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. Des pratiques basées sur l'architecture orientée services (SOA, Service Orientated Architecture) permettent aux entreprises d'identifier et de se concentrer sur des services clés de leur activité. Lorsque vous ajoutez des règles, nous ajoutons des points de contrôle et d'agilité pour l'entreprise et les technologies de l'information. Le résultat est que l'architecture SOA plus consommables, en améliorant la valeur temps pour des utilisateurs métier avec des coûts réduits pour leurs projets, et en accélérant l'adoption de solutions SOA.

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 de création de règles (PAP, Policy Authoring 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 ce modèle, le PAP est obtenu à l'aide de WSRR, et le PEP à l'aide de WebSphere DataPower.

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

- **Policy Authoring Point** (Point de création 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 règles pendant l'exécution. Inclut un référentiel pour stocker des règles. Dans ce modèle, ceci est obtenu à l'aide de WSRR.
- **Policy Enforcement Point** (point d'application de règles) - Un point d'application de règles est un point fonctionnel qui s'exécute sur le middleware qui :
  - 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 réellement appliquées et appliquées selon la phase du cycle de vie :
    - Lors de la phase de conception, le registre de services et le référentiel proprement dit constituent 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, ceci est obtenu à l'aide de WebSphere DataPower.

- **Policy Decision Point** (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. Il renvoie une décision d'autorisation, d'éligibilité ou de validation pour la fourniture de résultats calculés.
- **Policy Information Point** (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** (point de contrôle de règles) - 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. Ceci inclut :
  - 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).

  Remarque : Le contrôle n'est pas inclus dans ce modèle.

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 conduisant à des actions avec des règles SOA est présenté dans figure 1, à la page 3 et décrit ci-dessous.

