permet d'exécuter des fonctions UDF (fonctions personnalisées) et des procédures mémorisées en dehors de l'espace adresse utilisé par la base de données DB2. L'utilisateur isolé est un utilisateur sous lequel les procédures mémorisées "isolées" peuvent s'exécuter avec des droits restreints du système d'exploitation.
Mot de passe (db2fenc1)		Mot de passe de l'ID utilisateur isolé
Confirmation du mot de passe		Vérifie le mot de passe de l'utilisateur isolé.
Groupe d'utilisateurs DAS	dasadm1	Groupe auquel le propriétaire DAS DB2 appartient.
Utilisateur DAS	dasusr1	L'ID de l'utilisateur du serveur d'administration DB2 exécutant le serveur d'administration DB2 sur votre système.Cet ID utilisateur est également utilisé par les outils d'interface graphique DB2 pour accomplir des tâches d'administration sur les instances de base de données et les bases de données du serveur local.
Mot de passe (utilisateur DAS)	mot de passe	Mot de passe pour l'utilisateur DAS.
Confirmation du mot de passe	mot de passe	Vérifie le mot de passe de dasusr1.

Tableau 2. Paramètres configurables (suite)

Nom du paramètre	Valeur par défaut	Description
Port du service DB2	50000	La valeur du port est verrouillée et ne peut pas être modifiée.
Création de base de données	Create-new-database	Cette valeur est verrouillée et ne peut pas être modifiée.
Nom de la nouvelle base de données	WSRR	Cette valeur est verrouillée et ne peut pas être modifiée.
Page de codes de la nouvelle base de données	UTF-8	
Territoire de la nouvelle base de données	US	
Collecte de la nouvelle base de données	SYSTEM	
Taille de page de la nouvelle base de données	32768	Cette valeur est verrouillée et ne peut pas être modifiée.
Mode de compatibilité DB2	Default	Cette valeur est verrouillée et ne peut pas être modifiée.
Configurer tous les disques brut en vue de leur utilisation par DB2	NO	
Mot de passe (superutilisateur)		Le mot de passe pour l'ID utilisateur superutilisateur. Il s'agit du mot de passe du système d'exploitation de la machine virtuelle représentée par ce composant dans le modèle.
Confirmation du mot de passe		Vérifie le mot de passe du superutilisateur.
Mot de passe (utilisateur virtuel)		Le mot de passe de l'ID utilisateur de l'utilisateur virtuel du système d'exploitation. Cet ID utilisateur est utilisé en tant qu'ID utilisateur non superutilisateur pour la machine virtuelle.
Confirmation du mot de passe		Vérifie le mot de passe de l'utilisateur virtuel.
Activer VNC	True	Cette valeur est verrouillée et ne peut pas être modifiée.

Composant principal HADR DB2 Enterprise

Le composant principal HADR DB2 Enterprise fournit certaines options de configuration.

Les paramètres configurables du composant principal HADR DB2 Enterprise sont décrits dans le tableau suivant :

Tableau 3. Paramètres configurables

Nom du paramètre	Valeur par défaut	Description
Unités centrales virtuelles	1	Nombre de processeurs virtuels alloués pour la machine virtuelle représentée par cet élément.

Tableau 3. Paramètres configurables (suite)

Nom du paramètre	Valeur par défaut	Description
Taille de mémoire (Mo)	2048	Taille de la mémoire allouée à cette machine virtuelle, en mégaoctets.
Groupe du propriétaire d'instance	db2iadm1	Groupe auquel le propriétaire de l'instance DB2 appartient.
Propriétaire de l'instance	db2inst1	ID du propriétaire de l'instance DB2. Cet ID utilisateur est utilisé en tant que propriétaire de l'installation de l'instance DB2 et en tant que propriétaire des bases de données et des schémas.
Mot de passe (propriétaire de l'instance)	mot de passe	Le mot de passe de l'ID utilisateur db2inst1 du système d'exploitation.
Confirmation du mot de passe	mot de passe	Vérifie le mot de passe du propriétaire de l'instance.
Groupe d'utilisateurs isolés	db2fadm1	Groupe auquel le propriétaire isolé DB2 appartient.
Utilisateur isolé	db2fenc1	ID de l'utilisateur isolé DB2. L'ID de l'utilisateur isolé permet d'exécuter des fonctions UDF (fonctions personnalisées) et des procédures mémorisées en dehors de l'espace adresse utilisé par la base de données DB2. L'utilisateur isolé est un utilisateur sous lequel les procédures mémorisées "isolées" peuvent s'exécuter avec des droits restreints du système d'exploitation.
Mot de passe (db2fenc1)		Mot de passe de l'ID utilisateur isolé
Confirmation du mot de passe		Vérifie le mot de passe de l'utilisateur isolé.
Groupe d'utilisateurs DAS	dasadm1	Groupe auquel le propriétaire DAS DB2 appartient.
Utilisateur DAS	dasusr1	L'ID de l'utilisateur du serveur d'administration DB2 exécutant le serveur d'administration DB2 sur votre système. Cet ID utilisateur est également utilisé par les outils d'interface graphique DB2 pour accomplir des tâches d'administration sur les instances de base de données et les bases de données du serveur local.
Mot de passe (utilisateur DAS)	mot de passe	Mot de passe pour l'utilisateur DAS.
Confirmation du mot de passe	mot de passe	Vérifie le mot de passe de dasusr1.
Port du service DB2	50000	La valeur du port est verrouillée et ne peut pas être modifiée.
Création de base de données	Create-new-database	Cette valeur est verrouillée et ne peut pas être modifiée.
Nom de la nouvelle base de données	WSRR	Cette valeur est verrouillée et ne peut pas être modifiée.

Tableau 3. Paramètres configurables (suite)

Nom du paramètre	Valeur par défaut	Description
Page de codes de la nouvelle base de données	UTF-8	
Territoire de la nouvelle base de données	US	
Collecte de la nouvelle base de données	SYSTEM	
Taille de page de la nouvelle base de données	32768	Cette valeur est verrouillée et ne peut pas être modifiée.
Mode de compatibilité DB2	Default	Cette valeur est verrouillée et ne peut pas être modifiée.
Configurer tous les disques brut en vue de leur utilisation par DB2	NO	
Mot de passe (superutilisateur)		Le mot de passe pour l'ID utilisateur superutilisateur. Il s'agit du mot de passe du système d'exploitation de la machine virtuelle représentée par ce composant dans le modèle.
Confirmation du mot de passe		Vérifie le mot de passe du superutilisateur.
Mot de passe (utilisateur virtuel)		Le mot de passe de l'ID utilisateur de l'utilisateur virtuel du système d'exploitation. Cet ID utilisateur est utilisé en tant qu'ID utilisateur non superutilisateur pour la machine virtuelle.
Confirmation du mot de passe		Vérifie le mot de passe de l'utilisateur virtuel.
Activer VNC	True	Cette valeur est verrouillée et ne peut pas être modifiée.

Les autres paramètres sont hérités du modèle de système virtuel de base et sont verrouillés.

Composant de secours HADR DB2 Enterprise

Le composant de secours HADR DB2 Enterprise fournit certaines options de configuration.

Tableau 4. Paramètres configurables

Nom du paramètre	Valeur par défaut	Description
Unités centrales virtuelles	1	Nombre de processeurs virtuels alloués pour la machine virtuelle représentée par cet élément.
Taille de mémoire (Mo)	2048	Taille de la mémoire allouée à cette machine virtuelle, en mégaoctets.
Groupe du propriétaire d'instance	db2iadm1	Groupe auquel le propriétaire de l'instance DB2 appartient.

Tableau 4. Paramètres configurables (suite)

Nom du paramètre	Valeur par défaut	Description
Propriétaire de l'instance	db2inst1	ID du propriétaire de l'instance DB2. Cet ID utilisateur est utilisé en tant que propriétaire de l'installation de l'instance DB2 et en tant que propriétaire des bases de données et des schémas.
Mot de passe (propriétaire de l'instance)	mot de passe	Le mot de passe de l'ID utilisateur db2inst1 du système d'exploitation.
Confirmation du mot de passe	mot de passe	Vérifie le mot de passe du propriétaire de l'instance.
Groupe d'utilisateurs isolés	db2fadm1	Groupe auquel le propriétaire isolé DB2 appartient.
Utilisateur isolé	db2fenc1	ID de l'utilisateur isolé DB2. L'ID de l'utilisateur isolé permet d'exécuter des fonctions UDF (fonctions personnalisées) et des procédures mémorisées en dehors de l'espace adresse utilisé par la base de données DB2. L'utilisateur isolé est un utilisateur sous lequel les procédures mémorisées "isolées" peuvent s'exécuter avec des droits restreints du système d'exploitation.
Mot de passe (db2fenc1)		Mot de passe de l'ID utilisateur isolé
Confirmation du mot de passe		Vérifie le mot de passe de l'utilisateur isolé.
Groupe d'utilisateurs DAS	dasadm1	Groupe auquel le propriétaire DAS DB2 appartient.
Utilisateur DAS	dasusr1	L'ID de l'utilisateur du serveur d'administration DB2 exécutant le serveur d'administration DB2 sur votre système.Cet ID utilisateur est également utilisé par les outils d'interface graphique DB2 pour accomplir des tâches d'administration sur les instances de base de données et les bases de données du serveur local.
Mot de passe (utilisateur DAS)	mot de passe	Mot de passe pour l'utilisateur DAS.
Confirmation du mot de passe	mot de passe	Vérifie le mot de passe de dasusr1.
Port du service DB2	50000	La valeur du port est verrouillée et ne peut pas être modifiée.
Création de base de données	Create-new-database	Cette valeur est verrouillée et ne peut pas être modifiée.
Nom de la nouvelle base de données	WSRR	Cette valeur est verrouillée et ne peut pas être modifiée.
Page de codes de la nouvelle base de données	UTF-8	
Territoire de la nouvelle base de données	US	

Tableau 4. Paramètres configurables (suite)

Nom du paramètre	Valeur par défaut	Description
Collecte de la nouvelle base de données	SYSTEM	
Taille de page de la nouvelle base de données	32768	Cette valeur est verrouillée et ne peut pas être modifiée.
Mode de compatibilité DB2	Default	Cette valeur est verrouillée et ne peut pas être modifiée.
Configurer tous les disques brut en vue de leur utilisation par DB2	NO	
Mot de passe (superutilisateur)		Le mot de passe pour l'ID utilisateur superutilisateur. Il s'agit du mot de passe du système d'exploitation de la machine virtuelle représentée par ce composant dans le modèle.
Confirmation du mot de passe		Vérifie le mot de passe du superutilisateur.
Mot de passe (utilisateur virtuel)		Le mot de passe de l'ID utilisateur de l'utilisateur virtuel du système d'exploitation. Cet ID utilisateur est utilisé en tant qu'ID utilisateur non superutilisateur pour la machine virtuelle.
Confirmation du mot de passe		Vérifie le mot de passe de l'utilisateur virtuel.
Activer VNC	True	Cette valeur est verrouillée et ne peut pas être modifiée.

Les autres paramètres sont hérités du modèle de système virtuel de base et sont verrouillés.

Composant Serveur autonome WSRR

Le composant Serveur autonome WSRR fournit certaines options de configuration.

Les paramètres configurables du composant Serveur autonome WSRR sont décrits dans le tableau suivant :

Tableau 5. Paramètres configurés

Nom du paramètre	Valeur par défaut	Description
Unités centrales virtuelles	1	Nombre de processeurs virtuels alloués pour la machine virtuelle représentée par cet élément.
Taille de mémoire (Mo)	4096	Taille de la mémoire allouée à cette machine virtuelle, en mégaoctets.

Tableau 5. Paramètres configurés (suite)

Nom du paramètre	Valeur par défaut	Description
Nom de la cellule	L'une des valeurs suivantes : • SOAPolicySampleCell (canevas de modèle d'exécution basique) • SOAPolicyBasicCell (modèle d'exécution basique) • SOAPolicyBasicCell (modèle DataPower externe d'exécution basique)	
Nom du noeud	L'une des valeurs suivantes : • SOAPolicySampleNode (canevas de modèle d'exécution basique) • SOAPolicyBasicNode (modèle d'exécution basique) • SOAPolicyBasicNode (modèle DataPower externe d'exécution basique)	
Mot de passe (superutilisateur)		Le mot de passe pour l'ID utilisateur superutilisateur. Il s'agit du mot de passe du système d'exploitation de la machine virtuelle représentée par ce composant dans le modèle.
Confirmation du mot de passe		Vérifie l'entrée de l'utilisateur pour Mot de passe (superutilisateur).
Nom d'utilisateur administrateur WebSphere	virtuser	Nom d'utilisateur administrateur WebSphere Application Server. Vous ne devez pas modifier cette valeur.
Mot de passe de l'administrateur WebSphere		Mot de passe de l'utilisateur administrateur de WebSphere Application Server.
Confirmation du mot de passe		Vérifie l'entrée de l'utilisateur pour le mot de passe administrateur WebSphere Application Server.
Activer VNC	True	Cette valeur est verrouillée et ne peut pas être modifiée.

Composant Gestionnaire de déploiement WSRR

Le composant Gestionnaire de déploiement WSRR fournit certaines options de configuration.

Les paramètres configurables du composant Gestionnaire de déploiement WSRR sont décrits dans le tableau suivant :

Tableau 6. Paramètres configurables

Nom du paramètre	Valeur par défaut	Description
Unités centrales virtuelles	1	Nombre de processeurs virtuels alloués pour la machine virtuelle représentée par cet élément.
Taille de mémoire (Mo)	2048	Taille de la mémoire allouée à cette machine virtuelle, en mégaoctets.

Tableau 6. Paramètres configurables (suite)

Nom du paramètre	Valeur par défaut	Description
Nom de la cellule	SOAPolicyAdvancedCell	Nom de cellule pour le modèle d'exécution avancée Advanced Runtime.
Nom du noeud	SOAPolicyAdvancedNode	Nom de noeud pour le noeud résidant sur la machine virtuelle Gestionnaire de déploiement dans le modèle d'exécution avancée Advanced Runtime.
Mot de passe (superutilisateur)		Le mot de passe pour l'ID utilisateur superutilisateur. Il s'agit du mot de passe du système d'exploitation de la machine virtuelle représentée par ce composant dans le modèle.
Confirmation du mot de passe		Vérifie l'entrée de l'utilisateur pour Mot de passe (superutilisateur).
Nom d'utilisateur administrateur WebSphere	virtuser	Nom d'utilisateur administrateur WebSphere Application Server. Vous ne devez pas modifier cette valeur.
Mot de passe de l'administrateur WebSphere		Mot de passe de l'utilisateur administrateur de WebSphere Application Server.
Confirmation du mot de passe		Vérifie l'entrée de l'utilisateur pour le mot de passe administrateur WebSphere Application Server.
Activer VNC	True	Cette valeur est verrouillée et ne peut pas être modifiée.

Composant Noeuds personnalisés WSRR

Le composant Noeuds personnalisés WSRR fournit certaines options de configuration.

Les paramètres configurables du composant Noeuds personnalisés WSRR sont décrits dans le tableau suivant :

Tableau 7. Paramètres configurables

Nom du paramètre		Description
Unités centrales virtuelles	2	Nombre de processeurs virtuels alloués pour la machine virtuelle représentée par cet élément.
Taille de mémoire (Mo)	4096	Taille de la mémoire allouée à cette machine virtuelle, en mégaoctets.
Nom de la cellule	CloudBurstCell	La valeur du nom de cellule dans la configuration du composant Noeuds personnalisés est ignoré.
Nom du noeud	SOAPolicyAdvancedNode	Nom de noeud pour le noeud résidant sur la machine virtuelle du noeud personnalisé dans le modèle d'exécution avancée Advanced Runtime.

Tableau 7. Paramètres configurables (suite)

Nom du paramètre		Description
Mot de passe (superutilisateur)		Le mot de passe pour l'ID utilisateur superutilisateur. Il s'agit du mot de passe du système d'exploitation de la machine virtuelle représentée par ce composant dans le modèle.
Confirmation du mot de passe		Vérifie l'entrée de l'utilisateur pour le Mot de passe (superutilisateur).
Nom d'utilisateur administrateur WebSphere	virtuser	Nom d'utilisateur administrateur de l'environnement WebSphere Application Server. Vous ne devez pas modifier cette valeur.
Mot de passe de l'administrateur WebSphere		Mot de passe de l'utilisateur administrateur de l'environnement WebSphere Application Server.
Confirmation du mot de passe		Vérifie l'entrée de l'utilisateur pour le mot de passe administrateur WebSphere Application Server.
Activer VNC	True	Cette valeur est verrouillée et ne peut pas être modifiée.

Composant DataPower

Le composant DataPower possède des options de configuration.

Les paramètres configurables de l'image de système virtuel DataPower sont décrits dans le tableau suivant :

Tableau 8. Paramètres configurés

Nom du paramètre	Valeur par défaut	Description
Unités centrales virtuelles	4	Nombre de processeurs virtuels alloués pour la machine virtuelle représentée par cet élément.
Taille de mémoire (Mo)	4096	Taille de la mémoire allouée à cette machine virtuelle, en mégaoctets.
mot de passe d'administrateur		Mot de passe pour l'administrateur DataPower.
Confirmation du mot de passe		Vérifie l'entrée de l'utilisateur pour le mot de passe de l'administrateur.
Activer SSH	True	Active SSH (pour l'utilisation de l'interface de ligne de commande de DataPower).
Port SSH	22	Port de communication SSH.
Activer l'interface XML Management	True	Active l'interface XML Management. Une fois activée, cette interface permet à des administrateurs d'envoyer les requêtes de statut et de configuration au dispositif DataPower via une interface SOAP standard.
Port de l'interface de gestion XML	5550	Port de l'interface de gestion XML.

Tableau 8. Paramètres configurés (suite)

Nom du paramètre	Valeur par défaut	Description
Activer le service de gestion Web	True	Active l'interface WebGUI dans le cadre des interactions avec le dispositif DataPower.
Port du service de gestion Web	9090	Port de l'interface Web.
Répertoire RAID	raid0	Répertoire dans lequel vous pouvez accéder aux fichiers dans le stockage de données auxiliaire DataPower.

Packages de script

Sept packages de script sont fournis avec le modèle IBM SOA Policy Gateway Pattern.

Les packages de script incluent dans ce modèle sont les suivants :

- SOA Policy Gateway 2.5.0.0 - domaine DataPower
- SOA Policy Gateway 2.5.0.0 - Promotion
- SOA Policy Gateway 2.5.0.0 - Samples
- SOA Policy Gateway 2.5.0.0 - Security
- SOA Policy Gateway 2.5.0.0 - domaine DataPower
- SOA Policy Gateway 2.5.0.0 - Add Named Queries
- SOA Policy Gateway 2.5.0.0 - Tear Down

Les scripts Add Named Queries et Tear Down ne contiennent aucun paramètre personnalisable.

Script : SOA Policy Gateway 2.5.0.0 - DataPower Domain

Le script DataPower Domain met à disposition le domaine DataPower durant le déploiement. Le script configure la connexion entre la phase d'exécution de WSRR et jusqu'à 10 dispositifs (virtuels) de DataPower.

Paramètres

Tableau 9. Paramètres configurables

Nom du paramètre	Valeur par défaut	Description
DataPower_hostname	*Cette valeur est verrouillée et ne peut pas être modifiée.*	Nom de hôte nécessaire à la surveillance de l'instance ou du dispositif DataPower.
DataPower_admin_id	*Cette valeur est verrouillée et ne peut pas être modifiée.*	ID de l'utilisateur administrateur de cette instance ou de ce dispositif.
DataPower_XML_mgmt_port	*Cette valeur est verrouillée et ne peut pas être modifiée.*	Port utilisé pour les communications avec l'interface XML Management dans l'instance ou le dispositif DataPower.
DataPower_admin_password	*Cette valeur est verrouillée et ne peut pas être modifiée.*	Mot de passe de l'ID utilisateur administrateur.
Confirmation du mot de passe	*Cette valeur est verrouillée et ne peut pas être modifiée.*	Répétez le mot de passe pour l'ID de l'utilisateur administrateur.

Tableau 9. Paramètres configurables (suite)

Nom du paramètre	Valeur par défaut	Description
DataPower2_hostname	*Cette valeur est verrouillée et ne peut pas être modifiée.*	
DataPower2_admin_id	*Cette valeur est verrouillée et ne peut pas être modifiée.*	
DataPower2_XML_mgmt_port	*Cette valeur est verrouillée et ne peut pas être modifiée.*	
DataPower2_admin_password	*Cette valeur est verrouillée et ne peut pas être modifiée.*	
Confirmation du mot de passe	*Cette valeur est verrouillée et ne peut pas être modifiée.*	
...		...
DataPower10_hostname	*Cette valeur est verrouillée et ne peut pas être modifiée.*	
DataPower10_admin_id	*Cette valeur est verrouillée et ne peut pas être modifiée.*	
DataPower10_XML_mgmt_port	*Cette valeur est verrouillée et ne peut pas être modifiée.*	
DataPower10_admin_password	*Cette valeur est verrouillée et ne peut pas être modifiée.*	
Confirmation du mot de passe	*Cette valeur est verrouillée et ne peut pas être modifiée.*	
New_DataPower_domain	La valeur par défaut dépend du type de modèle : • SOAPolicyAdvancedRuntime • SOAPolicyBasicRuntime	Nouveau nom de domaine à créer pour chaque dispositif ou instance DataPower. Il ne doit pas correspondre à un domaine existant sinon le package de script échoue ou quitte. La valeur ne peut pas contenir d'espace.
Remove_security_files	True	Vous pouvez ignorer ce paramètre destiné à l'assistance technique.

Script : SOA Policy Gateway 2.5.0.0 - Promotion

Le script Promotion permet à un modèle d'exécution basique ou avancé d'être intégré à un modèle SOA Policy Gateway Governance Master prédéployé. Il établit une sécurité inter-cellule entre la phase Runtime et le modèle Governance, tout en configurant éventuellement une promotion WSRR dans la maître de gouvernance.

Paramètres

Tableau 10. Paramètres configurables

Nom du paramètre	Valeur par défaut	Description
WSRR_GOV_DMGR_hostname		Nom d'hôte de Dmgr pour le cluster WSRR.
WSRR_GOV_DMGR_cellname	SOAPolicyGMCell	Nom de cellule du cluster WSRR.
WSRR_GOV_admin_user	virtuser	ID administrateur pour la cellule Governance de WSRR.
WSRR_GOV_admin_password		Mot de passe de l'ID administrateur pour la cellule Governance de WSRR.