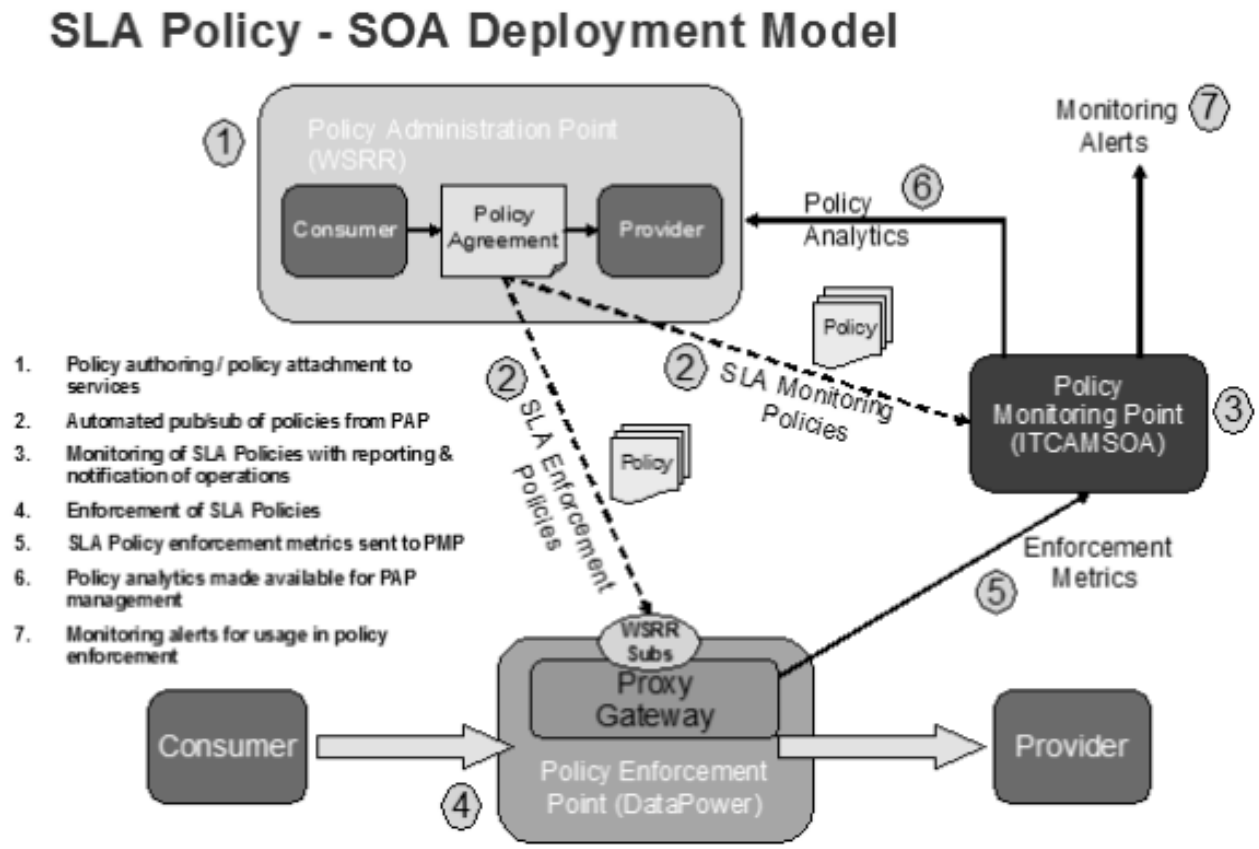


Figure 1. Règle d'accord sur les niveaux de licence (SLA) - le modèle de déploiement SOA

1. Les règles sont créées, puis associées à des services nécessitant cette règle. En général, les opérations sont menées dans l'ordre suivant :
   a. Tous les services sont chargés ou créés dans le référentiel de service. Il s'agit d'un composant du point de création de règles (PAP).
   b. Toutes les règles requises sont créées au niveau du point de création de règles (PAP) en utilisant le cycle de vie des règles :
      1) 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 de création de règles (PAP) pour le point d'application de règles (PEP) et le point de contrôle des règles (PMP) :

   Remarque : Le contrôle via ITCAM for SOA n'est pas inclus dans ce modèle.
   a. Lors de la configuration, ITCAM for SOA souscrit à la règle de surveillance issue de WSRR. Cet événement ne se produit qu'une seule fois.
   b. Lors de la configuration, des passerelles de proxy sont créées dans chaque dispositif WebSphere Data Power disposant de transactions de service avec une application de règles. Cet événement ne se produit qu'une seule fois, et est ajouté ou modifié, le cas échéant.
   c. Lors de la configuration, chaque passerelle de proxy du dispositif souscrit à des règles de WSRR pour les services dont elle a la responsabilité. Cet événement ne se produit qu'une seule fois, et est ajouté ou modifié, le cas échéant.

d. Lors de la configuration, WebSphere DataPower est configuré pour permettre le partage des règles par d'autres dispositifs au sein d'un cluster. Cet événement ne se produit qu'une seule fois, et est ajouté ou modifié, le cas échéant.
e. ITCAM for SOA télécharge les règles de contrôle à mesure de leur publication.
f. ITCAM for SOA convertit les règles en une présentation interne appelée règles de situation.
g. WebSphere DataPower télécharge les WSDL pour des services dont il a la responsabilité des transactions.
h. WebSphere DataPower télécharge les règles pour des services dont il a la responsabilité en cas de notification par WSRR.
i. WebSphereDataPower convertit les règles en une représentation WebSphere DataPower interne sous la forme d'objets SLM.

3. Contrôle des règles SOA avec génération de rapports et notification des opérations :
   a. Les règles de contrôle sont actives dans ITCAM pour la règle de situation SOA.
   b. ITCAM for SOA reçoit des informations de contrôle et place ces informations dans des espaces de travail.

   Remarque : Le contrôle n'est pas fourni dans ce modèle.
4. Application des règles SOA :
   a. Les règles d'application sont actives dans les différents dispositifs de WebSphere DataPower.
   b. WebSphereDataPower reçoit des transactions de service et applique des règles pour ce service consommateur ou service fournisseur.
5. Le point d'application de règles (PEP) envoie des statistiques de mise en application des règles SOA au point de contrôle des règles (PMP).

   Remarque : Le contrôle n'est pas inclus dans ce modèle.
6. Le point de contrôle de règles (PMP) envoie des événements de contrôle au point de création de règles (PAP) :
   a. Des événements sont configurés au niveau du point de création de règles (PAP) pour être contrôlés depuis le point de contrôle de règles (PMP). Ceci ne se produit qu'une seule fois, et est ajouté ou modifié, le cas échéant.
   b. 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).