Tableau 10. Paramètres configurables (suite)

Nom du paramètre	Valeur par défaut	Description
Confirmation du mot de passe		Vérifie l'entrée de l'utilisateur pour WSRR_GOV_admin_password.
Promotion_environment		Doit avoir la valeur staging, production ou Unset. Ces valeurs sont sensibles à la casse et doivent correspondre parfaitement.
LTPA_key_password		Une clé LTPA est exportée et utilisée au cours de l'exécution du package de script. La clé LTPA est issue de Governance Master et utilisée dans toutes les cellules dans l'environnement de promotion. Il s'agit du mot de passe utilisé lors de l'exportation de cette clé LTPA.
Confirmation du mot de passe		Vérifie l'entrée de l'utilisateur pour LTPA_key_password.

Script : SOA Policy Gateway 2.5.0.0 - Sample

Le script Sample configure les paramètres du modèle d'application à utiliser avec le modèle SOA Policy Gateway Basic Runtime Sample .

Paramètres

Aucun de ces paramètres ne peut être défini par l'utilisateur.

Tableau 11. Paramètres configurables

Nom du paramètre		Description
SCP_host	*Cette valeur est verrouillée et ne peut pas être modifiée.*	
SCP_user	*Cette valeur est verrouillée et ne peut pas être modifiée.*	
SCP_password	*Cette valeur est verrouillée et ne peut pas être modifiée.*	
Confirmation du mot de passe	*Cette valeur est verrouillée et ne peut pas être modifiée.*	
SCP_zip_location	*Cette valeur est verrouillée et ne peut pas être modifiée.*	
CLIENT_PUBLIC_KEY_file	*Cette valeur est verrouillée et ne peut pas être modifiée.*	
CLIENT_PUBLIC _KEY_password	*Cette valeur est verrouillée et ne peut pas être modifiée.*	
Confirmation du mot de passe		
CLIENT_PRIVATE_KEY_file	*Cette valeur est verrouillée et ne peut pas être modifiée.*	
CLIENT_PRIVATE_KEY_password	*Cette valeur est verrouillée et ne peut pas être modifiée.*	
Confirmation du mot de passe		

Tableau 11. Paramètres configurables (suite)

Nom du paramètre		Description
CLI_FILE_file	*Cette valeur est verrouillée et ne peut pas être modifiée.*	
Confirmation du mot de passe	*Cette valeur est verrouillée et ne peut pas être modifiée.*	
DataPower_hostname	*Cette valeur est verrouillée et ne peut pas être modifiée.*	Nom d'hôte de l'instance DataPower.
DataPower_XML_mgmt_port	*Cette valeur est verrouillée et ne peut pas être modifiée.*	Port utilisé pour l'interface de gestion XML DataPower.
DataPower_admin_id	*Cette valeur est verrouillée et ne peut pas être modifiée.*	ID utilisateur de l'administrateur disposant des droits appropriés pour utiliser l'interface de gestion XML.
DataPower_admin_password	*Cette valeur est verrouillée et ne peut pas être modifiée.*	Mot de passe pour DataPower_admin_id.
Confirmation du mot de passe	*Cette valeur est verrouillée et ne peut pas être modifiée.*	Vérifie l'entrée de l'utilisateur pour DataPower_admin_password.
SOAPolicySample_DataPower_domain	*Cette valeur est verrouillée et ne peut pas être modifiée.*	Exemple de nom de domaine. Il ne doit pas correspondre à un domaine existant de l'instance DataPower.
SamplePolicySample_starting_port	*Cette valeur est verrouillée et ne peut pas être modifiée.*	L'application nécessite 5 ports libres qui sont utilisés en séquence à partir de cette valeur. Par exemple, si la valeur est 62000, les ports 62000-62004 sont utilisés. Le script ne vérifie pas la disponibilité des ports.
LDAP_hostname	*Cette valeur est verrouillée et ne peut pas être modifiée.*	Nom d'hôte du port autonome WSRR sur lequel un serveur LDAP est également hébergé.
LDAP_port	*Cette valeur est verrouillée et ne peut pas être modifiée.*	Port destiné au serveur LDAP.
LDAP_password	*Cette valeur est verrouillée et ne peut pas être modifiée.*	Mot de passe utilisé lors de la liaison avec LDAP_DN.
Confirmation du mot de passe	*Cette valeur est verrouillée et ne peut pas être modifiée.*	Vérifie l'entrée de l'utilisateur pour LDAP_password.
LDAP_DN	*Cette valeur est verrouillée et ne peut pas être modifiée.*	Nom distinctif utilisé pour la liaison à LDAP.

Script : SOA Policy Gateway 2.5.0.0 - Security

Le script Security copie les informations de sécurité (certificats et autres) entre les systèmes DataPower et WSRR dans le modèle.

Les paramètres de configuration des fichiers du script de sécurité sont destinés à l'assistance technique. Vous devez conserver leurs valeurs par défaut.

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

Le script DataPower Monitoring indique les paramètres de connexion pour le service partagé de surveillance DataPower. L'agent et les collecteurs de données ITCAM DataPower s'exécutent dans le composant Core OS.

Paramètres

Le service de surveillance peut contrôler jusqu'à 10 dispositifs virtuels DataPower.

Tableau 12. Paramètres configurables

Nom du paramètre	Valeur par défaut	Description
DataPower1_hostname		Nom de hôte nécessaire à la surveillance du dispositif virtuel DataPower.
DataPower1_admin_id	admin	ID de l'utilisateur administrateur de ce dispositif virtuel.
DataPower1_XML_mgmt_port	5550	Port utilisé pour les communications avec l'interface XML Management dans le dispositif virtuelDataPower.
DataPower1_admin_password		Mot de passe de l'ID utilisateur administrateur.
Confirmation du mot de passe		Répétez le mot de passe pour l'ID de l'utilisateur administrateur.
DataPower2_hostname		
DataPower2_admin_id	admin	
DataPower2_XML_mgmt_port	5550	
DataPower2_admin_password		
Confirmation du mot de passe		
...		...
DataPower10_hostname		
DataPower10_admin_id	admin	
DataPower10_XML_mgmt_port	5550	
DataPower10_admin_password		
Confirmation du mot de passe		

Script : SOA Policy Gateway 2.5.0.0 - Surveillance DataPower externe

Le script DataPower Monitoring indique les paramètres de connexion pour le service partagé de surveillance DataPower. L'agent et les collecteurs de données ITCAM DataPower s'exécutent dans le composant Core OS.

Paramètres

Le service de surveillance peut contrôler jusqu'à 10 dispositifs DataPower.

Tableau 13. Paramètres configurables

Nom du paramètre	Valeur par défaut	Description
DataPower1_hostname		Nom de hôte nécessaire à la surveillance du dispositif DataPower.
DataPower1_admin_id	admin	ID de l'utilisateur administrateur de ce dispositif.
DataPower1_XML_mgmt_port	5550	Port utilisé pour les communications avec l'interface XML Management dans le dispositif DataPower.

Tableau 13. Paramètres configurables (suite)

Nom du paramètre	Valeur par défaut	Description
DataPower1_admin_password		Mot de passe de l'ID utilisateur administrateur.
Confirmation du mot de passe		Répétez le mot de passe pour l'ID de l'utilisateur administrateur.
DataPower2_hostname		
DataPower2_admin_id	admin	
DataPower2_XML_mgmt_port	5550	
DataPower2_admin_password		
Confirmation du mot de passe		
...		...
DataPower10_hostname		
DataPower10_admin_id	admin	
DataPower10_XML_mgmt_port	5550	
DataPower10_admin_password		
Confirmation du mot de passe		

Chapitre 5. Utilisation du IBM SOA Policy Gateway Pattern

Le modèle IBM SOA Policy Gateway Pattern fournit les définitions de modèle permettant de répéter le déploiement. Ces rubriques décrivent la procédure de déploiement des modèles.

Dans le cadre du processus de déploiement, configurez les paramètres de l'élément. Pour plus d'informations, voir «Déploiement des modèles», à la page 47. Les modèles sont décrits dans Chapitre 4, «Modèles, composant et packages de script», à la page 19.

Tâches associées:

Chapitre 3, «Guide d'initiation à IBM SOA Policy Gateway Pattern», à la page 13
Ce modèle utilise WebSphere DataPower pour contrôler des messages utilisant des règles gouvernées et des définitions de service dans WSRR. Lisez les rubriques de cette section pour comprendre comment télécharger et installer le modèle, comment vérifier le modèle après l'installation, accepter les licences et les rôles utilisateur impliqués.

Planification de la configuration du modèle et prérequis des modèles

Le modèle IBM SOA Policy Gateway Pattern offre un moyen de mettre à disposition rapidement et de manière fiable un environnement permettant d'administrer des définitions et des règles de service et de mettre en application des règles. Le déploiement du modèle commence avec le maître de gouvernance suivi du modèle d'exécution.

Préparation et déploiement du modèle IBM SOA Policy Gateway Pattern

- Si vous utilisez un dispositif DataPower externe, préparez-le pour l'administration à distance. Pour plus d'informations, voir «Configuration d'un dispositif DataPower pour les modèles IBM SOA Policy Gateway Pattern», à la page 46.

Déployez le modèle de maître de gouvernance :

1. Déployez un modèle SOA Policy Gateway Governance Master. Attendez que le déploiement soit terminé avant de déployer des modèles d'exécution. Pour plus d'informations, voir «Déploiement du modèle Governance Master», à la page 50.

Déployez les modèles d'exécution :

1. Déterminez le type de modèle d'exécution requis : basique avec un environnement autonome ou avancé avec un environnement de clusters.
2. Déterminez le nombre d'instances ou de dispositifs DataPower requis par vos modèles d'exécution.

   Les modèles comportant DataPower possède deux instances DataPower par défaut. Vous pouvez configurer jusqu'à 10 instances DataPower. Pour plus d'informations, voir «Ajout d'instances DataPower à un modèle», à la page 56.

   Les modèles avec DataPower externe peuvent être configurer pour fonctionner avec un maximum de 10 dispositifs DataPower. Voir «Déploiement des modèles DataPower externes basiques et avancés», à la page 57.

Remarque : Il n'est pas possible d'ajouter des instances et dispositifs DataPower supplémentaires une fois cette configuration réalisée.

3. Configurez le modèle d'exécution avec les informations du modèle de maître de gouvernance. Pour plus d'informations, voir «Informations sur le déploiement de SOA Policy Gateway Governance Master», à la page 51. Vous pouvez omettre les informations du modèle de maître de gouvernance pour déployer un système autonome, si nécessaire (l'erreur qui s'affiche lors du déploiement peut être ignorée).
4. Indiquez si le système d'exécution est utilisé en test ou en production.
5. Déployez votre modèle. Pour plus d'informations, voir «Déploiement d'un modèle d'exécution avancé», à la page 53 ou «Déploiement d'un modèle d'exécution basique», à la page 52.
6. Attendez que le déploiement complet soit terminé avant de déployer un autre environnement d'exécution.

Lorsque le déploiement des modèles d'exécution est terminé :

1. WSRR et la sécurité WebSphere peuvent être mis à jour à partir de la configuration de sécurité par défaut. Pour plus d'informations, voir «Sécurité appliquée aux modèles IBM SOA Policy Gateway Pattern».
2. Le domaine DataPower est maintenant prêt pour une configuration de passerelle. Si vous utilisez un dispositif DataPower virtuel, vous devez appliquer le dernier groupe de correctifs («Mise à jour de DataPower dans l'instance déployée», à la page 54).

Configuration d'un dispositif DataPower pour les modèles IBM SOA Policy Gateway Pattern

Exécutez les étapes suivantes de configuration de DataPower avant les scripts SOAPolicy.

Procédure

1. Ouvrez une session sur le dispositif DataPower en tant qu'administrateur.
2. Recherchez `XML Management Interface` (Interface de gestion XML).
3. Vérifiez que son état soit activé.
4. Vérifiez que les éléments suivants sont actifs et correctement sécurisés :
   - SOAP Management URI (Identificateur URI de gestion SOAP)
   - SOAP Configuration Management (Gestion des configurations SOAP)
   - SOAP Configuration Management (Gestion des configurations SOAP) (v2004)
   - AMP Endpoint (Noeud final AMP)
   - SLM Endpoint (Noeud final SLM)
   - WS-Management Endpoint (Noeud final de gestion WS)
   - WSDM Endpoint (Noeud final WSDM)
   - UDDI Subscription (Abonnement UDDI)
   - WSRR Subscription (Abonnement WSRR)

Sécurité appliquée aux modèles IBM SOA Policy Gateway Pattern

L'authentification mutuelle se produit entre les applications DataPower et les scripts des modèles Basic et Advanced. Les scripts effectuent l'échange de certificats requis. Notez que les certificats SSL par défaut fournis avec le modèle sont attribués à l'hôte qui a été utilisé pour créer le modèle.

Renforcement de la sécurité

Les images WSRR et les images WebSphere Application Server utilisées dans les modèles n'ont qu'une sécurité par défaut en place. Pour produire un environnement plus sécurisé, vous pouvez vous appuyer sur des techniques de sécurité WebSphere Application Server standard.

Voir le Centre de documentation de WebSphere Network Deployment Version 8.0 à l'aide des liens suivants :

- WebSphere Application Server, Déploiement réseau (Plateformes réparties et Windows), Version 8.0: IBM WebSphere Application Server, Déploiement réseau (plateformes réparties et Windows), Version 8.0 - Centre de documentation
- Sécurité d'application : IBM WebSphere Application Server, Déploiement réseau (plateformes réparties et Windows), Version 8.0 - Centre de documentation - Sécurisation des applications et leur environnement
- Chemins de bout en bout dédiés à la sécurité : IBM WebSphere Application Server, Déploiement réseau (plateformes réparties et Windows), Version 8.0 - Centre de documentation - Sécurisation des applications et leur environnement

Déploiement des modèles

Le déploiement des modèles avec IBM PureApplication System dans le cloud fournit un environnement de passerelle de règles SOA actif. Vous pouvez déployer les canevas prédéfinis disponibles avec les images IBM SOA Policy Gateway Pattern ou déployer les canevas que vous avez créés.

Avant de commencer

Pour déployer un modèle, vous devez d'abord avoir un modèle prédéfini ou un nouveau modèle qui est finalisé, avec tous les composants requis configurés. Vous avez besoin des informations détaillées sur l'environnement, le groupe de clouds et le groupe d'adresses IP à déployer à partir de votre profil administrateur système PureAS.

Pourquoi et quand exécuter cette tâche

Vous déployez le modèle à l'aide de la console Workload.

Procédure

Pour déployer les modèles IBM SOA Policy Gateway Pattern à exécuter dans votre cloud privé, procédez comme suit :

1. Dans la liste de modèles de la fenêtre Modèles de systèmes virtuels, sélectionnez le modèle à déployer.
2. Cliquez sur l'icône **Déployer**.
3. Complétez les zones requises pour déployer le modèle. Dans la fenêtre, entrez un nom pour le système virtuel et complétez les autres information requises. Une coche en regard de chaque élément indique qu'il ne nécessite pas de configuration supplémentaire. Vous pouvez modifier les paramètres des composants configurés, avant de déployer le modèle, en cliquant sur le nom du composant pour ouvrir l'éditeur pour celui-ci. Les machines virtuelles sont créées, dans l'ordre requis, puis démarrées.

Résultats

Le processus de déploiement crée et démarre des machines virtuelles pour les composants définis et fournit des liens vers les consoles requises. La durée de déploiement dépend de la complexité du modèle déployé. Un modèle déployé est un système virtuel ou un système mettant nouvellement à disposition l'environnement d'exécution du modèle IBM SOA Policy Gateway Pattern.

Que faire ensuite

Vous pouvez afficher l'état de votre instance, pour voir si le déploiement est terminé et commencer à l'administrer, à partir de la fenêtre Instances de système virtuel.

Information associée:

IBM PureApplication System : Gestion des modèles de système virtuel

Déploiement du service partagé de surveillance du système

Le déploiement du service partagé System Monitoring for SOA Policy Gateway fournit les composants de surveillance pour votre système virtuel.

Avant de commencer

L'administrateur système PureAS doit démarrer le service partagé System Monitoring et vous indiquez les informations de groupe et d'environnement de cloud dans lequel le service partagé démarre. Vous devez utiliser les mêmes environnement et groupe de clouds pour le déploiement du service partagé de surveillance système SOA Policy Gateway et vos modèles d'exécution et de gouvernance.

La surveillance des instances WSRR requiert également le démarrage du service partagé System Monitoring for WebSphere Application Server. Vous devez donc vous assurer que celui-ci est présent sur votre système PureAS.

Procédure

Dans la console Workload Console, procédez comme suit :

1. Cliquez sur **Instances** > **Services partagés**.
2. Vérifiez que le service System Monitoring s'exécute dans le groupe de clouds dans lequel vous allez effectuer le déploiement. S'il ne s'exécute pas, contactez votre administrateur PureAS pour le démarrer.
3. Pour activer le service partagé de surveillance DataPower :
   a. Cliquez sur **Cloud** > **Types de canevas**.
   b. Sélectionnez l'entrée **System Monitoring for SOA Policy Gateway Pattern 2.5.0.0** dans la sous-fenêtre Types de modèle.
   c. Cliquez sur **Activer** dans la zone **Statut** et attendez que la zone de statut indique **Désactiver**.
4. Pour démarrer le service partagé de surveillance WebSphere Application Server :
   a. Cliquez sur **Instances** > **Services partagés**.
   b. Cliquez le symbole plus dans la sous-fenêtre d'Instances de service partagé pour ouvrir la fenêtre Déployer le service partagé.

c. Sélectionnez **System Monitoring for WebSphere Application Server** et cliquez sur **OK**.
d. Dans la fenêtre Configurer et déployer un service partagé, indiquez si vous souhaitez que le service démarre sur des modèles précédemment déployés en sélectionnant les deux cases à cocher du bas. Cliquez sur **OK**.
e. Dans la fenêtre Déployer une application virtuelle, indiquez le **Groupe de clouds cible**, le **Groupe d'adresses IP** et le **Profil** qui sont des informations fournies par votre administrateur système PureAS. Ces informations doivent être identiques à celles de votre déploiement Systèmes virtuels.

5. Pour démarrer le service partagé de surveillance WebSphere DataPower :
   a. Cliquez sur **Instances** > **Services partagés** dans la barre de menus.
   b. Cliquez le symbole plus dans la sous-fenêtre d'Instances de service partagé pour ouvrir la fenêtre Déployer le service partagé.
   c. Sélectionnez **Surveillance du système pour WebSphere DataPower** dans la liste, puis cliquez sur **OK**.
   d. Dans la fenêtre Configurer et déployer un service partagé, indiquez si vous souhaitez que la surveillance démarre sur des modèles précédemment déployés en sélectionnant les deux cases à cocher du bas. Cliquez sur **OK**.
   e. Dans la fenêtre Déployer une application virtuelle, indiquez le **Groupe de clouds cible**, le **Groupe d'adresses IP** et le **Profil** qui sont des informations fournies par votre administrateur système PureAS. Ces informations doivent être identiques à celles de votre déploiement Systèmes virtuels.
   f. Générez et enregistrez une clé SSH si vous avez besoin d'un accès de débogage au service partagé de surveillance.
   g. Cliquez sur **OK**.

Résultats

Le service partagé System Monitoring for WebSphere DataPower est signalé comme étant en cours d'exécution. Le service partagé System Monitoring for WebSphere Application Server est signalé comme étant en cours d'exécution.

Que faire ensuite

Pour vérifier le déploiement, voir «Vérification du déploiement», à la page 55.

Déploiement du modèle d'exécution basique

Le déploiement du modèle SOA Policy Gateway Basic Runtime Sample crée une instance de système virtuel d'exécution du modèle. Ce modèle est disponible uniquement sur les systèmes x86.

Pourquoi et quand exécuter cette tâche

Le déploiement d'un modèle crée une instance de système virtuel qui s'exécute dans le cloud.

Procédure

Pour déployer le modèle SOA Policy Gateway Basic Runtime, procédez comme suit :

1. Dans Workload Console, cliquez sur **Canevas** > **Systèmes virtuels**.

2. Dans la liste Modèles de systèmes virtuels, sélectionnez **SOA Policy Gateway 2.5.0.0 - Basic Runtime Sample**.
3. Cliquez sur l'icône **Déployer**.
4. Complétez les zones requises pour déployer le modèle. Une coche en regard de chaque élément indique qu'il ne nécessite pas de configuration supplémentaire.
   a. Dans la zone **Nom du système virtuel**, entrez un nom unique pour l'instance.
   b. Développez la section **Sélectionner l'environnement**, puis entrez le **Profil** comme indiqué par votre administrateur système PureAS.
   c. Configurer les modèles virtuels. Cliquez sur **Configurer les composants virtuels**, puis cliquez sur le nom du composant pour ouvrir l'éditeur pour les composants et scripts. Indiquez **Groupe de clouds** et **Groupe IP** comme vous le conseille votre administrateur système PureAS. Reportez-vous aux rubriques suivantes pour plus de détails sur les paramètres de configuration propres au modèle et au script.

      Remarque : Par défaut, tous les mots de passe pour ce modèle sont réglés sur `mot de passe`.
      - «Composant DataPower», à la page 37
      - «Composant DB2 Enterprise», à la page 28.
      - «Composant Serveur autonome WSRR», à la page 34
      - «Script : SOA Policy Gateway 2.5.0.0 - Sample», à la page 40
5. Cliquez sur **OK** pour déployer le modèle.

Que faire ensuite

Pour vérifier le déploiement, voir «Vérification du déploiement», à la page 55.

Déploiement du modèle Governance Master

Le déploiement du modèle SOA Policy Gateway Governance Master crée une instance de système virtuel d'exécution du modèle.

Procédure

Pour déployer le modèle SOA Policy Gateway Governance Master, procédez comme suit :

1. Dans Workload Console, cliquez sur **Canevas** > **Systèmes virtuels**.
2. Dans la liste Modèles de systèmes virtuels, sélectionnez **SOA Policy Gateway 2.5.0.0 - Governance Master**.
3. Cliquez sur l'icône **Déployer**.
4. Complétez les zones pour déployer le modèle. Une coche en regard de chaque élément indique qu'il ne nécessite pas de configuration supplémentaire.
   a. Dans la zone **Nom du système virtuel**, entrez un nom unique pour l'instance.
   b. Développez la section **Sélectionner l'environnement**, puis entrez le **Profil** comme indiqué par votre administrateur système PureAS.
   c. Configurer les modèles virtuels. Cliquez sur **Configurer les composants virtuels**, puis cliquez sur le nom du composant pour ouvrir l'éditeur pour les composants et scripts. Indiquez **Groupe de clouds** et **Groupe IP** comme

vous le conseille votre administrateur système PureAS. Reportez-vous aux rubriques suivantes pour plus de détails sur les paramètres de configuration propres au modèle et au script.

- «Composant principal HADR DB2 Enterprise», à la page 30
- «Composant Gestionnaire de déploiement WSRR», à la page 35
- «Composant Noeuds personnalisés WSRR», à la page 36
- «Composant de secours HADR DB2 Enterprise», à la page 32

5. Cliquez sur **OK** pour déployer le modèle.

Que faire ensuite

Pour vérifier le déploiement, voir «Vérification du déploiement», à la page 55.

Informations sur le déploiement de SOA Policy Gateway Governance Master

Le modèle Governance Master doit être déployé avant le déploiement des modèles de l'environnement d'exécution.

Pourquoi et quand exécuter cette tâche

Les informations de déploiement issues de l'instance Governance Master sont requises comme entrées pour des valeurs de déploiement destinées aux modèles de l'environnement d'exécution.

Procédure

Pour rechercher les valeurs requises à partir de l'instance de Governance Master, procédez comme suit :

1. Accédez à **Instances** > **Virtual Systems**.
2. Sélectionnez l'instance du déploiement de Governance Master.
3. Développez **Virtual machines** (Machines virtuelles).
4. Développez la machine virtuelle nommée ***WSRRDMGR***.
5. Prenez connaissance des informations suivantes :
   - Dans la section **Hardware and network** (matériels et logiciels), prenez en note du nom d'hôte et de l'adresse IP. Le nom d'hôte est la valeur **Network interface 0**.
   - Dans la section **WebSphere configuration**, prenez en note du nom de cellule (Cell).

   Le nom d'hôte ou l'IP, le nom de cellule et le nom d'utilisateur d'administrateur WebSphere et le mot de passe utilisés pendant le déploiement de l'instance de Governance Master sont des entrées obligatoires dans les modèles SOA Policy Gateway Basic Runtime External DataPower ou SOA Policy Gateway Advanced Runtime External DataPower :
   - WSRR_GOV_DMGR_hostname
   - WSRR_GOV_DMGR_cellname
   - WSRR_GOV_admin_user
   - WSRR_GOV_admin_password

   Si vous voulez déployer un modèle d'exécution comme système autonome, vous pouvez régler ces paramètres sur «Unset». Ce paramètre fait apparaître le

déploiement comme étant en échec (**failed**) dans **Système virtuel** > **Instances** parce que le package de script de promotion échoue. Le déploiement est encore utilisable, cependant.

Déploiement d'un modèle d'exécution basique

Le déploiement d'un modèle d'exécution basique crée une instance de système virtuel d'exécution du modèle.

Avant de commencer

Complétez ce qui suit avant de déployer le modèle d'exécution basique :

- Si vous déployez un modèle d'exécution basique avec une instance DataPower externe, configurez vos dispositifs DataPower pour le modèle IBM SOA Policy Gateway Pattern ; voir «Configuration d'un dispositif DataPower pour les modèles IBM SOA Policy Gateway Pattern», à la page 46. Sur les systèmes Power, seul un dispositif DataPower externe est pris en charge.
- Récupérez les informations de déploiement de Governance Master ; voir «Informations sur le déploiement de SOA Policy Gateway Governance Master», à la page 51.

Pourquoi et quand exécuter cette tâche

Le déploiement d'un modèle crée une instance de système virtuel qui s'exécute dans le cloud.

Remarque : Si vous utilisez le profil GEP (Governance Enablement Profile), vous ne pouvez pas déployer un environnement de transfert et un environnement de production simultanément dans les modèles d'exécution. Cette limitation peut provoquer un conflit au cours du processus de configuration des propriétés de promotion. Commencez par déployer l'environnement de transfert, puis continuez par l'environnement de production.

Procédure

Pour déployer un modèle d'exécution basique, procédez comme suit :

1. Cliquez sur **Modèles** > **Systèmes virtuels**.
2. Dans la liste Modèles de systèmes virtuels, sélectionnez **SOA Policy Gateway 2.5.0.0 - Advanced Runtime External DataPower** ou **SOA Policy Gateway 2.5.0.0 - Basic Runtime**.
3. Cliquez sur l'icône **Déployer**.
4. Complétez les zones requises pour déployer le modèle. Une coche en regard de chaque élément indique qu'il ne nécessite pas de configuration supplémentaire.
   a. Dans la zone **Nom du système virtuel**, entrez un nom unique pour l'instance.
   b. Développez la section **Sélectionner l'environnement**, puis entrez le **Profil** comme indiqué par votre administrateur système PureAS.
   c. Configurer les modèles virtuels. Cliquez sur **Configurer les composants virtuels**, puis cliquez sur le nom du composant pour ouvrir l'éditeur pour les composants et scripts. Indiquez **Groupe de clouds** et **Groupe IP** comme vous le conseille votre administrateur système PureAS. Reportez-vous aux rubriques suivantes pour plus de détails sur les paramètres de configuration propres au modèle et au script.

Remarque : Pour déployer le modèle sans maître de gouvernance, entrez 'Unset' pour paramètre de nom d'hôte du maître de gouvernance. Cela a pour effet mettre en échec le package du script de promotion durant le déploiement mais n'a pas d'autres conséquences.

- «Composant DataPower», à la page 37
- «Composant DB2 Enterprise», à la page 28
- «Composant Serveur autonome WSRR», à la page 34
- «Script : SOA Policy Gateway 2.5.0.0 - Security», à la page 41
- «Script : SOA Policy Gateway 2.5.0.0 - Promotion», à la page 39
- «Script : SOA Policy Gateway 2.5.0.0 - DataPower Domain», à la page 38
- «Script : SOA Policy Gateway 2.5.0.0 - DataPower Monitoring (x86 uniquement)», à la page 41

5. Cliquez sur **OK** pour déployer le modèle.

Que faire ensuite

Pour vérifier le déploiement, voir «Vérification du déploiement», à la page 55.

Déploiement d'un modèle d'exécution avancé

Le déploiement d'un modèle d'exécution avancé crée une instance de système virtuel d'exécution du modèle.

Avant de commencer

Complétez ce qui suit avant de déployer le modèle d'exécution avancé :

- Si vous déployez un modèle d'exécution avancé avec un dispositif DataPower externe, configurez vos dispositifs DataPower à connecter au modèle. Voir «Configuration d'un dispositif DataPower pour les modèles IBM SOA Policy Gateway Pattern», à la page 46. Sur les systèmes Power, seul un dispositif DataPower externe est pris en charge.
- Récupérez les informations de déploiement de Governance Master ; voir «Informations sur le déploiement de SOA Policy Gateway Governance Master», à la page 51.

Pourquoi et quand exécuter cette tâche

Le déploiement d'un modèle crée une instance de système virtuel qui s'exécute dans le cloud.

Remarque : Si vous utilisez le profil GEP (Governance Enablement Profile), vous ne pouvez pas déployer un environnement de transfert et un environnement de production simultanément dans les modèles d'exécution. Cette limitation peut provoquer un conflit au cours du processus de configuration des propriétés de promotion. Commencez par déployer l'environnement de transfert, puis continuez par l'environnement de production.

Procédure

Pour déployer un modèle d'exécution avancé, procédez comme suit :

1. Cliquez sur **Modèles** > **Systèmes virtuels**.

2. Dans la liste Modèles de systèmes virtuels, sélectionnez **SOA Policy Gateway 2.5.0.0 - Advanced Runtime External DataPower** ou **SOA Policy Gateway 2.5.0.0 - Advanced Runtime**.
3. Cliquez sur l'icône **Déployer**.
4. Complétez les zones requises pour déployer le modèle. Une coche en regard de chaque élément indique qu'il ne nécessite pas de configuration supplémentaire.
   a. Dans la zone **Nom du système virtuel**, entrez un nom unique pour l'instance.
   b. Développez la section **Sélectionner l'environnement**, puis entrez le **Profil** comme indiqué par votre administrateur système PureAS.
   c. Configurer les modèles virtuels. Cliquez sur **Configurer les composants virtuels**, puis cliquez sur le nom du composant pour ouvrir l'éditeur pour les composants et scripts. Indiquez **Groupe de clouds** et **Groupe IP** comme vous le conseille votre administrateur système PureAS. Reportez-vous aux rubriques suivantes pour plus de détails sur les paramètres de configuration propres au modèle et au script.

      Remarque : Pour déployer le modèle sans maître de gouvernance, entrez 'Unset' pour paramètre de nom d'hôte du maître de gouvernance. Cela a pour effet mettre en échec le package du script de promotion durant le déploiement mais n'a pas d'autres conséquences.
      - «Composant DataPower», à la page 37
      - «Composant principal HADR DB2 Enterprise», à la page 30
      - «Composant Gestionnaire de déploiement WSRR», à la page 35
      - «Script : SOA Policy Gateway 2.5.0.0 - Promotion», à la page 39
      - «Script : SOA Policy Gateway 2.5.0.0 - DataPower Domain», à la page 38
      - «Composant Noeuds personnalisés WSRR», à la page 36
      - «Composant de secours HADR DB2 Enterprise», à la page 32
      - «Script : SOA Policy Gateway 2.5.0.0 - DataPower Monitoring (x86 uniquement)», à la page 41
5. Cliquez sur **OK** pour déployer.

Que faire ensuite

Pour vérifier le déploiement, voir «Vérification du déploiement», à la page 55.

Mise à jour de DataPower dans l'instance déployée

Après avoir déployé un modèle comprenant un composant WebSphere DataPower, vous devez effectuer la mise à jour de DataPower avec le groupe de correctifs le plus récent.

Pourquoi et quand exécuter cette tâche

Vous mettez à jour DataPower en téléchargeant le groupe de correctifs depuis Fix central et en l'appliquant dans l'interface Web DataPower.

Procédure

1. Téléchargez le package de mises à jour depuis Fix Central :
   a. Dans Fix Central, recherchez les dispositifs WebSphere DataPower SOA.
   b. Sélectionnez et téléchargez le package XI52-virtual-6.0.0.1-Firmware.

2. Connectez-vous à l'interface Web de la machine virtuelle DataPower dans votre modèle déployé. Voir «Connexion à la console d'un dispositif DataPower virtuel», à la page 86.
3. Dans le panneau de commande, sélectionnez **Contrôle du système**.
4. Localisez la section **Image d'amorçage**.
5. Téléchargez vers le dispositif DataPower le fichier `xi6001.scrypt4` issu du groupe de correctifs reçu sur votre ordinateur. Utilisez le Gestionnaire de fichiers dans l'interface utilisateur Web DataPower.
6. Sélectionnez le script téléchargé dans la liste **Fichier de microprogramme**.
7. Acceptez les conditions de licence, puis cliquez **Image d'amorçage**.
8. Suivez les invites pour installer le groupe de correctifs.

Vérification du déploiement

Après avoir déployé le modèle, vérifiez que le déploiement a abouti.

Procédure

1. Consultez les journaux de déploiement à la recherche d'une quelconque défaillance dans l'historique de déploiement du système virtuel. Pour plus d'informations, voir «Identification et résolution de problèmes liés au déploiement», à la page 103.
2. Facultatif : Si vous avez déployé le modèle SOA Policy Gateway Basic Runtime Sample, testez l'instance déployée en suivant le tutoriel pour envoyer des exemples de messages à l'aide des exemples d'applications fournis. Voir «Exécution de l'exemple de scénario de test», à la page 61.

Ajout d'un environnement d'exécution supplémentaire

Le profil GEP est fourni avec un système de classification d'environnement prédéfini qui contient quatre environnements distincts : Development (Développement), Test, Staging (Transfert) et Production.

Pourquoi et quand exécuter cette tâche

Les environnements Staging et Production sont également codifiés dans le cycle de vie SOA qui définit le cycle de vie des versions de capacité Capability Versions, comme Service Versions. Il existe des états et des transitions qui sont spécifiques des environnements Staging et Production, ce qui autorise une promotion contrôlée dans ces environnements d'exécution en définissant les systèmes cible dans le fichier de configuration de la promotion. Cette procédure est appropriée si votre organisation définit des environnements de la même manière, avec Staging défini comme un environnement pré-production qui permet d'effectuer un test avant d'autoriser l'ouverture de la version de capacité pour une utilisation générale. Notez cependant que de nombreuses organisations nécessitent des environnements supplémentaires, des modifications sont alors nécessaires dans le profil pour prendre en charge ces différences. Cette section décrit une manière d'ajouter un nouvel environnement d'exécution dans le profil d'activation de gouvernance (Governance Enablement Profile) WSRR.

Pour plus d'informations sur la planification d'un environnement de déploiement, voir «Planification de la configuration du modèle et prérequis des modèles», à la page 45.

Procédure

1. Déployez le SOA Policy Gateway Governance Master prédéfini. Pour plus d'informations, voir «Déploiement du modèle Governance Master», à la page 50.
2. Facultatif : Modifiez le profile d'activation de la gouvernance WSRR. Pour plus d'informations, voir IBM WebSphere Service Registry and Repository Version 8.0 - Centre de documentation - Tutoriel : Customizing runtime environments.
3. Configurez les modèles d'exécution basique ou avancée avec les informations détaillées de Governance Master. Pour plus d'informations, voir «Informations sur le déploiement de SOA Policy Gateway Governance Master», à la page 51.

   Remarque : La valeur d'environnement de promotion doit être définie à «Unset».
4. Déployez les modèles d'exécution basique ou avancée. Pour plus d'informations, voir «Déploiement d'un modèle d'exécution basique», à la page 52 et «Déploiement d'un modèle d'exécution avancé», à la page 53.

Ajout d'instances DataPower à un modèle

Les modèles basique et avancé avec instances DataPower internes possèdent deux instances par défaut. Chaque modèle peut posséder jusqu'à 10 instances DataPower au total.

Pourquoi et quand exécuter cette tâche

Les modèles eux-mêmes ne peuvent pas être édités. Vous pouvez ajouter plus d'instances DataPower aux modèles d'exécution basique ou avancé en effectuant une copie du modèle et en l'éditant.

Procédure

1. Ouvrez le modèle dans la console Workload Console.
2. Cliquez sur **Clone**, et indiquez un nom pour la copie du modèle.
3. Cliquez sur **Editer**.
4. Faites glisser d'autres composants DataPower depuis la liste de composants pour les ajouter au modèle.
5. Cliquez sur **Done editing** (Edition terminée).

Suppression d'instances DataPower d'un modèle

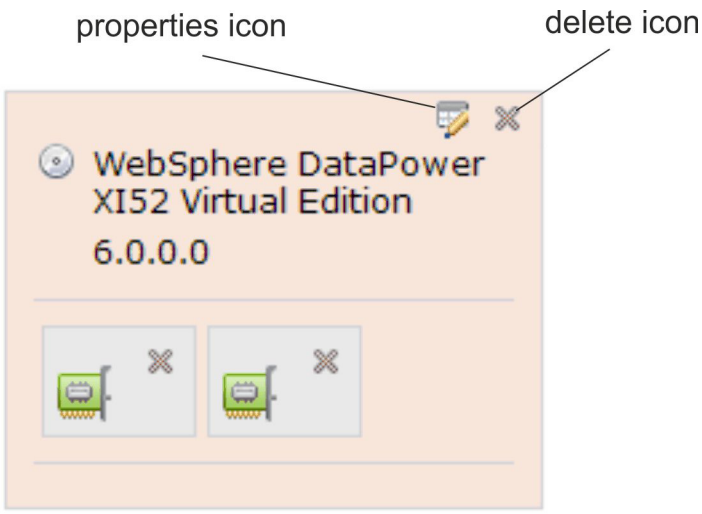
Vous pouvez supprimer des instances DataPower internes d'un modèle si nécessaire.

Pourquoi et quand exécuter cette tâche

Les modèles eux-mêmes ne peuvent pas être édités. Vous pouvez supprimer des instances DataPower des modèles d'exécution basique ou avancé en effectuant une copie du modèle et en l'éditant.

Procédure

1. Ouvrez le modèle dans la console Workload Console.
2. Cliquez sur **Clone**, et indiquez un nom pour la copie du modèle.
3. Cliquez sur **Editer**.
4. Supprimez une instance DataPower en cliquant sur l'icône de suppression.



Remarque : Les instances DataPower doivent être supprimées dans l'ordre numérique inverse. Chaque instance DataPower du modèle possède un numéro figurant dans la zone de nom, visible lorsque vous cliquez sur l'icône de propriétés. Le nom est défini dans le format : 'DataPower_XI52*x*' où *x* correspond au numéro (la première instance DataPower ne possède pas de numéro, son nom est : 'DataPower_XI52'). Les instances DataPower portant les numéros les plus élevés figurent généralement dans la partie supérieure gauche du modèle.

5. Cliquez sur **Done editing** (Edition terminée).

Déploiement des modèles DataPower externes basiques et avancés

Les modèles SOA Policy Gateway Basic Runtime External DataPower et SOA Policy Gateway Advanced Runtime External DataPower peuvent être déployés avec 10 dispositifs DataPower au maximum.

Pourquoi et quand exécuter cette tâche

Pour plus d'informations sur le déploiement des modèles, voir «Déploiement d'un modèle d'exécution basique», à la page 52 ou «Déploiement d'un modèle d'exécution avancé», à la page 53. Pour plus d'informations sur les paramètres de configuration pour lesquels vous devez définir des valeurs, voir «Composant Serveur autonome WSRR», à la page 34, «Composant Gestionnaire de déploiement WSRR», à la page 35 et «Script : SOA Policy Gateway 2.5.0.0 - DataPower Monitoring (x86 uniquement)», à la page 41.

Procédure

1. Déployez le modèle, puis cliquez sur **Configurer les composants virtuels**.
2. Pour le composant autonome WSRR ou gestionnaire de déploiement WSRR, entrez les informations suivantes pour chaque dispositif :
   - DataPower_hostname
   - DataPower_XML_mgmt_port
   - DataPower_admin_id
   - DataPower_admin_password
   - Confirmation du mot de passe
   - New_DataPower_domain

Modèle d'application

Le modèle d'application se compose d'un service Web et d'une API RESTful décrits et régis dans WSRR. Un domaine DataPower est configuré avec WSRR pour jouer le rôle de passerelle, et un client Web exemple est fourni pour exercer les services.

Le scénario de base du modèle d'application est une application d'inventaire pour un magasin (entrepôt) et un service RESTful qui duplique l'une des opérations pour la version mobile. Le service Web de magasin compte trois opérations :

- purchase
- findInventory
- returnProduct

La dernière opération, findInventory, est également disponible en tant que service RESTful.

Service Web exemple

La définition de niveau de service (SLD) de base contient deux règles de médiation jointes :

- Validation par rapport à Store.wsdl. L'exemple suppose que la validation DataPower est désactivée.
- Rejet s'il y a plus de 5 messages en 90 secondes. Ce seuil est bas pour simplifier la démonstration.

Le consommateur du service Store est l'application StoreConsumer, qui a pour ID Consommateur «CEO». Ce consommateur possède deux accords sur les niveaux de licence (SLA) : Gold et Anonymous. Si DataPower reçoit une requête avec l'ID Consommateur «CEO» et l'ID de contexte «Silver», la requête est autorisée car le SLA Silver est en place. Si l'ID Consommateur est «CEO» et que l'ID de contexte est «Gold», le SLA Gold est utilisé. Ce SLA possède une règle rattachée de sorte que la requête est réacheminée vers un point de terminaison alternatif défini dans la règle.

En cas de réception d'une requête ayant un ID Consommateur autre que «CEO», il n'existe pas de version d'application avec cet ID Consommateur. Par conséquent, un SLA ne correspond, car il s'agit d'un consommateur anonyme. En tant que telles, les règles rattachées au SLA anonyme sont appliquées. Dans ce cas, une notification figure dans les journaux. Notez que l'exemple ne comporte pas de procédure d'envoi d'une demande avec un ID Consommateur autre que «CEO».

Le scénario exécute également l'autorisation pour l'opération findInventory, selon l'appartenance à un groupe d'utilisateurs. Un serveur LDAP est fourni avec l'exemple pour mapper les données d'identification utilisateur avec le groupe approprié.

L'organigramme de flux d'application fourni en exemple affiche le flux de l'application avec chaque zone représentant une passerelle DataPower différente.

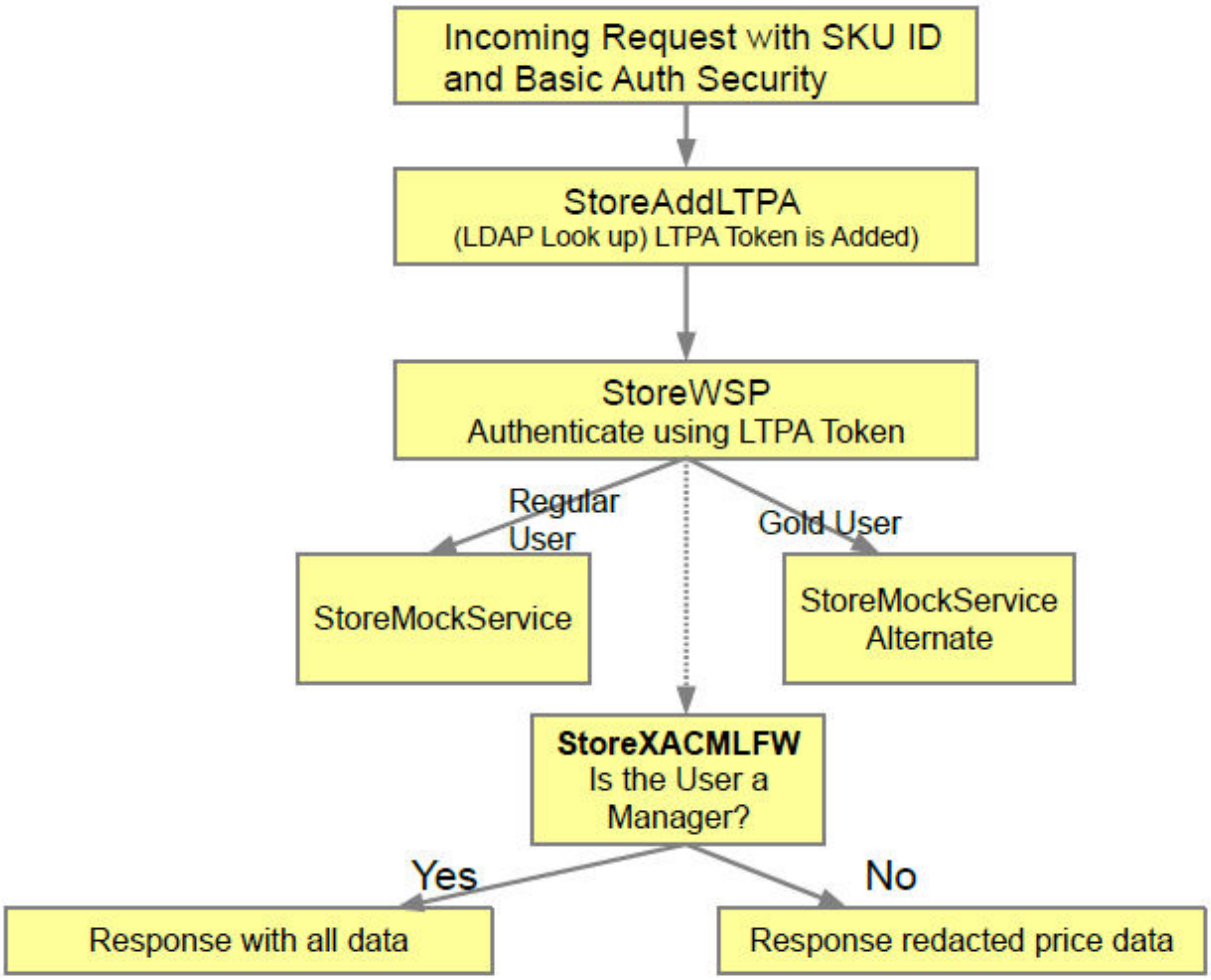


Figure 10. Le diagramme du flux du modèle d'application

Service RESTful fourni en exemple

Le service RESTful est gouverné de façon similaire au service Web, sauf en ce qui concerne l'utilisation des règles. Comme avec le service Web, on compte deux SLA : l'un pour les consommateurs Silver, l'autre pour les consommateurs Gold. Pour le service REST, cependant, aucune règle n'est rattachée au niveau du SLD (appliqué à toutes les requêtes). Au lieu de cela, une règle est rattachée à chaque SLA. Le SLA Gold comporte une règle qui rejette les messages quand plus de cinq requêtes ont eu lieu en 90 secondes, tandis que le SLA Silver autorise plus de deux requêtes en 90 secondes avant de rejeter les messages reçus.

Présentation des artefacts WSRR de l'exemple

Les artefacts WSRR décrivant le service de magasin sont présentés ici. Les artefacts suivent un modèle similaire pour le service REST.

L'entrepôt de Bob est l'organisation qui possède le service de fourniture de magasin et l'application de consommation StoreConsumer.

Le service métier de l'entrepôt est l'objet sous lequel résident toutes les versions du service de magasin. La version du service de magasin représente une version particulière de service de magasin. Cette version est le service fourni en vue de sa réutilisation. La définition de niveau de service (SLD) de magasin possède deux règles jointes ; la première règle rejette les messages après 5 messages dans les 90 secondes et la deuxième effectue une validation par rapport au schéma Store.wsdl. Ces règles signifient que les demandes adressées au service de magasin sont validées, et un maximum de 5 demandes est autorisé au niveau du service par intervalle de 90 secondes, indépendamment de l'émetteur de la demande. Le SLD possède un contrat de licence de niveau de service anonyme (SLA). Les règles jointes à ce SLA sont appliquées lors de la réception des demandes ne possédant pas de SLA correspondant. UN SLA correspond si les conditions suivantes sont satisfaites :

- Une version d'application consommatrice correspond à l'ID consommateur dans la requête.
- Un SLA est défini entre la version de cette application consommatrice et le SLD pour le service en cours d'utilisation correspondant à l'ID de contexte dans la requête

L'application métier StoreConsumer représente l'application StoreConsumer, alors que la version d'application StoreConsumer est une version particulière de cette application. Cette application est consommatrice : elle réutilise le service de mémoire. Elle a pour ID consommateur «CEO». Deux SLA sont définis pour cette application qui constitue un contrat autorisant cette application à consommer le service de magasin. L'un a pour ID de contexte «Gold», ce qui signifie qu'il correspond à des requêtes de l'application StoreConsumer ayant pour ID de contexte «Gold» dans la requête, et l'autre a pour ID de contexte Silver. Le SLA Gold possède une stratégie jointe pour réacheminer les requêtes, de sorte que des requêtes émanant de l'application StoreConsumer et ayant pour ID de contexte Gold sont réacheminés au point de terminaison indiqué dans la règle. Le SLA Silver ne possède pas de règles jointes. Son existence signifie que les requêtes émanant de l'application StoreConsumer et ayant pour ID de contexte Silver sont acceptées, bien qu'aucune règle ne soit appliquée.

Dans cet exemple, aucune règle de notification n'est jointe au SLA anonyme.

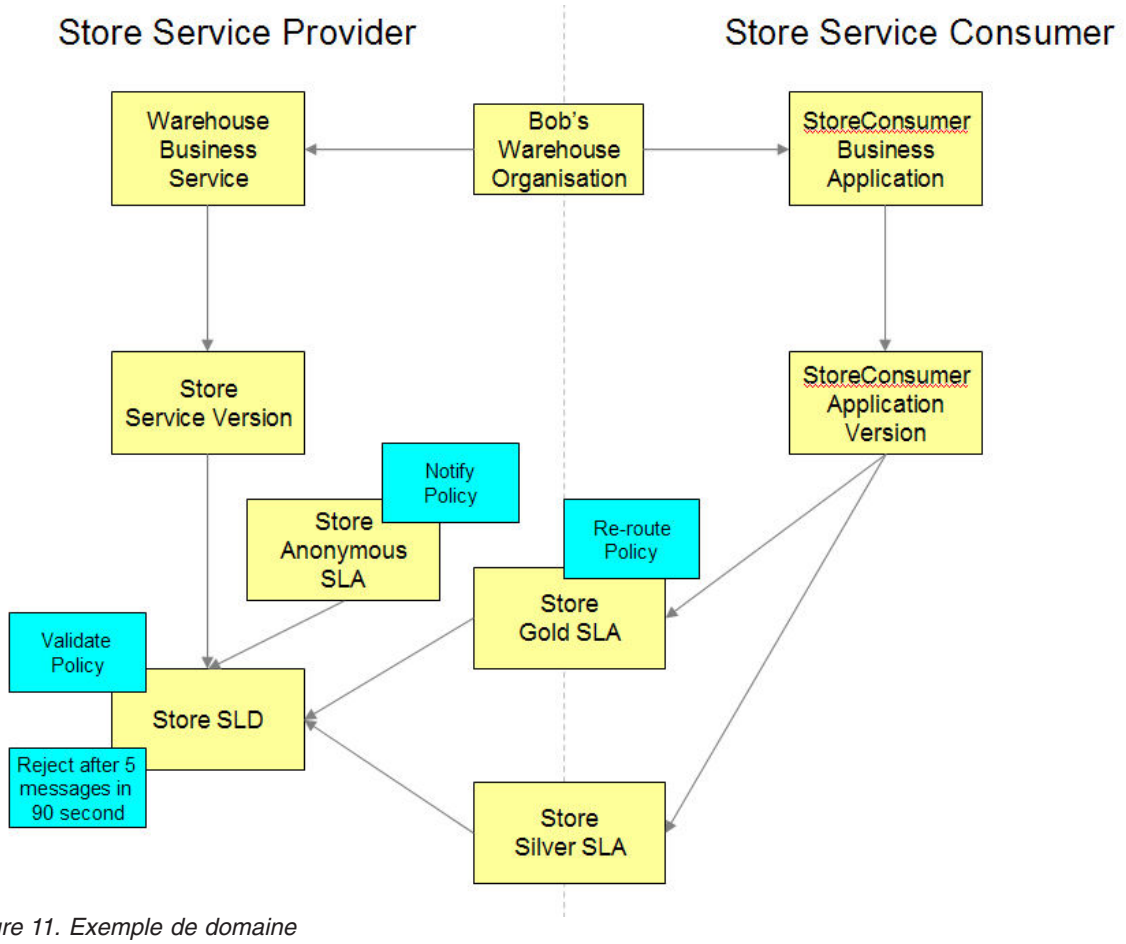


Figure 11. Exemple de domaine

Exécution de l'exemple de scénario de test

Vous pouvez utiliser un exemple d'application Web ou la ligne de commande pour tester le modèle d'application sur le modèle SOA Policy Gateway Basic Runtime Sample déployé. Six variations de test peuvent être exécutées sur le modèle d'application via la ligne de commande.

Pour déployer le modèle Basic Sample Runtime, voir «Déploiement du modèle d'exécution basique», à la page 49.

Scénario de test de l'exemple d'application Web

Pour exécuter ce scénario de test d'application Web, procédez comme suit :

1. Recherchez le nom d'hôte de l'environnement WSRR déployé en ouvrant l'instance de système virtuel déployée. Pour trouver le nom d'hôte, développez la section **Machines virtuelles** et sélectionnez la machine virtuelle du serveur WSRR autonome pour afficher les détails de la machine virtuelle. Dans la section **Matériel et réseau**, le nom d'hôte correspond à la valeur **Interface réseau 0**.
2. Ouvrez l'adresse URL dans un navigateur Web : `http://<nom_hôte_wssr>:9080/SoaPolicyTester`
3. Les options suivantes sont disponibles :

- **Standard Request** - Envoie une requête findInventory au service du magasin. L'ID de contexte est un utilisateur Silver. L'ID consommateur est CEO. Le résultat est réussi lorsque le texte «Part: SKU10 Price: 401.73» s'affiche.
- **Routing Policy Test** - Similaire à Standard Request, mais un ID de contexte Gold. La requête est dirigée vers un autre noeud final exécutant le service. Un résultat correcte renvoie «Part: GOLDSKU10 Price: 401.73».
- **Validation Policy Test** - Envoie une requête avec un contenu non valide. La règle de validation requiert DataPower pour valider la requête et rejeter les messages non valides. Un résultat réussi est un message de réponse émanant de DataPower, à savoir `"Internal Error (from client)"`.
- **REST Gold** - Envoie une requête au service RESTful SKU avec l'ID Consommateur CEO et l'ID de contexte Gold. Les requêtes gold sont soumises à une règle autorisant uniquement 5 messages en 90 secondes. Une requête réussie affiche le résultat «Part: SKU33 Price: 136.43».
- **REST Silver** - Similaire à Rest GOLD, mais avec l'ID de contexte Silver. Les requêtes Silver sont autorisés au nombre de 3 par tranche de 90 secondes. Une requête réussie affiche le résultat «Part: SKU33 Price: 136.43».
- **ID utilisateur** - Cette option autorisé les valeurs suivantes : Full Content ou Redacted Content. Chaque option traite les requêtes émanant d'utilisateurs différents. L'exemple utilise une règle XACML qui limite l'affichage du prix aux Managers. Dans le message de réponse, la valeur du prix est rédigée sauf si Full Content est sélectionné. Lorsque Redacted Content est sélectionné, un résultat réussi pour les requêtes contient «Price: 0.0». Le service RESTful ne gère pas la rédaction. L'utilisateur sélectionné n'a aucun effet.

4. Ouvrez la console WSRR et explorez le service et les règles. Pour plus d'informations, voir «Connexion à WSRR - Business Space», à la page 82.

L'échantillon peut également être exercé à l'aide de la ligne de commande. Il s'agit du seul moyen d'envoyer du trafic utilisant le SLA anonyme

Démonstration de XACML Permit/Deny avec le scénario Redaction à l'aide de la ligne de commande

La requête XML suivante peut être envoyée au service DataPower StoreAddLTPA :

```
<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>
```

En supposant que l'exemple de requête XML est contenu dans un fichier nommé `silver.xml`, exécutez la commande curl suivante :

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

Dans cet exemple, ConsumerX est un Manager et les informations complètes sur les prix doivent s'afficher comme réponse :

```
<?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>
```

Exécution du scénario Redaction à l'aide de la ligne de commande

ConsumerA n'est pas un Manager, nous devons donc voir une réponse différente. Exécutez la commande curl :

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

Notez le prix est rédigé dans la réponse. Le prix est affiché en tant que 0.0 :

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
<soapenv:Header><KD4NS:KD4SoapHeaderV2
xmlns:KD4NS="http://www.ibm.com/KD4Soap">AFIAAgAkZmExODgzNTQtY2Q1ZC0zYjU0L
WEyMzItZGM3MmEzNWY0MTAzACRmYWVjYjA1Mi1jMWUxLTMyODEtOWY3Ni0wY2IxNm
RhMDc4MjkAAw==</KD4NS:KD4SoapHeaderV2>
</soapenv:Header>
<soapenv:Body>
<b:findInventoryResponse xmlns:a="http://company.ibm.com/"
xmlns:b="http://company.ibm.com/store">
<findInventoryRes>
<sku>SKU10</sku>
<price>0.0</price>
<inventory>460</inventory>
<msrp>923.46</msrp>
<supplierID>IBM</supplierID>
</findInventoryRes>
</b:findInventoryResponse>
</soapenv:Body></soapenv:Envelope>
```

Test de la stratégie de routage à l'aide de la ligne de commande

Pour que la règle de routage rattachée au SLA Gold s'applique, il est nécessaire que le ID de contexte et le ID consommateur correspondent. Dans ce cas, le SLA des consommateurs Gold a Gold pour ID de contexte, tandis que la version du service consommateur a CEO pour ID consommateur. Voici le contenu d'un exemple de requête (vous pouvez constater que le ID de contexte et le ID consommateur coïncident comme exigé) :

```
<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>
```

En supposant que l'exemple de requête XML est contenu dans un fichier nommé `gold.xml`, exécutez la commande curl suivante :

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

La réponse est la suivante :

```
<?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>
```

Notez que la réponse en retour contient un `GOLDSKU` pour la valeur de SKU, indiquant que le noeud final Gold a été utilisé.

Test de la validation du schéma à l'aide de la ligne de commande

La règle de validation vérifie le schéma de la requête par rapport à Store.wsdl et est associé à Company.xsd.

Le code XML suivant, `badvalid.xml`, présente une requête qui n'est pas valide car le corps contient un élément nommé `<skubad>` alors qu'il doit être `<sku>` :

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:stor="http://company.ibm.com/store">
<soapenv:Header>
<store:ConsumerIdentifier xmlns:store="http://store.com">CEO</store:ConsumerIdentifier>
<store:ContextIdentifier xmlns:store="http://store.com">silver</store:ContextIdentifier>
</soapenv:Header>
<soapenv:Body>
<stor:findInventory>
<findInventoryReq>
<skubad>SKU10</skubad>
</findInventoryReq>
</stor:findInventory>
</soapenv:Body></soapenv:Envelope>
```

Si vous entrez la requête curl suivante :

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

Le message d'erreur suivant s'affiche :

```
<?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>
```

Test du refus dans la règle de médiation à l'aide de la ligne de commande

L'une des règles de médiation incluses dans l'exemple teste le refus après que le nombre de messages atteint 5 dans l'espace de 90 secondes. Exécutez la commande suivante 6 fois :

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

L'exemple de requête est comme suit :

```
<?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>
```

Dans ce cas, ConsumerX est un gestionnaire. En conséquence, les informations complètes sur les prix sont affichées ainsi pour les cinq premières exécutions :

```
<?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>
```

Pour la sixième exécution, vous devez voir l'erreur suivante :

```
<?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>
```

Remarque : Vous pourriez voir cette erreur plus tôt en exécutant d'autres tests dans l'intervalle de 90 secondes.

Test de notification dans la règle de médiation à l'aide de la ligne de commande

La règle de notification est rattachée au SLA anonyme. Ceci s'applique lorsqu'une demande émane d'un consommateur ne disposant pas de SLA. Dans cet exemple, le seul consommateur disposant de SLA est le directeur. Aussi une demande dont l'ID consommateur est réglé sur une autre valeur implique l'application du SLA anonyme par la règle. Dans ce cas, ConsumerX est un gestionnaire, nous devons donc voir les informations complètes sur les prix comme suit :

Pour tester cette fonctionnalité à l'aide de la ligne de commande, créez un fichier nommé `anon.xml` qui contient le code xml suivant :

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:stor="http://company.ibm.com/store">
<soapenv:Header>
  <store:ConsumerIdentifier xmlns:store="http://store.com">ABC</store:ConsumerIdentifier>
  <store:ContextIdentifier xmlns:store="http://store.com">Gold</store:ContextIdentifier>
</soapenv:Header><soapenv:Body>
<stor:findInventory><findInventoryReq>
  <sku>SKU10</sku>
  </findInventoryReq>
</stor:findInventory>
</soapenv:Body></soapenv:Envelope>
```

Entrez ensuite la commande suivante :

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

Le message suivant est émis dans le journal par défaut du domaine :

```
Notify action triggered ('operation_38_2_sla1-1-filter_1-notify') from source policy ('LogEveryTime_287d0790-83d9-11e1-a255
```

Remarque : La consignation doit être réglée sur «notice» pour que ce message s'affiche. Autrement, cliquez sur l'icône de dépannage (**Identification et résolution des problèmes**) dans la console Web de DataPower. Dans la section Consignation, changez la valeur Log level pour «notice», puis cliquez sur **Set Log Level**. Pour trouver le journal, retournez dans le panneau de commande, puis cliquez sur l'icône d'affichage des journaux (**View Logs**).

Test du service RESTful à l'aide de la ligne de commande

Vous pouvez également accéder à l'interface RESTful à l'aide de la commande curl sur la ligne de commande. Comme avec le client Web, un ID de contexte de type gold permet 5 messages par tranche de 90 secondes contre 2 messages par tranche de 90 seconde pour un ID de contexte de type silver.

Pour tester cette fonctionnalité à l'aide de la ligne de commande, créez un fichier nommé restRequest.xml qui contient le code xml suivant :

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

Entrez ensuite la commande suivante pour tester l'ID de contexte de type gold :

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

Pour tester l'ID de contexte de type silver, utilisez la même commande en remplaçant Gold par Silver.

Une réponse réussie se présente sous une forme similaire :

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

Après que le seuil a été atteint, vous recevez le message suivant :

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

Pour tester le SLA anonyme pour le service RESTful, qui possède simplement une règle de notification jointe, utilisez n'importe quels ID de contexte et ID consommateur autres que ceux enregistrés. La notification s'affiche dans le journal DataPower comme décrit précédemment pour l'exemple des services Web.

Tâches associées:

«Déploiement du modèle d'exécution basique», à la page 49
Le déploiement du modèle SOA Policy Gateway Basic Runtime Sample crée une instance de système virtuel d'exécution du modèle. Ce modèle est disponible uniquement sur les systèmes x86.

Extension du modèle d'application

Le modèle d'application peut être modifié en modifiant la feuille de style Bindings et les feuilles de style XSL.

Modifications apportées à la feuille de style de liaisons Bindings

La variable xacml-subjects a été ajoutée à la feuille de style `apil-xacml-binding-new.xsl`. Elle englobe la création de la section subjects de la requête. Cette variable est ensuite accessible dans `sendToPDP.xsl`.

```
<xsl:variable name="xacml-subjects">
  <xacml-context:Subject SubjectCategory="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject">
<!--
***********************************************
A partir d'ici, utilisez le résultat MC comme sujet
***********************************************
```

sendToPDP.xsl

Cette feuille de style appelle le pare-feu StoreXACMLFW à l'aide d'url-open. L'appel s'effectue sur le dispositif DataPower vers un autre pare-feu XML, donc aucun profil de proxy SSL n'est utilisé. Pour déplacer le point de décision de règles (PDP) vers un autre dispositif DataPower, un profil de proxy SSL peut être créé et utilisé avec l'appel url-open.

```
<xsl:param name="resource" />
<!--
<xsl:variable name="incoming_resource">
<xsl:value-of select="$resource" />
</xsl:variable>
<xsl:message dp:priority="debug">
********** ABOUT TO CALL PDP for RESOURCE equal *************
<xsl:value-of select="$incoming_resource" />
</xsl:message>
-->
- <!--
génération de la requête XACML pour masquage
-->
<xsl:variable name="customized-request">
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
<soapenv:Header />
<soapenv:Body>
<xacml-context:Request xmlns:wsa="http://www.w3.org/2005/08/addressing" xmlns:soap="http://schemas.xmlsoap.org/soap/envelop
xmlns:xacml-context="urn:oasis:names:tc:xacml:2.0:context:schema:os" xmlns:ws="http://docs.oasis-open.org/wss/2004/01/oasis
wss-wssecurity-secext-1.0.xsd">
- <!--
copie dans les sujets (subjects ) enregistrés à partir d'un traitement de requête AAA
-->
<xsl:copy-of select="dp:variable('var://context/snip/xacml/xacmlSubjects')/*" />
<xacml-context:Resource>
<xacml-context:ResourceContent>
<xsl:copy-of select="./soap:Envelope/soap:Body" />
</xacml-context:ResourceContent>
<xacml-context:Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#string">
<xacml-context:AttributeValue>PriceInfo</xacml-context:AttributeValue>
</xacml-context:Attribute>
</xacml-context:Resource>
<xacml-context:Action>
<xacml-context:Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
DataType="http://www.w3.org/2001/XMLSchema#string">
<xacml-context:AttributeValue>View</xacml-context:AttributeValue>
</xacml-context:Attribute>
</xacml-context:Action>
<xacml-context:Environment>
<xacml-context:Attribute AttributeId="ContextId" DataType="http://www.w3.org/2001/XMLSchema#string"
Issuer="http://security.tivoli.ibm.com/policy/distribution">
<xacml-context:AttributeValue>StorePriceData</xacml-context:AttributeValue>
</xacml-context:Attribute>
</xacml-context:Environment>
</xacml-context:Request>
</soapenv:Body>
</soapenv:Envelope>
</xsl:variable>
- <!--
Utilisation de set-variable pour qu'elle soit visible dans la sonde (Probe), ce qui est pratique
```

```
-->
<dp:set-variable name="'var://context/snip/xacml/BacksideXacmlRequest'" value="$customized-request" />
- <!--
Signalement de XACML-REQUEST dans le journal de débogage
-->
<xsl:message dp:priority="debug">
<XACML-REQUEST>
<xsl:copy-of select="$customized-request" />
</XACML-REQUEST>
</xsl:message>
<xsl:variable name="headers">
<header name="SOAPAction">xacml:authorization</header>
</xsl:variable>
- <!--
Appel du point de décision de règles (PDP) XACML pour décision
-->
<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>
- <!--
Utilisation de set-variable pour qu'elle soit visible dans la sonde (Probe), ce qui est pratique
-->
<dp:set-variable name="'var://context/snip/xacml/BacksideXacmlResponse'" value="$rtss-response" />
- <!--
Signalement de XACML-RESPONSE dans le journal de débogage
-->
<xsl:message dp:priority="debug">
<XACML-RESPONSE>
<xsl:value-of select="$rtss-response" />
</XACML-RESPONSE>
</xsl:message>
</xsl:template>
</xsl:stylesheet>
```

Notez les points suivants relatifs au fichier `sendToPDP.xsl` :

1. La feuille de style récupère le port pour XACMLFW à partir de `soavars.xsl`.
2. La variable rtssResponse est prévue pour être exactement de la forme que les services de sécurité d'exécution (Runtime Security Services) doivent utiliser, et en retour de la forme que le point de décision de règles (PDP) du dispositif DataPower peut traiter.
3. La feuille de style génère une requête SOAP. Les informations de l'objet sont créées par la feuille de style `apil-binding.xsl` précédente et sont obtenues par la copie suivante de la requête de sélection :

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

4. L'opération consiste simplement à afficher l'action : `<xacml-context:AttributeValue>View</xacml-context:AttributeValue>`
5. L'environnement est StorePriceData, connu comme un objet d'application dans la technologie IBM Tivoli Security Policy Manager ou Runtime Security Services.

StorePrivateDataXACML.xml

Le code suivant correspond à la feuille de style des règles pour la réécriture.

```
<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>
```

Prenez connaissance des informations suivantes :

- Le rôle doit être Manager :

```
<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>
```

- La ressources doit être PriceInfo :

```
<ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
<xacml:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"
 xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os">PriceInfo</xacml:AttributeValue>
```

- L'action doit être View :

```
<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>
```

Modification de l'exemple de feuilles de style XSL

Vous pouvez modifier la feuille de style de rédaction `noPriceInfo.xsl`

Procédure

Modifier la feuille de style de rédaction (Redaction).
La feuille de style `noPriceInfo.xsl` contient le code suivant, qui remplace toutes les valeurs de prix par des zéros. Vous pouvez ajouter d'autres zones à la logique de rédaction ou ajouter des transformations plus complexes qui impliquent un calcul permettant de déterminer les valeurs pour les zones.

```
<!-- accès privé aux zones uniquement -->
<xsl:template match="price">
<price>0.0</price>
</xsl:template>
<xsl:template match="Price">
<Price>0.0</Price>
</xsl:template>
```

Par la suite, la feuille de style effectue une transformation d'identité sur tous les autres éléments.

Exploration plus approfondie de l'exemple

Pour en savoir plus sur l'exemple, vous pouvez configurer le point de décision de règles (PDP) XACML sous DataPower et éditer les documents de règles.

Modification du point de décision de règles XACML sous DataPower

Vous pouvez explorer la modification de XACML utilisée pour le point de décision de règles de sécurité dans DataPower pour en savoir plus sur le contrôle d'accès avec XACML.

Procédure

Pour changer ou ajouter un point de décision de règles, procédez comme suit :

1. Dans le panneau de commande de DataPower, recherchez `XACML PDP`.
2. Cliquez sur un point de décision de règles existant ou cliquez sur **Ajouter**.
3. Entrez une adresse URL ; par exemple `local:///storePrivateDataXACML.xml`.
4. Ajoutez tous les fichiers dépendants ou de répertoire requis pour prendre en charge la règle.

   Remarque : Si vous modifiez un fichier de règles XACML directement sur le système de fichiers, vous devez revenir sur la définition du point de décision de règles (PDP) et entrer à nouveau l'adresse URL ou tout ce que vous avez changé, ou redémarrer le domaine pour que vos changements prennent effet.

Ajout ou édition de documents de règles

Utilisez l'interface utilisateur de Business Space pour créer ou éditer des documents de règles.

Avant de commencer

Configurez l'espace de gouvernance SOA. Pour plus d'informations, voir «Configuration de Business Space pour la première utilisation», à la page 83.

Procédure

1. Créez une règle de médiation avec les conditions et actions requises ; par exemple, une condition sur le nombre de messages > 5 messages dans l'espace

de 5 minutes et une action de refus. Pour plus d'informations sur la création d'une règle de médiation, voir «Création de règles de médiation», à la page 98.

2. Administrez le règle de médiation. Pour plus d'informations sur l'administration d'un document de règles, voir «Gérer le cycle de vie de la règle», à la page 100.
   a. Cliquez sur le document de règles dans le navigateur de Service Registry or recherchez-le dans le widget de recherche. Les actions sont affichées dans l'éditeur de documents de règles.
   b. Cliquez sur **Proposer la spécification**.
   c. Cliquez sur **Approuver la spécification**.

   La règle est approuvée. Vous pouvez redéfinir, remplacer ou supprimer les règles pour gérer le cycle de vie ou modifier une définition existante.
3. Joignez la règle. Dans Business Space, recherchez le SLD ou le SLA auquel vous souhaitez rattacher la règle. Vous pouvez effectuer cette opération à quatre endroits différents dans l'exemple :
   - SLD Store - rattachez votre règle ici pour qu'elle s'applique à n'importe quelle utilisation du service Store.
   - SLA Gold - rattachez votre règle ici pour qu'elle s'applique uniquement aux requêtes Gold émanant du consommateur CEO.
   - SLA Silver - rattachez votre règle ici pour qu'elle s'applique uniquement aux requêtes Silver émanant du consommateur CEO.
   - SLA Anonymous - rattachez votre règle ici pour qu'elle s'applique aux requêtes émanant de consommateurs autres que CEO.

Tâches associées:

«Création de règles de médiation», à la page 98
Vous pouvez créer des règles de médiation à l'aide de l'interface utilisateur de Business Space. Lorsque vous créez des règles de médiation, indiquez les conditions et actions qui s'y rattachent.

«Gérer le cycle de vie de la règle», à la page 100
Les règles peuvent être en transition entre des états de gouvernance à l'aide de l'interface utilisateur de Business Space. Les règles doivent être à l'état Approuvé pour pouvoir être implémentées par DataPower.

Information associée:

Centre de documentation d'IBM WebSphere Service Registry and Repository version 8.0 - Utilisation de l'interface utilisateur Business Space

Exemple de domaine DataPower

Le modèle fournit un exemple de domaine DataPower qui vous permet de commencer à utiliser le modèle. En tant que développeur de DataPower, vous pouvez utiliser les passerelles existantes comme modèles pour vos propres applications. L'exemple d'environnement contient cinq passerelles. Vous trouverez une passerelle principale dédiée au service de magasin et quatre passerelles de support fournissant des exemples de dorsales pour la passerelle de magasin à appeler, un support XACML pour un scénario de réécriture et un support frontal offrant des fonctionnalités de sécurité supplémentaires.

StoreWSP (Store Web Service Proxy)

StoreWSP (Store Web Service Proxy) est la passerelle principale du domaine d'application. Elle reçoit une requête avec un jeton LTPA joint.

Si demandée, la règle de traitement pour la requête exécute les actions suivantes :

1. Validation de la requête, comme demandée par les règles de validation. Pour plus d'informations, voir «Présentation des artefacts WSRR de l'exemple», à la page 59.
2. Acheminement de la requête vers un noeud final de remplacement, si l'accord sur les niveaux de service (SLA) est «Gold».
3. Exécution des opérations AAA (authentification, autorisation et comptabilité) sur la requête. L'authentification inclut les actions suivantes :
   a. Authentification de l'utilisateur muni d'un jeton LTPA.
   b. Mappage les données d'identification par rapport au serveur LDAP qui fournit des informations comme les groupes auxquels le client appartient. Ces groupes incluent Manager, Clerk et Customer.
   c. Transformation des entrées fournies en objet de demande que le point de décision de règles (PDP) XACML est en mesure d'interpréter.
   d. Réalisation de l'autorisation à l'aide d'un point de décision de règles (PDP) XACML (sur la zone DataPower), avec un document de règles XACML qui peut être créé dans IBM Tivoli Security Policy Manager. Le critère de la règle est que l'utilisateur doit être un Manager, Customer ou Clerk. Pour l'opération findInventory, les retours nécessitent Manager ou Clerk tandis que les achats peuvent être effectués par des clients.
4. Définit la valeur ID_consommateur à l'aide d'un script XSL.
5. Supprimer l'intégralité de l'en-tête de sécurité HTTP de la requête.
6. Appelle le système dorsal du service de magasin.

Lors du traitement de la requête, la règle de traitement de réponse exécute les actions suivantes :

1. Appel de la passerelle StoreXACMLFW, qui agit comme le point de décision de règles (PDP) dans le scénario.
2. Suivant la réponse, la zone d'information sur les prix (PriceInfo) est réécrite (mise à zéro) selon que l'utilisateur a le rôle de Manager ou non.

Pare-feu XML dans l'exemple

Les pare-feu XML suivants sont définis dans l'exemple.

Pare-feu XML StoreAddLTPA

Le pare-feu XML d'authentification LTPA StoreAdd a pour fonction de fournir un support frontal doté d'un port que des utilisateurs peuvent appeler en utilisant une authentification de base (par exemple, aucune authentification LTPA). La règle de traitement de la requête :

1. Identifie via l'authentification de base.
2. Authentifie via une recherche LDAP simple.
3. Ajoute un jeton LTPA comme composant du post-traitement.
4. Transfère la requête à la règle de sécurité StoreWSP avec les informations LTPA maintenant jointes.

Pare-feu XML StoreMockService

StoreMockService est un exemple de service qui utilise un pare-feu XML comme une implémentation. Les opérations 'findInventory', 'purchase' et 'return' sont toutes prises en charge. Les valeurs de réponse sont statiques. Cet exemple de service est créé lorsqu'il n'est pas possible d'inclure WebSphere Application Server dans le modèle. Les trois règles de demande de la stratégie utilisent une action de mise en correspondance qui détermine l'opération de demande et qui s'appuie sur

une correspondance et répond avec une réponse SOAP statique. Les réponses SOAP statiques sont fournies en fonction de l'opération de demande au lieu d'une implémentation de service complet.

Pare-feu XML StoreMockServiceAlternate

StoreServiceAlternate est un exemple de service qui utilise un pare-feu XML comme une implémentation. Les opérations 'findInventory', 'purchase' et 'return' sont toutes prises en charge. Ce service est utilisé pour illustrer la mise en application de la politique de routage.

Pare-feu StoreXACMLFW

Ce scénario effectue une réécriture selon le résultat d'un processus XACML basé sur un mécanisme d'autorisation/refus. Dans DataPower, il n'existe aucun moyen d'appeler une action AAA individuelle dans le flux de réponses. Une passerelle distincte est créée pour contenir le point de décision de règles (PDP) XACML. Ce point de décision de règles (PDP) a été encapsulé dans une action AAA de la règle de demande de StoreXACMLFW.

StoreXACMLFW est une passerelle de pare-feu XML de DataPower. Cette implémentation est utilisée car il s'agit d'un moyen simple de fournir la fonctionnalité. Le pare-feu StoreXML utilise la même interface WSDL interface que le serveur Tivoli Runtime Security Services. La passerelle StoreWSP crée l'objet de requête et l'envoie, protégé par SSL, à la passerelle StoreXMLFW.

La règle de demande du pare-feu StoreXML exécute les opérations suivantes :

1. Exécution de l'action AAA à l'aide des informations pour authentification.
2. Traitement de l'autorisation à l'aide du point de décision de règles XACML du dispositif DataPower. La règle utilisée par le point de décision de règles (PDP) est initialement créée dans IBM Tivoli Security Policy Manager, mais elle peut être recréée à l'aide d'un éditeur standard, et le schéma est défini dans la spécification XACML.
3. Aucune transformation de la requête n'est nécessaire dans ce traitement d'autorisation.
4. Si la requête XACML est valide, la règle de traitement de la requête effectue l'extraction d'une réponse "Permit" (autorisé) et retourne vers le client. Sinon, une exception est émise, elle est gérée par la règle de traitement d'exception et renvoie une réponse Deny (refusé) au client.

Remarque : Le processus Permit/Deny/Indeterminate n'est qu'une réponse au niveau de l'exemple. D'autres informations d'erreur peuvent très bien être incluses dans un flux spécifique du client.

Politique de sécurité XACML

Cette rubrique explique comment des documents XACML sont créés.

Les documents XACML utilisés dans l'exemple ont été créés par l'éditeur de règles de IBM Tivoli Security Policy Manager (TSPM) ; vous pouvez également utiliser tout autre éditeur de texte ou éditeur XML pour créer de tels documents. Pour construire ou modifier des politiques XACML existantes, voir les spécifications OASIS : https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml.

La règle de sécurité XACML utilisée dans l'exemple est contenue dans `storeSWPXACML.xml` et dans `storePrivateDataXACML.xml`. Ces politiques permettent d'évaluer les requêtes entrant dans le point de décision de règles (PDP). La requête est constituée de quatre éléments clé :

1. La section Subjects qui contient les détails du nom descriptif de l'appelant de la requête, ainsi que les groupes auxquels l'appelant appartient.
2. La section Resource qui contient les documents auxquels l'appelant veut avoir accès. Deux types de ressource sont utilisés dans l'exemple. Le premier type est l'opération sur le service Web et le deuxième est l'autorisation aux données sur la réponse, ici, la ressource d'informations sur les prix : priceInfo.
3. La section Environment qui contient des informations sur l'environnement de la requête.
4. L'action - Que souhaite faire l'utilisateur avec les éléments autorisés. Dans le scénario de réécriture, l'action consiste simplement à afficher les données priceInfo d'informations sur les prix.

Politique de sécurité de StoreWSP

La politique de sécurité du fichier `storeSWPXACML.xml` mappe des groupes avec des opérations de services Web.

Voici un exemple de règle de sécurité :

```
<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>
```

Remarque : Dans la section subjects (objets), une correspondance apparaît sur le nom x500 ou le rôle objet du Manager (Gestionnaire). Si vous examinez l'intégralité du fichier de règles `.xml`, vous pouvez voir qu'il existe des mappages similaires pour Customer et Clerk. Vous pouvez voir que l'opération findInventory est autorisée à utiliser les trois groupes tandis les opérations returnProduce et purchase sont limitées à seulement certains groupes.

Passerelle Redaction

Détails concernant la feuille de style storeCallPDP.xsl.

Examinez la feuille de style storeCallPDP.xsl et notez les points suivants :

1. L'inclusion de la feuille de style storeSendToPDP.xsl. Il s'agit de la feuille style disposant de la logique d'appel de storeXAMLFW.
2. L'appel au modèle call_PDP au sein de storeSendToPDP.
3. L'extraction de la décision à partir de la réponse à l'appel, par exemple «Permit».
4. Le paramètre de la valeur `var:/context/response/displayfilter` pour les feuilles de style allData.xsl ou noPriceInfo.xsl.
5. La structure de XACML pour Redaction, storePrivateDataXACML.xml, est pratiquement identique à la structure dans le scénario StoreWSP. La différence est que seul le rôle Manager dispose d'un accès.

storeCallPDP.xsl

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

```
      </xsl:when>
      <xsl:otherwise>
        I<dp:set-variable name="'var://context/response/displayFilter'" value="'local:///noPriceInfo.xsl'" />
      </xsl:otherwise>
    </xsl:choose>
  </xsl:template>
</xsl:stylesheet>
```

Artefacts WSRR créés dans le modèle SOA Policy Gateway Basic Runtime Sample

Artefacts WSRR créés dans le modèle SOA Policy Gateway Basic Runtime Sample et comment l'exemple les utilisent.

Tableau 14. Artefacts WSRR créés pour le modèle SOA Policy Gateway Basic Runtime Sample

Objet	Description
Organisation	Entrepôt de Bob. Il s'agit du site de l'entreprise possédant le service Store
Fonction métier	Entrepôt. Représente toutes les versions du service Store, rattaché à l'entrepôt de Bob.
Version de service	Magasin. Représente la version 1.0 du service de magasin.
WSDL	Store.wsdl
XSD	Company.xsd
Politique	• Validate.xml • RouteForGold.xml • LogEveryTime.xml • RejectAfter5MsgIn90Seconds.xml
SLD	Magasin SLD. Toutes les règles jointes ici s'appliquent à toute requête de ce service.
Gold SLA	SLA Gold. L'existence de ce SLA signifie que les requêtes gold du directeur des produits grand public ne doivent pas être considérés comme anonymes. Toutes les règles jointes ici sont appliquées aux requêtes gold émanant du directeur des produits grand public.
Silver SLA	SLA Silver. L'existence de ce SLA signifie que les requêtes argent du directeur des produits grand public ne doivent pas être considérés comme anonymes. Sans règles jointes, la requête est autorisée.
Anonymous SLA	Utilisateurs anonymes. Les règles jointes ici sont appliquées pour toute requête ne disposant pas d'un SLA correspondant. Dans cet exemple, les règles de SLA anonymes sont appliquées à toute requête émanant d'un client autre que le directeur ou toute requête du directeur autre que Gold ou Silver.

Artefacts DataPower créés dans le modèle SOA Policy Gateway Basic Runtime Sample

Les artefacts DataPower ont été créés dans le modèle SOA Policy Gateway Basic Runtime Sample.

Tableau 15. Artefacts DataPower créés pour le modèle SOA Policy Gateway Basic Runtime Sample

Type	Nom	Objet
Proxy service Web	StoreWSP	Service principal.

Tableau 15. Artefacts DataPower créés pour le modèle SOA Policy Gateway Basic Runtime Sample (suite)

Type	Nom	Objet
Pare-feu XML	StoreAddLTPA StoreMockService StoreAlternateMockService StoreXACMLFW	Authentifie et ajoute le jeton LTPA. Le fournisseur de service pour des clients non Gold Le fournisseur de service pour des clients Gold Vérifie l'accès à PriceInfo.
Serveur WSRR	WSRRSVR	Connexion à WSRR.
Abonnement à WSRR	StoreSub	Fournit des informations de recherche pour l'espace de nom, l'objet, etc. WSRR.
Stratégie AAA	StoreAddLTPA	Identification et authentification de base pour LDAP. Recherche une authentification. Ajoute le jeton LTPA à la requête.
Stratégie AAA	StoreWSDLAAA	Identification et authentification LTPA Mappage de groupes pour l'autorisation Autorisation XACML.
Stratégie AAA	StoreXACMLFWAZ	Autorisation XACML pour PriceInfo.
Profil de proxy SSL	WSRRPP	Profil de proxy SSL pour le serveur WSRR.
Profil Crypto	WSRRCP	Profil Crypto pour le serveur WSRR.
Données d'identification de validation	WSRRVC	Les données d'identification de validation contiennent le certificat Crypto WSRRCERT. Tous les autres paramètres sont par défaut.
Crypto Certificate	WSRRCERT	WSRRCERT utilise le certificat de signataire. Ce certificat a été extrait de NodeDefaultKeyStore, certificat par défaut pour un serveur unique ou du certificat par défaut CMSKeyStore dans le cas d'un environnement ND au sein duquel un serveur HTTP IBM était présent.

Règles de traitement de la passerelle StoreWSP

La passerelle centrale de l'exemple est StoreWSP (Store Web Service Proxy). La stratégie associée à la passerelle contient une règle de demande et de réponse.

Règle de demande

L'action de règle principale de StoreWSP_default_request-rule est appelée AAA. Dans l'action AAA, le jeton LTPA est validé, les groupes d'utilisateurs sont extraits et une autorisation est lancée pour déterminer si l'utilisateur appartient au groupe LDAP Manager, Clerk ou Customer. Cette validation est exécutée lorsque l'étape

AAA AZ appelle le point de décision de règles (PDP) StoreWSDLPDP, sur le dispositif DataPower. Ce point de décision de règles (PDP) utilise la règle XACML storeWSPXACML.xml.

Règle de réponse

Dans la règle de réponse, StoreWSP_default_response-rule, la transformation appelle le service de pare-feu XML StoreXACMLFW.

Cette transformation détermine si l'utilisateur est autorisé à accéder aux informations sur les prix selon son appartenance au groupe Manager. S'il appartient à ce groupe, la variable *var:///context/response/displayFilter* est définie à `local:///allData.xsl`. Sinon, la variable *var:///context/response/displayFilter* est définie à `local:///noPriceInfo.xsl`.

La transformation exécute ensuite les actions de la feuille de style sur la réponse.

Règle de traitement de StoreXAMLFW

La feuille de style personnalisée storeSendToPDP.xsl effectue un appel au service de pare-feu XML StoreXACMLFW. Deux règles de traitement sont utilisées dans ce pare-feu. StoreXACMLFW_request contient une action unique de stratégie AAA qui utilise la transformation allData.xsl. Cette action AAA, StoreXACMLFWAZ, appelle à son tour l'action StorePDP du point de décision de règles XACML. L'utilisation de la règle XACML storePrivateDataXACML.xml permet d'effectuer une détermination pour savoir si l'utilisateur est autorisé à connaître les informations sur les prix.

Exemple de feuilles de style XSL

L'exemple d'application contient les feuilles de style suivantes dont le nom se termine par `.xsl` et qui se trouvent dans le répertoire local du domaine installé.

Tableau 16. Feuilles de style du modèle d'application

Feuille de style	Objet
`allData.xsl`	Feuille de style de type Identity qui copie toutes les données de la source vers la cible. Elle est utilisée pour la fonction de réécriture et pour l'appel à la passerelle XML XACML.
`apil-xacml-binding-new.xsl`	Utilise les informations de mappage de données d'identification pour créer une requête SOAP qui peut être traitée par le point de décision de règles (PDP) du dispositif DataPower. Cette feuille de style est une modification de la feuille de style tspm-xacml-binding-sample.xsl qui est fournie dans le répertoire de stockage du dispositif XI50 DataPower. La fonctionnalité principale de ce script adapté consiste à ajouter une variable accessible en externe qui rend l'information de l'objet de la requête XACML accessible à la feuille de style de réécriture.
`noPriceInfo.xsl`	Cette feuille de style définit l'élément de prix à la valeur 0.0.

Tableau 16. Feuilles de style du modèle d'application (suite)

Feuille de style	Objet
rgxacml.xsl	Cette feuille de style est une personnalisation de la feuille de style tspm-retrieve-groups.xsl du répertoire de stockage du dispositif DataPower. Cette feuille de style a pour objectif principal de fournir le nom distinctif LDAP, le nom d'hôte, le mot de passe, le port, etc. pour permettre à l'utilisateur entrant d'être reconnu et d'avoir ses informations de groupe extraites.
soavars.xsl	Il s'agit ici uniquement d'un exemple de feuille de style qui définit les informations LDAP dans des variables utilisées par la feuille de style rgxacml.xsl. Dans l'exemple, le mot de passe est chiffré, ce qui n'est pas une pratique de production.
storeCallPDP.xsl	Cette feuille de style dispose du code permettant d'appeler la passerelle XACML, gère les décisions Permit/Deny (autorisation/refus) et envoie la variable de filtrage pour exécuter allData.xsl ou noPriceInfo.xsl.
storeSendToPDP.xsl	Cette feuille de style construit une requête SOAP qui est envoyée à la passerelle XACML. Elle contient les informations sur le sujet obtenues dans la feuille de style apil-xacml-binding-new.xsl, les informations sur les ressources, les informations d'action et les informations d'environnement.

Objets DataPower qui utilisent des feuilles de style XSL

Les objets DataPower utilisent certaines feuilles de style XSL fournies avec le modèle d'application.

Tableau 17. Objets DataPower qui utilisent des feuilles de style XSL

Feuille de style	Objet
allData.xsl	Utilisée en interne dans la feuille de style storeCallPDP.xsl. La feuille de style est utilisée comme la transformation personnalisée d'une règle AAA StoreXACMLFWAZ.
apil-xacml-binding-new.xsl	Utilisée comme la feuille de style personnalisée dans l'étape AZ de la stratégie AAA StoreWSDLAAA.
noPriceInfo.xsl	Utilisée en interne dans la feuille de style storeCallPDP.xsl.
soavars.xsl	Utilisée en interne dans la feuille de style rgxacml.xsl.
storeCallPDP.xsl	Appelée sous la forme d'une transformation dans la règle Store_default-response.
storeSendToPDP.xsl	Utilisée en interne dans la feuille de style storeCallPDP.xsl.

Chapitre 6. Utilisation de l'instance déployée

Après le déploiement de l'un des modèles IBM SOA Policy Gateway Pattern, vous pouvez visualiser l'instance déployée en cliquant sur **Instances** > **Systèmes virtuels** dans la console Workload.

Affichage des détails de l'instance

Pour afficher les détails d'une instance déployée, sélectionnez-la dans la liste des instances de la fenêtre Instances de système virtuel. Les détails de l'instance du système virtuel s'affichent. Les détails incluent la liste des machines virtuelles mises à disposition dans l'infrastructure de cloud pour ce déploiement, l'adresse IP et le statut de la machine virtuelle.

Pour voir l'état de mise à disposition et de déploiement d'une instance, voir la valeur **Statut actuel** dans la vue détaillée.

Pour afficher le statut des machines virtuelles et des scripts lors de la mise à disposition, développez la section **Historique** dans la vue détaillée.

Pour afficher les détails des machines virtuelles et des journaux de script, développez la section **Machines virtuelles** dans la vue détaillée. L'hôte et l'adresse IP du système correspondent à la valeur **Interface réseau 0** dans la section **Matériel et réseau**. Les journaux de script sont accessibles dans la section **Packages de script**. Vous pouvez vous connecter aux consoles disponibles à l'aide des liens de la section **Consoles**.

Accès aux instances déployées

Après avoir déployé un modèle de système virtuel, vous pouvez afficher l'instance de système virtuel qui a été créée afin de voir votre environnement de IBM SOA Policy Gateway Pattern et ses composantes.

Avant de commencer

Pour afficher une instance de système virtuel, vous devez déployer un modèle de système virtuel.

Pourquoi et quand exécuter cette tâche

Le déploiement d'un modèle créé une instance du système virtuel, ou un environnement d'exécution IBM SOA Policy Gateway Pattern récemment mis à disposition. Une fois le déploiement terminé, l'instance de système virtuel s'exécute.

Procédure

Pour gérer les instances de système virtuel du IBM SOA Policy Gateway Pattern, procédez comme suit :

1. Cliquez sur **Instances** > **Systèmes virtuels** pour accéder à la fenêtre Instances de système virtuel.

2. De la liste d'instances dans la fenêtre d'Instances de système virtuel, sélectionnez l'instance qui a été déployée.
3. Si l'instance est en cours d'exécution, vous pouvez ouvrir une session dans les composants du système virtuel à partir des liens de la console dans la vue Système virtuel. Les composants disponibles dépendent du modèle que vous avez créé. Ils peuvent inclure les éléments suivants :
   - Console d'administration de WebSphere Application Server
   - Interface utilisateur Web WSRR
   - WSRR Business Space
   - DataPower WebGUI

Connexion à WSRR - Business Space

Gérez WSRR à l'aide de l'interface utilisateur de Business Space.

Pourquoi et quand exécuter cette tâche

Business Space est l'une des deux interfaces graphiques que vous pouvez employer pour travailler avec WSRR. Le centre de documentation de WSRR propose une description complète de l'utilisation de Business Space avec WSRR (voir lien connexe).

Vous pouvez vous connecter à l'instance WSRR Business Space dans votre modèle déployé en cliquant sur un lien dans la console de la charge de travail ou en entrant l'URL dans le navigateur Web.

Procédure

1. Pour vous connecter depuis la console Workload Console :
   a. Cliquez sur **Instances** > **Systèmes virtuels** pour accéder à la fenêtre Instances de système virtuel.
   b. Dans la liste des instances de la fenêtre Instances de système virtuel, sélectionnez votre système déployé.
   c. Cliquez **Machines virtuelles** dans la vue de détails du système pour développer la liste.
   d. Localisez WSRR dans la liste de machines virtuelles et cliquez le signe plus pour visualiser les détails.
   e. Sous la section **Consoles**, cliquez sur **WSRR_Business_Space**.
   f. Entrez l'ID et le mot de passe de l'utilisateur administrateur.
2. Pour vous connecter à un navigateur Web :
   a. Ouvrez un navigateur Web.
   b. Recherchez le nom d'hôte et les numéros de port pour WSRR. Affichez les détails de votre déploiement tel que décrit à l'étape 1. Développez la section **Machines virtuelles** et sélectionnez la machine virtuelle du serveur WSRR afin d'afficher les détails de la machine virtuelle. Dans la section **Matériel et réseau**, le nom d'hôte correspond à la valeur **Interface réseau 0**.
   c. Entrez l'URl de l'interface graphique de WSRR : http://*nom_hôte*:9443/BusinessSpace, dans laquelle *nom_hôte* est le nom d'hôte du serveur WSRR.
   d. Entrez l'ID et le mot de passe de l'utilisateur administrateur.

Résultats

Business Space est affiché, et peut être utilisée pour ajouter, éditer ou supprimer des règles de médiation, ainsi que d'autres artefacts.

Que faire ensuite

Si vous utilisez Business Space sur le système WSRR pour la première fois, reportez-vous à la section «Configuration de Business Space pour la première utilisation» et suivez les étapes pour créer l'espace Gouvernance SOA.

Information associée:

Centre de documentation d'IBM WebSphere Service Registry and Repository version 8.0

Configuration de Business Space pour la première utilisation

Pour pouvoir utiliser l'interface utilisation de Business Space et créer des règles, vous devez tout d'abord créer l'espace de gouvernance SOA.

Avant de commencer

Pour plus d'informations sur l'accès à Business Space, voir «Connexion à WSRR - Business Space», à la page 82.

Pourquoi et quand exécuter cette tâche

Pour utiliser les widgets de Business Space, vous devez créer un espace. Les espaces sont définis pour des rôles spécifiques. Une création de règle s'adapte mieux dans un espace de gouvernance de l'architecture SOA. Si un espace de gouvernance SOA n'existe pas encore, vous devez le créer. Pour créer un espace basé sur le modèle Service Registry for SOA Governance, procédez comme suit :

Procédure

1. En haut de la page, cliquez sur **Gérer les espaces**. La boîte de dialogue du gestionnaire d'espace Space Manager s'affiche.
2. Cliquez sur **Créer un espace**. La boîte de dialogue Créer un espace s'affiche.
3. Entrez un nom dans la zone **Nom de l'espace** ; par exemple, `Gouvernance SOA`. Vous pouvez également entrer une description.
4. Sélectionnez **Service Registry for SOA Governance** dans la liste **Créer un nouvel espace à l'aide d'un modèle**, puis cliquez sur **Sauvegarder**.
5. Le nouvel espace s'affiche dans la liste **Gestionnaire d'espaces**. Cliquez sur le nouvel espace pour l'ouvrir.

Résultats

L'espace Gouvernance SOA est créé. Pour ouvrir l'espace Gouvernance SOA, procédez comme suit :

1. Cliquez sur **Accéder aux espaces** en haut de la page. La boîte de dialogue Accéder aux espaces s'affiche.
2. Cliquez sur l'espace pour les utilisateurs SOA Governance. Le nom spécifique dépend des éléments spécifiés lors de la création de l'espace.

Que faire ensuite

Vous pouvez ajouter des actions supplémentaires au widget Service Registry Actions :

1. Dans Business Space, cliquez sur **Edit Page**.
2. Dans le widget Service Registry Actions, cliquez sur **Edit Settings**.
3. Sélectionnez les actions suivantes à afficher :
   - Créez une définition de niveau de service
   - Créez une version de service
   - Créez un accord sur les niveaux de service
   - Créez une fonctionnalité métier
4. Dans le widget Service Registry Actions, cliquez sur **Save and Close**.
5. Cliquez sur **Finish Editing**.

Connexion à WSRR - Interface utilisateur Web WSRR

L'interface graphique Web WSRR permet de travailler avec WSRR.

Pourquoi et quand exécuter cette tâche

L'interface utilisateur Web WSRR est l'une des deux interfaces graphiques que vous pouvez employer pour travailler avec WSRR. Le centre de documentation de WSRR propose une description complète de l'utilisation de l'interface utilisateur Web WSRR (voir lien connexe). Le plus souvent, vous souhaiterez utiliser l'interface Business Space mais certaines tâches (comme la création de règles de surveillance) doivent être réalisées dans l'interface utilisateur Web WSRR.

Vous pouvez vous connecter à l'instance graphique Web WSRR dans votre modèle déployé en cliquant sur un lien dans la console de la charge de travail ou en entrant l'URL dans le navigateur Web.

Procédure

1. Pour vous connecter depuis la console Workload Console :
   a. Cliquez sur **Instances** > **Systèmes virtuels** pour accéder à la fenêtre Instances de système virtuel.
   b. Dans la liste des instances de la fenêtre Instances de système virtuel, sélectionnez votre système déployé.
   c. Cliquez **Machines virtuelles** dans la vue de détails du système pour développer la liste.
   d. Localisez WSRR dans la liste de machines virtuelles et cliquez le signe plus pour visualiser les détails.
   e. Sous la section **Consoles**, cliquez sur **WSRR_Web_UI**.
   f. Entrez l'ID et le mot de passe de l'utilisateur administrateur.
2. Pour vous connecter à un navigateur Web :
   a. Ouvrez un navigateur Web.
   b. Recherchez le nom d'hôte et les numéros de port pour WSRR. Affichez les détails de votre déploiement tel que décrit à l'étape 1. Développez la section **Machines virtuelles** et sélectionnez la machine virtuelle du serveur WSRR afin d'afficher les détails de la machine virtuelle. Dans la section **Matériel et réseau**, le nom d'hôte correspond à la valeur **Interface réseau 0**.

c. Entrez l'URl de l'interface graphique de WSRR : http://*nom_hôte*:9443/ServiceRegistry, dans laquelle *nom_hôte* est le nom d'hôte du serveur WSRR.
d. Entrez l'ID et le mot de passe de l'utilisateur administrateur.

Information associée:

Centre de documentation d'IBM WebSphere Service Registry and Repository version 8.0

Connexion à la console d'administration de WebSphere Application Server

Utilisez la console d'administration d'Application Server de WebSphere pour régler avec précision des paramètres de sécurité et pour effectuer d'autres tâches d'administration.

Pourquoi et quand exécuter cette tâche

Le centre de documentation fournit les documents complets sur le fonctionnement de la console d'administration WebSphere Application Server. Suivez le lien connexe.

Vous pouvez vous connecter à la console d'administration de WebSphere Application Server dans votre modèle déployé en cliquant sur un lien dans la console de la charge de travail ou en entrant l'URL dans le navigateur Web.

Procédure

1. Pour vous connecter depuis la console Workload Console :
   a. Cliquez sur **Instances** > **Systèmes virtuels** pour accéder à la fenêtre Instances de système virtuel.
   b. Dans la liste des instances de la fenêtre Instances de système virtuel, sélectionnez votre système déployé.
   c. Cliquez **Machines virtuelles** dans la vue de détails du système pour développer la liste.
   d. Localisez WSRR dans la liste de machines virtuelles et cliquez le signe plus pour visualiser les détails.
   e. Sous la section **Consoles**, cliquez sur **WebSphere**.
   f. Entrez l'ID et le mot de passe de l'utilisateur administrateur.
2. Pour vous connecter à un navigateur Web :
   a. Ouvrez un navigateur Web.
   b. Recherchez le nom d'hôte et les numéros de port pour WSRR. Affichez les détails de votre déploiement tel que décrit à l'étape 1. Développez la section **Machines virtuelles** et sélectionnez la machine virtuelle du serveur WSRR afin d'afficher les détails de la machine virtuelle. Dans la section **Matériel et réseau**, le nom d'hôte correspond à la valeur **Interface réseau 0**.
   c. Entrez l'URl de l'interface graphique de WSRR : http://*nom_hôte*:9043/ibm/console, dans laquelle *nom_hôte* est le nom d'hôte du serveur WSRR.
   d. Entrez l'ID et le mot de passe de l'utilisateur administrateur.

Information associée:

Centre de documentation de WebSphere Application Server V8.0

Connexion à la console d'un dispositif DataPower virtuel

Utilisez la console DataPower pour configurer le point d'application de la règle (PEP, Policy Enforcement Point).

Pourquoi et quand exécuter cette tâche

Le centre de documentation WebSphere DataPower comporte les détails complets de configuration de votre passerelle. Suivez le lien connexe.

Vous vous connectez à la console à l'aide d'un navigateur Web. Pour récupérer les détails de connexion, vous visualisez le modèle déployé dans la console Workload Console.

Procédure

1. Récupérez les détails dont vous avez besoin à l'aide de la console Workload Console :
   a. Cliquez sur **Instances** > **Systèmes virtuels** pour accéder à la fenêtre Instances de système virtuel.
   b. Dans la liste des instances de la fenêtre Instances de système virtuel, sélectionnez votre système déployé.
   c. Dans la vue de détail, développez la section **Machines virtuelles** et sélectionnez la machine virtuelle du dispositif DataPower pour afficher les détails de la machine virtuelle. Dans la section **Matériel et réseau**, le nom d'hôte correspond à la valeur **Interface réseau 0**.
2. Dans un navigateur Web, saisissez l'URL `https://`*`nom_hôte`*`:9090/dp`, dans lequel *nom_hôte* est le nom d'hôte de votre dispositif virtuel.

Information associée:

Centre de documentation de WebSphere DataPower 6.0

Connexion à la console de contrôle

Utilisez la console de contrôle pour visualiser les informations de surveillance.

Pourquoi et quand exécuter cette tâche

Accédez à la console de contrôle depuis la fenêtre Instances de système virtuel.

La fonctionnalité de surveillance est fournie par ITCAM for SOA. Téléchargez la documentation à partir du lien connexe pour plus d'informations, puis recherchez les informations sur les installations DataPower.

Procédure

1. Cliquez sur **Instances** > **Systèmes virtuels** pour accéder à la fenêtre Instances de système virtuel.
2. De la liste d'instances dans la fenêtre d'Instances de système virtuel, sélectionnez l'instance qui a été déployée. Les détails de l'instance s'affichent.
3. Développez la section **Machines virtuelles** et sélectionnez la machine virtuelle que vous souhaitez surveiller.
4. Sous **Informations générales**, recherchez **Surveillance** et cliquez sur le lien **Cliquer pour ouvrir**.

Information associée:

Documentation ITCAM for SOA 7.2.1 (de Fix Central)

Arrêt et démarrage de l'instance déployée

Vous pouvez arrêter et démarrer l'instance déployée dans la console de la charge de travail. Vous pouvez arrêter et démarrer des machines virtuelles individuelles dans le modèle.

Pour arrêter une instance déployée en cours d'exécution :

1. Sélectionnez **Instances** > **Systèmes virtuels** et sélectionnez l'instance dans la liste **Instances de système virtuel**.
2. Cliquez sur l'icône **Arrêt** dans la barre de titre de l'instance.

Pour démarrer une instance déployée arrêtée :

1. Sélectionnez **Instances** > **Systèmes virtuels** et sélectionnez l'instance dans la liste **Instances de système virtuel**.
2. Cliquez sur l'icône **Démarrage** dans la barre de titre de l'instance.

Remarque : Un défaut connu dans DB2 10.1.0.2 se produit dans les processus DB2 qui ne redémarrent pas toujours lorsque l'instance s'arrête et redémarre. Dans ce cas, vous devez démarrez le processus manuellement en vous connectant au noeud DB2 en tant que db2inst1 et en exécutant **db2start**. Vous pouvez également avoir besoin de redémarrer les processus WSRR sur les noeuds WSRR.

Pour arrêter différentes machines virtuelles.

1. Développez la section **Machines virtuelles** de l'affichage de l'instance.
2. Sélectionnez le lien **Gérer** pour la machine que vous voulez arrêter.
3. Cliquez l'icône d'arrêt dans la barre de gestion.

Pour démarrer différentes machines virtuelles.

1. Développez la section **Machines virtuelles** de l'affichage de l'instance.
2. Sélectionnez le lien **Gérer** pour la machine que vous voulez démarrer.
3. Cliquez l'icône de démarrage dans la barre de gestion.

Vous pouvez arrêter et démarrer WSRR et DB2 depuis la ligne de commande. Cliquez sur le lien **Connexion** pour vous connecter à l'aide de la console SSH.

Vous arrêtez et démarrez WSRR en arrêtant et démarrant le profil WebSphere Application Server. Voir Gestion des profils à l'aide de commandes dans le centre de documentation WebSphere Application Server.

Dans le modèle avancé, une fois que le DMGR et les noeuds personnalisés ont redémarré, le cluster WSRR doit redémarrer. Pour ce faire, ouvrez la console d'administration WebSphere Application Server et sélectionnez **Serveus** > **Clusters** > **Clusters WebSphere Application Server**. Sélectionnez **WSRRCluster_1**, puis cliquez sur **Démarrage**.

Vous pouvez arrêter et démarrer DB2 à l'aide des commandes système. Voir Commandes système dans le centre de documentation DB2.

Configuration d'un modèle de post-déploiement

Après avoir déployé les modèles, vous devez configurer la sécurité ainsi que d'autres paramètres.

Configuration du point d'application de règles

Le dispositif ou l'instance DataPower est le point d'application de règles (PEP, Policy Enforcement Point) du modèle IBM SOA Policy Gateway Pattern. Lors du déploiement du domaine d'application, il est possible de créer le contenu de ce domaine.

Procédure

Lors de l'installation de vos configurations, assurez-vous que différents noms de domaine sont utilisés sur chaque dispositif DataPower, de sorte que des données correctes s'affichent dans les espaces de travail de topologie ITCAM pour SOA.
Créez un proxy de service Web (WSP, Web Service Proxy) :

1. Dans le panneau de commande de DataPower, cliquez sur **Web Service Proxy**.
2. Cliquez sur **Add** (Ajouter) et entrez un nom pour le proxy.
3. Ouvrez l'onglet **WSRR Subscription** (Abonnement WSRR). Dans la liste WSRR Server, cliquez sur **WSRRSVR**.
4. Complétez les autres informations requises, comme Front Side Handler, l'espace de nom, le nom de l'objet, etc., pour créer la configuration du proxy de services Web (Web Service Proxy).

Créez des règles pour le WSP (Web Service Proxy) :

5. Ouvrez l'onglet **Policy** pour l'éditeur de proxy de service Web (WSP Editor).
6. Cliquez sur **Processing Rules** (Traitement des règles) au niveau approprié. Vous pouvez créer une règle ou modifier la règle par défaut fournie. L'action de stratégie de clés à ajouter est **AAA Action**. Cette action gère l'identification, l'authentification et l'autorisation qui sont des données importantes pour le modèle.

   Les éléments importants que vous devez spécifier pour l'action AAA incluent l'entrée et la sortie, ainsi que la stratégie AAA. Vous pouvez créer la règle durant la création de l'action de stratégie AAA ou vous pouvez la créer préalablement à l'aide de l'éditeur AAA.

   - L'identification est l'étape durant laquelle l'utilisateur est identifié. Dans notre exemple, deux formes d'identification sont employées. Dans le pare-feu XML StoreAddLTPA, l'identification a été effectuée avec une authentification de base. Dans le pare-feu StoreWSP, l'identification a été fournie par le jeton LTPA.
   - L'authentification est l'étape dans laquelle il est admis que l'utilisateur est connu du système. Vous avez le choix parmi de nombreuses options. Ici, deux exemples sont présentés ; dans le premier, l'utilisateur était recherché à l'aide de LDAP et dans le deuxième, il a été accepté au moyen d'un jeton LTPA valide.
   - L'autorisation est l'étape dans laquelle l'utilisateur est autorisé pour la ressource, ici, les opérations de service Web. Les éléments importants suivants doivent être spécifiés pour utiliser une autorisation de point de décision de règles XACML du dispositif DataPower :
     - La méthode : **Use XACML Authorization** (Utiliser une autorisation XACML).
     - La version XACML ; par exemple 2.0.
     - Le type de point de décision de règles (PDP) ; par exemple, PDP fondé sur un refus.
     - L'utilisation du point de décision de règles du dispositif DataPower : **On** (activé)
     - Le nom du point de décision de règles (PDP), dont XACML est spécifié.

– Configurez le point de décision de règles (PDP). Pour plus d'informations, voir «Modification du point de décision de règles XACML sous DataPower», à la page 71.
– La feuille de style XSL personnalisée pour lier AAA et XACML : utilisez `apil-xacml-bindingnew.xsl` comme point de départ.

Pour configurer la passerelle afin qu'elle utilise la rédaction :

7. Modifiez le fichier XACML `.xml` pour l'adapter aux règles de sécurité que vous souhaitez appliquer à la rédaction.
8. Créez un pare-feu XML avec une action AAA qui suit l'exemple de rédaction.
9. Modifiez le point de décision de règles (PDP) utilisé par l'action AAA ci-dessus pour pointer sur la feuille de style que vous utilisez pour appliquer la rédaction.
10. Copiez et modifiez la feuille de style `storeCallPDP.xsl`, qui crée la charge SOAP pour le service XACML. En particulier, assurez-vous que l'action et la ressource correspondent à vos exigences pour le document de stratégie XACML que vous avez créé.
11. Vérifiez que votre feuille de style modifiée appelle le port approprié pour votre nouveau pare-feu XML XACML.

Objets DataPower créés dans les modèles d'exécution basique et d'exécution avancée

Présentation des objets DataPower créés dans les modèles d'exécution basique et d'exécution avancée, ainsi que leur fonction.

Tableau 18. Objets du modèle DataPower

Objet	Description
Domaine	Domaine utilisable pour l'application des utilisateurs.
Serveur WSRR	WSRRSVR nommé. L'adresse URL, le nom d'utilisateur et le mot de passe SOAP sont configurés ainsi que le profil de proxy SSL avec les données d'identification de validation.
Profil de proxy SSL	WSRRPP nommé, il s'agit d'un profil (client) transmis. Il utilise le profil Crypto WSRRCP. Toutes les autres valeurs par défaut sont utilisées.
Profil Crypto	WSRRCP contient un objet de données d'identification de validation WSRRVC, qui contient le certificat de signataire qui a été téléchargé comme élément de scripts de modèles.
Données d'identification de validation	Les données d'identification de validation WSRR contiennent le certificat Crypto Certificate WSRRCERT. Tous les autres paramètres sont par défaut.
Crypto Certificate	WSRRCERT utilise le certificat de signataire. Ce certificat a été extrait de NodeDefaultKeyStore, certificat par défaut pour un serveur unique ou du certificat par défaut CMSKeyStore dans le cas d'un environnement ND au sein duquel un serveur HTTP IBM était présent.

L'exemple utilise la définition de serveur WSRR dans le proxy de service Web :

1. Dans le panneau de commande de DataPower, cliquez sur **Web Service Proxy**.
2. Cliquez sur **Ajouter** et indiquez un **Nom** pour le Proxy.
3. Web Service ProxyEnsuite, sélectionnez l'onglet **WSRR Subscription** (Abonnement WSRR)

4. Sélectionnez WSRR Server dans le menu. L'objet WSRRSVR est accessible.
5. Complétez les autres informations requises, comme Front Side Handler, l'espace de nom, le nom de l'objet, etc., pour créer la configuration du proxy de services Web (Web Service Proxy).

Valeurs de noms distinctifs de certificats pour des certificats DataPower

Si vous utilisez SSL avec les modèles IBM SOA Policy Gateway Pattern fournis, la vérification d'hôte des noms distinctifs (DN) est plus stricte que la sécurité par défaut de WebSphere Application Server. (Cette rubrique s'applique aux dispositifs DataPower externes.)

La vérification d'hôte des noms distinctifs n'est pas activée par défaut dans WebSphere Application Server. Notez que dans les packages de script utilisés par les modèles IBM SOA Policy Gateway Pattern, la vérification d'hôte des noms distinctifs est activée et il n'est pas possible de la désactiver. Un certificat spécifique qui fonctionne entre le système WebSphere Application Server par défaut et DataPower risque de ne pas fonctionner pour le package de script «SOA Policy Gateway 2.5.0.0 - Security» ou le package de script «SOA Policy Gateway 2.5.0.0 - Sample» utilisé avec le modèle IBM SOA Policy Gateway Pattern. Par exemple, le nom distinctif `myserver.yourcompany.com` serait accepté comme nom par défaut par WebSphere Application Server, mais pas par les modules d'extension de scripts. Pour ajouter ou supprimer les certificats DataPower utilisés avec le déploiement, voir «Suppression ou ajout de certificats DataPower au fichier de clés certifiées WSRR».

Suppression ou ajout de certificats DataPower au fichier de clés certifiées WSRR

Cette tâche décrit comment ajouter ou supprimer des certificats DataPower. Cette rubrique s'applique aux modèles déployés avec des dispositifs DataPower externes.

Pourquoi et quand exécuter cette tâche

Les certificats DataPower sont téléchargés vers le magasin de clés certifiées WSRR afin de simplifier la mise à jour de la synchronisation entre WSRR et DataPower dans le cadre des mises à jour des règles. Si cette fonction n'est pas nécessaire, vous pouvez supprimer des certificats DataPower. Vous pouvez également ajouter des certificats DataPower si les certificats doivent être modifiés.

Procédure

1. Pour supprimer des certificats :
   a. Connectez-vous à la console d'administration WebSphere Application Server à l'adresse `https://`*`nom_hôte`*`:9043/ibm/console`, où *nom_hôte* est le nom d'hôte du système WSRR. Entrez le nom et le mot de passe de l'utilisateur administrateur.
   b. Accédez à **Security, SSL certficates and key management**.
   c. Cliquez sur **Key Stores and Certificates**.
   d. Cliquez sur **NodeDefaultTrustStore** si votre déploiement est basé sur un modèle d'exécution basique, ou sur **CellDefaultTruststore** si vous avez déployé un modèle d'exécution avancée.
   e. Cliquez sur **Certificats de signataire**.
   f. Sélectionnez les cases à cocher des certificats que vous souhaitez supprimer.

g. Cliquez sur **Supprimer**.
h. Cliquez sur **Enregistrer**.

2. Pour ajouter de nouveaux certificats DataPower, cliquez sur **Ajouter** pour ajouter le nouveau certificat.
   a. Connectez-vous à la console d'administration WebSphere Application Server à l'adresse `https://nom_hôte:9043/ibm/console`, où *nom_hôte* est le nom d'hôte du système WSRR. Entrez le nom et le mot de passe de l'utilisateur administrateur.
   b. Accédez à **Security, SSL certficates and key management**.
   c. Cliquez sur **Key Stores and Certificates**.
   d. Cliquez sur **NodeDefaultTrustStore** si votre déploiement est basé sur un modèle d'exécution basique, ou sur **CellDefaultTruststore** si vous avez déployé un modèle d'exécution avancée.
   e. Cliquez sur **Certificats de signataire**.
   f. Cliquez sur **Ajouter** et indiquez les nouveaux certificats.
   g. Cliquez sur **Enregistrer**.

Changement des clés LTPA

Cette procédure décrit comment changer la clé LTPA. La clé LTPA est partagée parmi toutes les cellules des modèles. Elle n'est pas utilisée dans le modèle SOA Policy Gateway Basic Runtime Sample. La clé LTPA est exportée à partir de Governance Master et importée dans les environnements d'exécution, comme transfert ou production.

Pourquoi et quand exécuter cette tâche

Vous effectuez ces actions dans la console d'administration WebSphere Application Server. Pour plus d'informations, suivez le lien connexe.

Procédure

1. Exportez la nouvelle clé LTPA à partir du Dmgr du maître de gouvernance WSRR.
2. Importer la clé LTPA dans les instances de l'environnement d'exécution WSRR, qui sont Dmgr ou Stand Alone.
3. Si l'instance de l'environnement d'exécution est basée sur un modèle d'exécution avancée, effectuez les actions suivantes dans l'ordre :
   a. Synchronisez tous les noeuds.
   b. Arrêtez le cluster WSRR.
   c. Arrêtez les agents de noeud.
   d. Arrêtez le Dmgr.
4. Si le système WSRR est basé sur un modèle d'exécution avancée, il doit être démarré dans l'ordre inverse :
   a. Démarrez le Dmgr.
   b. Démarrez les agents de noeud.
   c. Démarrez le cluster WSRR.
5. Si le WSRR est un serveur autonome (basé sur un modèle d'exécution basique), vous devez l'arrêter et le redémarrer pour que le changement de clé LTPA prenne effet.

Information associée:

Création et gouvernance des services

Utilisez l'interface utilisateur de WSRR Business Space pour créer et administrer des services métier et leurs objets associés.

L'espace SOA Governance doit être créé dans l'espace métier avant de pouvoir créer des règles. Si l'espace de gouvernance SOA n'existe pas, reportez-vous à «Configuration de Business Space pour la première utilisation», à la page 83 et suivez les étapes pour créer l'espace.

Pour plus d'informations sur la création d'un service gouverné (administré), voir IBM WebSphere Service Registry and Repository Version 8.0 - Centre de documentation - Tutoriel : Gouvernance d'un nouveau service.

Pour plus d'informations sur l'administration d'un service existant, voir IBM WebSphere Service Registry and Repository Version 8.0 - Centre de documentation - Tutoriel : Gouvernance d'un service existant.

Tâches associées:

«Connexion à WSRR - Business Space», à la page 82
Gérez WSRR à l'aide de l'interface utilisateur de Business Space.

Règles

Détails de l'implémentation pour utiliser WSRR comme point de création de règle (PAP, Policy Authoring Point) et WebSphere DataPower comme point d'application de règles (PEP, Policy Enforcement Point) lorsque vous créez des règles de médiation.

Règles dans WSRR

Vous pouvez utiliser WSRR pour créer toutes les règles SOA, notamment les règles d'accord sur les niveaux de licence (SLA, Service Level Agreement), les règles de médiation, les règles de contrôle et les règles personnalisées. L'interface utilisateur de Business Space vous permet de créer, de mettre à jour ou de supprimer un document de règles dans WSRR. Le document de règles peut contenir une expression de règles qui spécifie plusieurs règles pour un domaine de règles spécifique. Vous pouvez également créer un document de règles qui rassemble des règles existantes issues d'autres documents. Les règles individuelles sont consultées à l'aide identificateurs de règles, que vous spécifiez lorsque vous ajoutez des règles à votre document. Une expression de règles représente la déclaration d'une règle. Elle est équivalente à un élément `<wsp:Policy>` contenu dans un document WS-Policy.

Pour créer une règle de médiation dans Business Space, voir «Création de règles de médiation», à la page 98.

Assertions de règles de médiation

Les accords sur les niveaux de licence (SLA, Service Level Agreement) proviennent d'une exigence exprimée par l'entreprise pour laquelle la qualité de service fournie par un service répond à une norme spécifique. A mesure qu'un service se conçoit, des exigences fonctionnelles sont créées pour guider la logique de ce que le service a à réaliser. Parallèlement à cela, des exigences non fonctionnelles sont spécifiées

dans le cadre de l'analyse et de la conception dudit service pour qualifier la qualité de service attendue avec la fourniture du service. Par exemple, l'entreprise peut avoir un service qui fournit des informations en réponse à une requête de client transmise par Internet. La cible consiste à renvoyer la réponse dans les 3 secondes. Dans le cadre d'une opération de transaction conduite de bout en bout, il a été déterminé que ce service doit renvoyer ses informations dans les 2 secondes pour satisfaire les exigences métier non fonctionnelles.

Vous pouvez écrire une règle qui implémente des contrôles d'exécution sur les performances du service et qui agit pour garantir que le service satisfait son SLA. Par exemple, vous pouvez avoir un noeud final principal de service qui est normalement en mesure (95% du temps) de fournir une réponse de service dans les 2 secondes. L'architecte SOA crée un noeud final secondaire sur un autre serveur qui peut être utilisé comme noeud de secours automatique en cas d'indisponibilités du noeud final principal, mais est également autorisé à être utilisé pour le trafic de dépassement lorsque le noeud final principal n'est pas en mesure de faire face à la charge des transactions. Vous pouvez écrire une règle qui vérifie le temps de réponse du service et réacheminent le trafic si nécessaire pour se conformer au SLA.

Voici un autre exemple de gestion des accords sur les niveaux de service (SLA) par le biais d'une régle d'exécution, prenons une situation dans laquelle un service répond à des transactions ayant différents consommateurs, chacun ayant un niveau de priorité différent. Un exemple simple peut comporter des consommateurs "Gold" et "Bronze", dans lequel l'entreprise garantit uniquement une qualité de service spécifique aux consommateurs "Gold". Dans cet exemple, vous pouvez vérifier que si le consommateur est "Gold", il est réacheminé vers le noeud final secondaire, alors que nous laissons le consommateur "Bronze" être confronté à des temps de réponse plus longs. L'entreprise a pris cette décision car le revenu incrémentiel des consommateurs "Bronze" est insuffisant pour justifier des frais associés à des temps de réponse d'ingénierie permettant de répondre au SLA des consommateurs "Gold".

Dans un troisième exemple, vous pouvez identifier une situation dans laquelle un service conduit au mieux ses opérations, mais lorsque celui-ci détermine qu'il est phase de chargement, il se voit contraint de mettre en file d'attente voire de refuser des messages issus de services consommateurs à priorité faible. Prenons comme exemple, une routine en traitement par lots qui inonde le système avec des demandes de consommateurs à un moment inattendu. Afin de protéger la qualité de service du service, vous pouvez créer une règle d'exécution qui est active uniquement pendant les heures ouvrables et qui rejette toutes les demandes en traitement par lots arrivant durant cette période.

Plus généralement, la règle de médiation prend en compte la validation et la transformation sur le message entrant provenant du client (consommateur) avant sa présentation au serveur (fournisseur).

Règles prenant en charge ce type de validation et de transformation de messages. Il est possible de spécifier des règles pour un service de fournisseur uniquement, pour une paire consommateur-fournisseur spécifique ou pour des consommateurs anonymes en rapport avec un service de fournisseur. Les règles destinées aux consommateurs anonymes offrent un moyen de définir une règle par défaut qui s'applique uniquement à des consommateurs pour lesquels aucune autre règle ne s'applique. Cette caractéristique va permettre à des règles d'être spécifiées pour des consommateurs indésirables qui ne s'identifient pas eux-mêmes. De tels services de consommateurs peuvent très bien avoir ensuite leurs transactions rejetées. Ceci

peut s'avérer utile pour prévenir une attaque par saturation de pirates informatiques tentant d'inonder le système avec les transactions visant à abattre le service d'un fournisseur.

Conditions de règle de médiation

Des assertions de médiation peuvent être effectuées, ce qui permet à une règle d'exécution de contrôler l'accord sur les niveaux de service (SLA) du service, la transformation des messages du consommateur au fournisseur ou de valider le schéma du message du consommateur.

Les conditions de règles d'accord sur les niveaux de service (SLA), un type spécifique de règle de médiation, tiennent compte effectivement d'une construction classique "if-then-else" avec une condition, puis d'un ensemble d'actions à exécuter selon le mode d'évaluation de la condition. La spécification d'une condition est facultative. Si aucune condition n'est spécifiée, il s'agit alors d'une opération équivalente à une condition logique d'évaluation à True et toutes les actions spécifiées sont mises en application en conséquence.

Si spécifiée, la condition doit être une expression booléenne ou une spécification de planification ou la condition peut inclure les deux.

Planification

Si spécifiée, la planification identifie les moments où la règle s'applique. Les dates et l'heure sont évaluées par le point d'application de règles (PEP, Policy Enforcement Point) local et le fuseau horaire du point d'application de règles. Si aucune planification n'est spécifiée, la règle démarre dès qu'elle est téléchargée du point de création de règles (PAP, Policy Authoring Point) au point d'application de règles (PEP, Policy Enforcement Point), et se poursuit indéfiniment.

La planification définit une date de démarrage et une date d'arrêt, toutes deux facultatives, une période quotidienne facultative et une liste facultative de jours de la semaine. Par exemple, vous pouvez définir une planification devenant effective du 1er octobre 2012 au 30 octobre 2012, de 8h00 à 17h00 les mercredis et dimanches.

Les paramètres de planification qui peuvent être indiqués sont les suivantes :

- **StartDate** - Cet attribut facultatif indique la date au format xs:date à laquelle la planification devient effective. L'attribut StartDate est inclusif et s'il est maquant, la planification devient effective immédiatement ce jour même. (Cliquez sur le lien hypertexte xs:heure pour vous informer sur cette norme de l'industrie).
- **StopDate** - Cet attribut facultatif indique la date au format xs:date à laquelle la planification cesse d'être effective. La date de fin est exclusive et la date spécifiée doit être postérieure à la date de début. Si la date de fin est antérieure ou identique à la date de départ, la planification ne démarre jamais. Si cet attribut est manquant, la planification est effective indéfiniment.
- **Daily** (Quotidien) - Cet élément facultatif indique la période quotidienne durant laquelle la planification est effective. Si cet attribut est manquant, la planification est effective toute la journée.
  - **StartTime** (Heure de début) – Si l'attribut Daily est spécifié, l'attribut StartTime est obligatoire. Il indique, au format xs:heure, l'heure à laquelle la planification démarre chaque jour. (Cliquez sur le lien hypertexte xs:heure pour vous informer sur cette norme de l'industrie).

– **StopTime** (Heure de fin) – Si l'attribut Daily est spécifié, l'attribut StopTime est obligatoire. Il indique, au format xs:heure, l'heure à laquelle la planification s'arrête chaque jour. L'attribut StopTime est exclusif et si l'heure spécifiée est antérieure ou identique à l'heure de début quotidienne, la planification s'arrête le jour suivant à l'heure de fin spécifiée.

- **Weekdays** (Jours de semaine) - Cet attribut facultatif indique les jours de la semaine inclus dans la planification. Si cet attribut est manquant, tous les jours de la semaine sont compris dans la planification. Cet attribut n'affecte que le début de la période quotidienne puisque l'exécution des planifications est autorisée une fois passé minuit. Par exemple, si une planification est définie pour démarrer à 23 heures et s'exécuter pendant 2 heures les mercredis, la planification se termine en réalité le jeudi à 01h00.
  – **Days** (Jours) - Si l'attribut Weekdays est spécifié, cet attribut est obligatoire. Il répertorie les jours de la semaine inclus dans la planification, sous la forme d'une liste de noms séparés par le signe ('+'), par exemple "Monday+Tuesday+Wednesday+Thursday+Friday+Saturday+Sunday" (lundi+mardi+mercredi+jeudi+vendredi+samedi+dimanche).

Expression de condition d'une règle de médiation

L'expression de condition, si spécifiée, est un élément non répétitif qui indique une expression booléenne.

L'expression se compose de trois paramètres (un attribut, un opérateur et une valeur) plus deux paramètres facultatifs d'intervalle et de limite. Si l'application de l'opérateur sur l'attribut et la valeur, plus l'intervalle et la limite, le cas échéant, s'évalue à True, l'expression est évaluée à True (Vrai). L'élément de limite n'est utilisé qu'avec les opérateurs HighLow et TokenBucket. Si non spécifiée, la valeur de Limit est 0. Si Interval n'est pas spécifié, la valeur par défaut est 60 secondes.

Les paramètres de l'expression peuvent être spécifiés comme suit :

- **Attribut** - Le tableau suivant récapitule les attributs définis et leur type.

Tableau 19. Attributs définis

Attribut	Description et Type
ErrorCount	Nombre d'erreurs observées au cours de cet intervalle de contrôle.
MessageCount	Nombre de messages réels interceptés au cours de l'intervalle de contrôle.
InternalLatency	Temps d'attente interne (temps de traitement) en secondes.
BackendLatency	Temps d'attente du dispositif au serveur, exprimé en secondes.
TotalLatency	Le total des temps d'attente d'arrière plan et interne, exprimé en secondes.

- **Opérateur** - Le tableau suivant récapitule les opérateurs disponibles et leur signification :

Tableau 20. opérateurs

Opérateur	Signification
GreaterThan	Algorithme numérique simple qui évalue à True lorsque l'attribut est supérieur à la valeur définie.

Tableau 20. opérateurs (suite)

Opérateur	Signification
LessThan	Algorithme numérique simple qui évalue à True lorsque l'attribut est inférieur à la valeur définie.
TokenBucket	Algorithme basé sur le taux qui autorise des pics. L'algorithme est constitué d'une pile contenant une capacité maximale de jetons Limite. La pile se remplit à une vitesse constante de jetons Valeur par Intervalle, alors que pour chaque unité d'Attribut, un jeton est retiré. Cet algorithme renvoie la valeur True lorsqu'il n'y a pas de jetons dans la pile, sinon renvoie la valeur False. Voici un exemple permettant d'expliquer l'algorithme : supposons que Limite=100, Valeur=5, Intervalle=1 seconde et Attribut=MessageCount. 1. La pile démarre pleine avec une capacité maximale de 100 jetons. 2. A l'arrivée d'un message, l'algorithme vérifie si la pile possède des jetons. a. Si c'est le cas, l'algorithme renvoie False (Faux) et un seul jeton est retiré de la pile b. Sinon, l'algorithme renvoie True. 3. Ce faisant, toutes les secondes, l'algorithme rajoute 5 jetons à la pile tant qu'il reste de la place.
HighLow	Algorithme qui renvoie True si l'attribut atteint le seuil supérieur spécifié comme valeur, puis continue de renvoyer True jusqu'à ce que Attribut atteigne le seuil bas spécifié comme Limite.

- **Value** (Valeur) – Il s'agit d'un élément entier positif. "0" (zéro) est une valeur valide.
- **Interval** - Cet élément facultatif définit l'intervalle de temps, utilisé comme une fenêtre dynamique, pour mesurer l'attribut wsme:Attribute lors de l'évaluation de l'expression, au format xs:durée. Si non spécifié, l'intervalle utilisé est de 60 secondes. Si indiqué, il convient de spécifier une valeur raisonnable, prenant en compte les fonctions configurées du point d'application de règles (PEP). Autrement dit, plus la valeur est élevée, plus le point d'application de règles requiert de mémoire pour conserver une trace de l'attribut. (Cliquez sur le lien hypertexte xs:durée pour vous informer sur cette norme de l'industrie).
- **Limit** (Limite) - Cet élément entier facultatif définit l'argument Limite supplémentaire requis lorsque wsme:Operator est TokenBucket ou HighLow. L'unité dépend de la spécification de wsme:Operator.

  Si wsme:Operator est HighLow, ceci définit le seuil bas tandis que wsme:Value définit le seuil haut. Le seuil spécifié doit être inférieur à wsme:Value. Sans spécification de ce type, la valeur par défaut de Limite est 0 (zéro).

  Si wsme:Operator est TokenBucket, il définit la taille maximale de la rafale ou le nombre maximal de jetons dans la pile, alors Valeur indique la vitesse à laquelle la pile se remplit, en nombre de jetons par intervalle. Si non spécifié, la valeur par défaut de Limite est 0 (zéro) et TokenBucket est alors équivalent à une opération GreaterThan.

Action d'une règle de médiation

L'élément Mediation Action (action de médiation) indique les actions à entreprendre. Bien que la syntaxe autorise de nombreuses combinaisons, celles-ci

ne sont pas toutes significatives et lorsque des actions en conflit sont spécifiées, comme demander qu'un message soit à la fois mis en file d'attente et supprimé, le point de création de règles rejette ce comportement. Les actions de la règle de médiation autorisées sont les suivantes :

- **QueueMessage** – Cette action indique que des transactions sont mises en file d'attente si la condition logique est satisfaite. Le traitement de message n'est pas reconduit tant que la condition logique est satisfaite. La méthodologie de file d'attente et tous les délais d'attente associés sont comme définis par le point d'application de règles (PEP), dans ce cas WebSphere DataPower. Lorsque plusieurs actions sont spécifiées, au sein d'un même élément Action, QueueMessage doit être la première action.
- **RejectMessage** – Cette action indique que des transactions sont rejetées si la condition logique est satisfaite. Les transactions continuent d'être rejetées tant que la condition logique est satisfaite. Lorsque des transactions sont rejetées, une erreur SOAP est renvoyée au service client (consommateur). Lorsque plusieurs actions sont spécifiées, au sein d'un même élément Action, RejectMessage doit être la première action. QueueMessage et RejectMessage sont mutuellement exclusif.
- **Notify** - Cet élément facultatif indique qu'une notification se produit si la condition logique est satisfaite. Pour DataPower, un message est écrit dans le journal système de DataPower.
- **RouteMessage** - Cet élément facultatif indique que des messages sont acheminés vers une destination de noeud final spécifiée si la condition logique est satisfaite. Les messages continuent à être acheminés vers le noeud final spécifié tant que la condition logique est satisfaite.
  - **EndPoint** – Ce paramètre est obligatoire si une action de RouteMessage est spécifiée. La valeur du noeud final prise en charge peut être une adresse IP, un nom d'hôte ou un hôte virtuel, comme un groupe d'équilibreurs de charge.
- **ValidateMessage** - Cet élément facultatif indique que des messages est validé par rapport à la grammaire spécifiée. Les messages sont refusés lorsque la validation échoue. Vous devez indiquer XSD ou WSDL comme sous-paramètre si ValidateMessage est spécifié. SCOPE est facultatif et s'il n'est pas spécifié, SOAPBody est alors utilisé pour la validation.
  - **XSD** - Indique que des messages sont validés par rapport au schéma XML identifié par l'identificateur URI qu'il contient.
  - **WSDL** - Indique que des messages sont validés par rapport à la description de service Web (WSDL) identifié par l'identificateur URI qu'elle contient.
  - **SCOPE** – Indique quelle partie du message est validée. Le tableau suivant répertorie les valeurs possibles et leur signification :

Tableau 21. Eléments ValidateMessage

Valeur	Description
SOAPBody	Contenu de l'élément Body de SOAP, sans traitement particulier pour les erreurs de SOAP. (Par défaut)
SOAPBodyOrDetails	Contenu de l'élément Details pour les erreurs SOAP, sinon le contenu de Body de SOAP.
SOAPEnvelope	Message SOAP complet, y compris l'enveloppe.
SOAPIgnoreFaults	Aucune validation si le message est une erreur SOAP, sinon contenu de Body de SOAP.

- **ExecuteXSL** - Indique qu'une transformation XSL doit être exécutée avec la feuille de style et les paramètres spécifiés. Les transactions sont rejetées si l'exécution échoue. Les informations de feuille de style doivent être spécifiée,

tandis que les paramètres sont facultatifs et doivent être indiqués si nécessaire par la feuille de style particulière spécifiée.

– **Stylesheet** - Indique que l'opération de transformation utilise la feuille de style spécifiée par l'identificateur URI contenu. La feuille de style DOIT être un fichier XSLT.
– **Parameter** - Cet élément répétitif facultatif spécifie qu'un paramètre de feuille de style doit être utilisé pour l'opération ExecuteXSL.
  - **Name** – Cet attribut est obligatoire pour chaque paramètre Parameter correspondant et donne le nom du paramètre.
  - **Value** – Cet attribut est obligatoire pour chaque paramètre Name correspondant et donne la valeur du paramètre.

Création de règles de médiation

Vous pouvez créer des règles de médiation à l'aide de l'interface utilisateur de Business Space. Lorsque vous créez des règles de médiation, indiquez les conditions et actions qui s'y rattachent.

Avant de commencer

Pour plus d'informations sur l'accès à Business Space, voir «Connexion à WSRR - Business Space», à la page 82.

Vous devez créer l'espace de gouvernance SOA (SOA Governance) avant de pouvoir créer des règles. Si l'espace de gouvernance SOA n'existe pas, reportez-vous à «Configuration de Business Space pour la première utilisation», à la page 83 et suivez les étapes pour créer l'espace.

Vous devez également configurer Business Space pour créer des règles de médiation WS-MediationPolicy à partir du widget Actions. Voir Widget Actions du registre de services

Pourquoi et quand exécuter cette tâche

Création de règles à l'aide de l'espace de gouvernance SOA.

Procédure

1. Ouvrez l'espace de gouvernance SOA :
   a. Cliquez sur **Accéder aux espaces**. La boîte de dialogue Accéder aux espaces s'affiche.
   b. Cliquez sur l'espace pour les utilisateurs de gouvernance SOA. Le nom spécifique dépend des éléments spécifiés lors de la création de l'espace.
2. Dans l'onglet Présentation, cliquez sur **Créer une règle de médiation**.
3. Entrez un nom significatif, ainsi qu'une description facultative.
4. Ajoutez des conditions et des actions, si nécessaire. Pour plus d'informations sur les conditions et actions, voir «Règles», à la page 92 et IBM WebSphere Service Registry and Repository Version 8.0 - Centre de documentation - Création d'une règle de médiation.
5. Cliquez sur **Terminer**.

Résultats

La règle est créée et stockée dans WSRR. Pour visualiser le document de règles de la règle que vous avez créée, sélectionnez celui-ci dans le widget Service Registry

Navigator. Vous pouvez également rechercher le nom que vous avez indiqué, en incluant `.xml` à la fin de celui-ci. Le document de règles s'affiche dans le widget de détails du registre de services situé sur la droite.

Concepts associés:

«Règles», à la page 92
Détails de l'implémentation pour utiliser WSRR comme point de création de règle (PAP, Policy Authoring Point) et WebSphere DataPower comme point d'application de règles (PEP, Policy Enforcement Point) lorsque vous créez des règles de médiation.

Information associée:

IBM WebSphere Service Registry and Repository Version 8.0 - Centre de documentation - Création d'une règle de médiation

Création de règles de surveillance

Vous pouvez créer des règles de surveillance à l'aide de l'interface Web de WSSR. Lorsque vous créez des règles de surveillance, indiquez les conditions et actions qui s'y rattachent.

Avant de commencer

Pour plus d'informations sur l'accès à l'interface Web de WSRR, voir «Connexion à WSRR - Interface utilisateur Web WSRR», à la page 84.

Procédure

1. Ouvrez l'interface utilisateur Web WSRR.
2. Cliquez sur **Vue** > **Documents de service** > **Documents de règles** et cliquez sur **Nouveau** dans la vue collecte.
3. Dans la liste des structures de règles disponibles, sélectionnez **Surveillance**. Cliquez sur **Suivant**. Un document de règles contenant une expression de règles racine est créé.
4. Entrez un nom significatif, ainsi qu'une description facultative.
5. Cliquez sur l'onglet Règle, cliquez sur **Editer le document de règles**, puis ajoutez les conditions et actions tel que demandé. Pour plus d'informations sur les conditions et actions, suivez les liens connexes.
6. Cliquez sur **Publier**.

Résultats

La règle est créée et stockée dans WSRR. Vous pouvez visualiser le document de règles dans Business Space, sélectionner le document de règles dans le widget Navigateur de Service Registry. Vous pouvez également rechercher le nom que vous avez indiqué, en incluant `.xml` à la fin de celui-ci. Le document de règles s'affiche dans le widget de détails du registre de services situé sur la droite.

Concepts associés:

«Règles», à la page 92
Détails de l'implémentation pour utiliser WSRR comme point de création de règle (PAP, Policy Authoring Point) et WebSphere DataPower comme point d'application de règles (PEP, Policy Enforcement Point) lorsque vous créez des règles de médiation.

Information associée:

Tâches de création de règles

Utilisation de l'outil de création de règles

Gérer des règles

Les règles peuvent être modifiées ou supprimées à l'aide de l'interface utilisateur de Business Space.

Avant de commencer

Configurez l'espace de gouvernance SOA. Pour plus d'informations, voir «Configuration de Business Space pour la première utilisation», à la page 83.

Procédure

1. Pour ouvrir le document de règles correspondant à la règle, sélectionnez le document de règles dans le widget du navigateur du registre de services en bas à gauche de l'écran. Vous pouvez également rechercher le nom que vous avez indiqué, en incluant `.xml` à la fin de celui-ci. Le document de règles s'affiche dans le widget de détails du registre de services situé sur la droite.
2. Pour changer les détails de la règle, procédez comme suit :
   a. Cliquez sur l'icône Editer dans ce widget pour éditer le document de règles. Une fenêtre s'affiche avec des options permettant de modifier les détails de la règle.
   b. Si la règle possède des conditions ou actions, celles-ci sont affichées. Créez et modifiez les conditions et les actions si nécessaire.
   c. Cliquez sur **Terminer** pour enregistrer et fermer l'éditeur de règles. Le widget des détails de Service Registry est actualisé pour afficher les modifications qui sont effectuées.
3. Pour supprimer la règle, procédez comme suit :
   a. La transition de la règle vers un état de gouvernance qui autorise l'édition ou la suppression du document de règles. Pour plus d'informations sur la transition d'une règle via le cycle de vie des règles SOA, voir «Gérer le cycle de vie de la règle».
   b. Cliquez sur **Action** > **Delete**. L'option Delete (Supprimer) figure dans le menu.
   c. Sélectionnez **Delete** (Supprimer) pour supprimer la règle.
   d. Cliquez sur **Oui** pour confirmer la suppression.

Information associée:

Centre de documentation d'IBM WebSphere Service Registry and Repository version 8.0

Centre de documentation d'IBM WebSphere Service Registry and Repository version 8.0 - Règles dans le profil d'activation de gouvernance

Gérer le cycle de vie de la règle

Les règles peuvent être en transition entre des états de gouvernance à l'aide de l'interface utilisateur de Business Space. Les règles doivent être à l'état Approuvé pour pouvoir être implémentées par DataPower.

Pourquoi et quand exécuter cette tâche

Pour plus d'informations sur la gouvernance, voir «Cycle de vie de règles SOA», à la page 5.

Procédure

Pour effectuer la transition d'une règle vers un état différent du cycle de vie, procédez comme suit. Répétez ces étapes autant de fois que nécessaire pour atteindre l'état de cycle de vie souhaité :

1. Dans Business Space, ouvrez le document de règles correspondant à la règle en sélectionnant le document de règles dans le widget du navigateur du registre de services. Vous pouvez également rechercher le nom que vous avez indiqué, en incluant `.xml` à la fin de celui-ci. Le document de règles s'affiche dans le widget Détails du registre de services. La propriété **Etat de gouvernance** affiche l'état de gouvernance en cours pour le profil.
2. Cliquez sur **Action**. La liste des transitions de cycle de vie possibles est affichée avec d'autres opérations possibles.
3. Sélectionnez la transition de cycle de vie requise pour déplacer la règle vers l'état requis. La propriété **Etat de gouvernance** de la règle est mise à jour pour afficher le nouvel état de cycle de vie.

Concepts associés:

«Cycle de vie de règles SOA», à la page 5
Les règles sont régies par le cycle de vie de règles SOA. Ce cycle de vie prend la règle depuis son identification initiale jusqu'à ce qu'elle soit plus requise et considérée comme obsolète, en passant par son déploiement en production.

Information associée:

Centre de documentation d'IBM WebSphere Service Registry and Repository version 8.0 - Cycle de vie des règles SOA

Règles associées à un service

Il est possible de joindre des règles à un service à l'aide de WSRR.

Pour plus d'informations, voir IBM WebSphere Service Registry and Repository Version 8.0 - Centre de documentation - Tâches d'association de règles.

Chapitre 7. Identification et résolution des problèmes

Obtenez de l'aide pour diagnostiquer des problèmes que vous pouvez avoir avant, pendant et après le déploiement du modèle.

Utilisez les liens pour trouver les rubriques pertinentes pour un problème avec les modèles.

Identification et résolution de problèmes liés au déploiement

Vous pouvez identifier et résoudre des problèmes courants rencontrés lors du déploiement de modèles dans IBM SOA Policy Gateway Pattern.

Echec de la connexion à un dispositif DataPower externe au cours du déploiement

Essayez les solutions suivantes :

- Vérifiez la validité de l'utilisateur et du mot de passe auprès de l'administrateur de DataPower :
  - Dans l'interface Web DataPower, validez l'existence de l'utilisateur en accédant à **Panneau de commande** > **Comptes d'utilisateurs**.
  - Vérifiez que le compte existe.
  - Vérifiez que l'utilisateur dispose des droits d'utiliser l'interface de gestion XML, comme l'administrateur système.
  - L'administrateur de DataPower peut avoir besoin de vérifier que le compte utilisateur est activé dans les paramètres de l'agent d'utilisateur, par exemple, les paramètres d'authentification de base.
- Vérifiez que le nom d'hôte DataPower est correct.
- Vérifiez que l'interface de gestion XML de DataPower est activé.

Identification et résolution d'une erreur pour le domaine déjà existant

Essayez la solution suivante :

- Sur le panneau de commande de DataPower ouvrez les domaines d'application (Application Domains). Vérifiez que le domaine existe déjà.

Identification et résolution de l'erreur de chevauchement de ports (port overlap) pour l'exemple d'application

Si l'un des exemples de services n'est pas disponible, vérifiez si les ports dans votre domaine sont en conflit avec d'autres domaines.

Essayez les solutions suivantes :

- Ouvrez une session dans DataPower et passez à l'exemple de domaine. Puis, ouvrez le panneau de commande, puis cliquez sur l'icône du pare-feu XML (XML Firewall). Vérifiez que les pare-feu XML sont tous à l'état Up (Actif).
- Recherchez un gestionnaire HTTP Front Side Handler. Vérifiez que le gestionnaire HTTP Front Side unique est à l'état Actif.

Identification et résolution de l'échec de promotion

De nombreux problèmes peuvent survenir lors d'une promotion, notamment l'échec de la connexion à Governance Master au cours du déploiement.

Essayez les solutions suivantes :

- Vérifiez les paramètres :
  - Vérifiez l'utilisateur du maître de gouvernance WSRRCELL.
  - Vérifiez le mot de passe de l'utilisateur de la cellule du maître de gouvernance WSRR.
  - Vérifiez le nom d'hôte de la cellule du maître de gouvernance WSRR.
  - Vérifiez le nom de cellule (CELL) de la cellule du maître de gouvernance WSRR.
- Vérifiez l'échange de certificat de signataire :
  - Accédez à CellDefaultTrustStore de la cellule Governance Master et vérifiez qu'il existe une entrée de certificat pour le Dmgr ou que le serveur autonome de l'environnement d'exécution existe.
  - Accédez à l'environnement d'exécution, puis vérifiez CellDefaultTrustStore (dans le cas d'un environnement de déploiement réseau (ND)) ou NodeDefaultTrustStore (pour des serveurs autonomes WSRR) pour vous assurer qu'il existe un certificat pour le Dmgr de Governance Master.
  - Exportez les clés LTPA à partir des deux cellules en utilisant le même mot de passe, puis vérifiez qu'ils sont identiques (par exemple, en comparant le nombre d'octets).
- Vérifiez que le fichier des propriétés de promotion contient des sections de serveur avec l'hôte et le port appropriés, ainsi que les informations d'utilisateur et de mot de passe. Vous pouvez trouver ces informations dans la console ServiceRegistry pour Governance Master :
  - Accédez à GovernanceMasterDMgrHost ou ServiceRegistry, puis à la perspective des configurations. Dans la section Actions, recherchez **Promotion**, puis ouvrez le fichier de propriétés de promotion. Pour chaque environnement, il doit exister des éléments XML pour chaque serveur dans le noeud ou cluster WSRR de transfert. Si un cluster ou noeud de production existe, il doit exister des entrées de port de serveur pour chacun d'eux, en outre, il doit y avoir des informations d'utilisateur et de mot de passe.
- Vérifiez que la version de service et le noeud final SOAP disposent tous les deux d'une classification de transfert ou de production.
  - Dans la console Service Registry, sélectionnez la perspective de gouvernance SOA. Ouvrez la version de service, puis sélectionnez l'onglet Classifications. Staging (transfert) et Production doivent être activés.

Identification et résolution des échecs d'interfaces CLI personnalisées

Essayez les solutions suivantes :

- Vérifiez le journal par défaut des messages d'erreur du domaine DataPower.
- Activez le débogage de l'interface CLI et vérifiez ces journaux avant toute exécution supplémentaire de l'interface de ligne de commande.

Identification et résolution des problèmes dans l'instance déployée

Vous pouvez identifier et résoudre les problèmes courants dans l'instance déployée.

Echec des connexions au serveur LDAP ou au port DataPower StoreWSP

Vous pourriez avoir un problème avec les paramètres du domaine (Domain) si les journaux de DataPower indiquent une erreur de connexion avec LDAP ou la passerelle StoreWSP et si vous utilisez le nom d'alias de l'hôte ; par exemple `xyz` au lieu du nom d'hôte qualifié complet `xyz.company.com` pour l'un des paramètres suivants dans le package de script :

- Nom d'hôte DataPower
- Nom d'hôte LDAP

Essayez la solution suivante :

1. Dans la console d'administration de DataPower, passez au domaine par défaut.
2. Recherchez `Configure DNS Settings`.
3. Cliquez sur l'onglet Search Domains.
4. Vérifiez que votre domaine, par exemple `company.com`, figure bien dans la liste. Si ce n'est pas le cas, cliquez sur `Add` et ajoutez-le à la liste.

Problèmes de surveillance

Si la surveillance est indisponible sur les noeuds, vous devez vérifier que les services partagés obligatoires s'exécutent. Accédez à **Instances** > **Services partagés**.

Vérifiez que System Monitoring et System Monitoring for WebSphere DataPower s'exécutent dans le même groupe de clouds que vos instances déployées. Pour la surveillance de WSRR, vérifiez également que System Monitoring for WebSphere Application Server s'exécute dans votre groupe de clouds.

Collecte d'informations de diagnostic

Vous pouvez utiliser les journaux pour vous aider à rechercher et résoudre les problèmes. Les journaux sont stockés sur l'appliance et peuvent être visualisés à partir de l'interface utilisateur, ou ils peuvent être téléchargés sur votre système de fichiers local.

Procédure

Pour collecter des informations de diagnostic, procédez comme suit :

1. Affichez les instances virtuelles :
   a. Cliquez sur **Instances** > **Système virtuel**.
   b. Sélectionnez l'instance dans la liste des instances dans la fenêtre Instances de système virtuel.
2. Pour la machine virtuelle WSRR :
   a. Dans la section **Machines virtuelles**, développez la machine virtuelle WSRR et examinez les erreurs dans la section **Packages de script**. Si l'un des packages de script comporte des erreurs, cliquez sur les liens du journal pour **remote_std_out.log** et **remote_std_err.log** en regard des noms de package de script.
   b. Connectez-vous à l'instance WSRR et vérifiez les erreurs de serveur.
   c. Reportez-vous aux guides d'identification et de résolution des problèmes de WSRR : http://pic.dhe.ibm.com/infocenter/sr/v8r0/topic/com.ibm.sr.doc/cwsr_troubleshootingandsupport.html

3. Pour DataPower :
   a. Récupérez le fichier **default.log** pour le domaine créé par le modèle.
   b. Récupérez le fichier **default.log** pour le modèle par défaut.
4. Pour les problèmes de surveillance, collectez ces journaux à partir des noeuds du SE de base et WSRR (à l'exclusion des noeuds personnalisés WSRR) :
   - `/0config/0config.log`
   - `/opt/IBM/maestro/ITCAMSOADP/lx8266/d4/KD4/logs/*` (x86)
   - `/opt/IBM/maestro/ITCAMSOADP/aix523/d4/KD4/logs/*` (Power)

Chapitre 8. Maintenance et support

Vous pouvez exécuter des fonctions de maintenance comme l'application de correctifs d'urgence.

Ajout d'un correctif d'urgence au catalogue

Les correctifs temporaires et les groupes de correctifs sont appliqués aux instances de systèmes virtuels comme des correctifs d'urgence. Vous pouvez ajouter à votre catalogue les correctifs d'urgence qui seront appliquées à vos images virtuelles.

Avant de commencer

Vous devez disposer de l'autorisation *Créer un nouveau contenu de catalogue* ou bénéficier du rôle *Administrateur* du dispositif IBM Workload Deployer avec des droits d'accès complets pour effectuer ces étapes.

Pourquoi et quand exécuter cette tâche

Les correctifs sont fournis par IBM ou par un fournisseur d'images et doivent être téléchargés. Vous pouvez télécharger les nouveaux correctifs à partir du site IBM Fix Central. Les correctifs sont ensuite téléchargés dans le catalogue et peuvent être appliqués à toutes les instances de système virtuel applicables.

Procédure

Procédez comme suit pour ajouter un correctif d'urgence à votre catalogue.

1. Recherchez et téléchargez le ou les correctifs d'urgence à partir de Fix Central.
2. Facultatif : Vous pouvez ajouter plusieurs correctifs temporaires à la fois. Pour ajouter plusieurs correctifs à la fois, téléchargez les fichiers compressés à partir de Fix Central et regroupez-les dans un fichier compressé unique.
3. Dans le menu, sélectionnez **Catalogue** > **Correctifs d'urgence**.
4. Cliquez sur l'icône d'ajout du panneau de gauche.
5. Entrez un nom pour le correctif à ajouter. Si vous le souhaitez, vous pouvez également ajouter une description du correctif que vous ajoutez. Le correctif s'affiche dans le panneau de gauche de la fenêtre Correctifs d'urgence et les informations sur le correctif s'affichent dans le panneau de droite.
6. Accédez à l'emplacement dans lequel vous avez stocké le correctif et cliquez sur **Télécharger**. Pour des raisons de sécurité, il est possible de télécharger uniquement des fichiers zip, tgz, et pak. Red Hat RPM est également pris en charge.
7. Remplissez les informations sur le correctif. Vous pouvez accorder l'accès aux utilisateurs et fournir une évaluation de gravité. Utilisez la zone **Applicable à** pour indiquer la ou les images virtuelles auxquelles s'applique ce correctif.

Résultats

Le correctif d'urgence se trouve dans le catalogue et est disponible pour être appliqué aux images du système virtuel.

Application d'un correctif d'urgence

Les correctifs temporaires et les groupes de correctifs sont appliqués aux instances de systèmes virtuels comme des correctifs d'urgence. Vous pouvez appliquer des correctifs d'urgence à vos images de système virtuel.

Avant de commencer

Vous devez disposer de l'accès complet à l'instance de système virtuel ou du rôle d'administration de l'appliance avec des droits d'accès complets pour exécuter ces étapes. L'instance de système virtuel doit être démarrée pour que le service soit planifié ou appliqué. Le correctif d'urgence doit être ajouté au catalogue avant de pouvoir être appliqué à un système virtuel.

Pourquoi et quand exécuter cette tâche

Lorsque vous ajoutez un correctif d'urgence, vous définissez les images virtuelles auxquelles il s'applique. La liste des correctifs disponibles lorsque vous planifiez une demande de service est construite à partir de tous les correctifs applicables à l'image virtuelle utilisée pour créer votre instance de système virtuel. Si un correctif a déjà été appliqué à votre système virtuel, il apparaît dans le liste **Historique** et n'est pas inclus dans la liste des correctifs disponibles.

Remarque : Vous devez arrêter tous les processus WSRR et WAS avant d'installer un correctif d'urgence. Connectez-vous à l'aide de SSH à tous les noeuds WSRR et arrêtez les processus à l'aide des commandes **stopServer.sh** et **stopNode.sh** (noeuds personnalisés uniquement).

Procédure

Exécutez les étapes suivantes pour appliquer un correctif temporaire.

1. Sélectionnez une instance de système virtuel à laquelle vous souhaitez appliquer le correctif à partir de la fenêtre Instances de système virtuel.
2. Cliquez sur l'icône **Appliquer le service**.
3. Facultatif : Planifiez une demande de service. Par défaut, le correctif est appliqué immédiatement. Pour planifier son application ultérieure, cliquez sur **Planifier le service** et fournissez les informations nécessaires.
4. Cliquez sur **Sélectionner un niveau de service ou des correctifs**.
5. Cliquez sur **Appliquer les correctifs d'urgence** pour visualiser et sélectionner le correctif à appliquer. Le correctif d'urgence est appliqué à toutes les machines virtuelles de l'instance de système virtuel. Le statut de l'instance de système virtuel indique que le service a été appliqué sur le système virtuel.
6. Vérifiez l'absence d'erreurs. Vérifiez les fichiers suivants pour vous assurer qu'aucune erreur ne s'est produite pendant le processus de l'application de correctifs d'urgence :
   - Remote_std_out.log
   - Remote_std_err.log

   Vous pouvez accéder aux fichiers journaux à partir de la fenêtre d'instances de systèmes virtuels.

Chapitre 9. Appendices

Notices

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

COPYRIGHT LICENSE:

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

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

Programming interface information

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

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

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

Trademarks

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

Sending your comments to IBM

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

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

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

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

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

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

- By mail, to this address:

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

WINCHESTER,
Hampshire
SO21 2JN
United Kingdom

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

Whichever method you use, ensure that you include:

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