   Remarque : Le contrôle n'est pas inclus dans ce modèle.
7. Contrôle des alertes :
   a. 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 de médiation sont gouvernées à l'aide du cycle de vie de règles SOA. Ceci 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 créés des normes pour répondre à l'exigences consistant à définir la règle qui doit s'appliquer 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/WSMediationPolicy1.6-20120124.pdf.

Le modèle de données WS-Policy inclut les éléments suivants :

- **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. Ceci est utilisé 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 serait qu'un appel d'un service Web doive signer ou chiffrer le corps du message, mais 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.

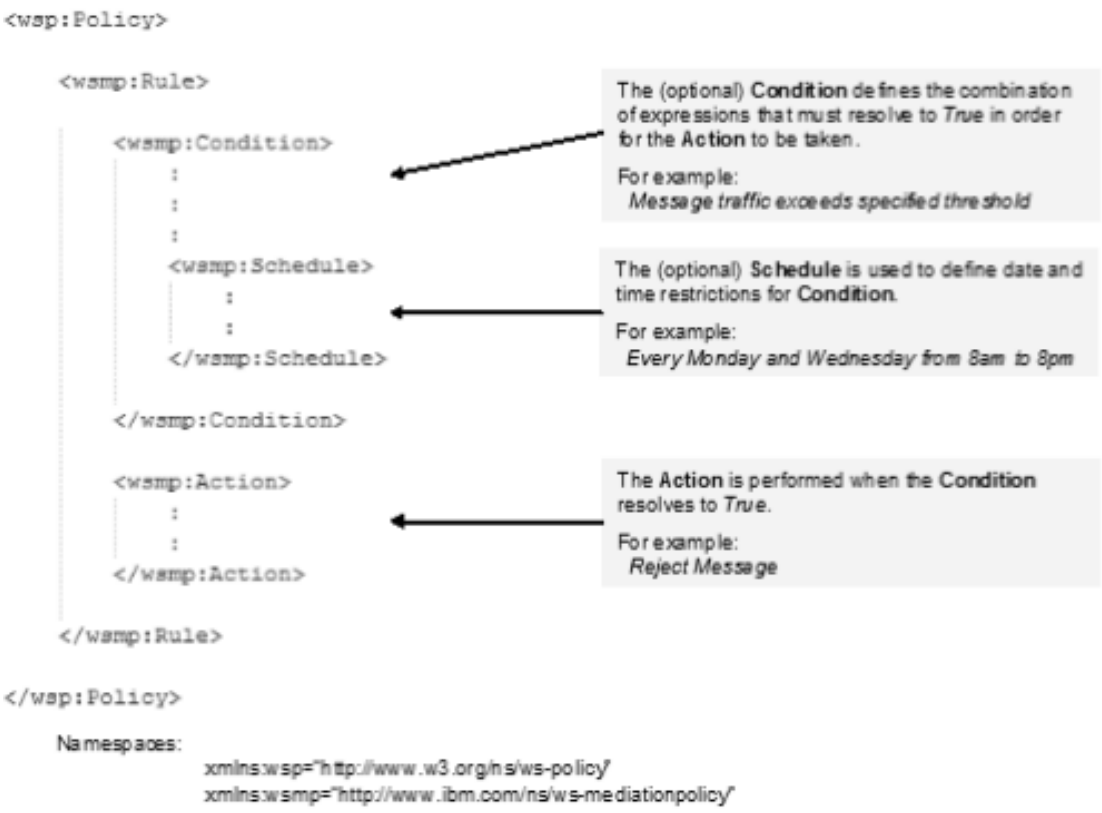


Figure 3. Présentation d'une structure de règle

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 figure 4, l'objet de règle spécifique du domaine auquel la règle s'applique (le fournisseur) est contenu dans la section `<wsp:AppliesTo>` 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 canevas de système virtuel fournissant un point d'application de règles et un point d'administration des règles. 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 est fourni par le dispositif WebSphere DataPower dans lequel un domaine est créé au cours du déploiement du canevas de système virtuel.

Il existe des exemples de règles dans de nombreux, si ce n'est pas dans tous les environnements avec architecture orientée services (SOA, Services Orientated 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 cela, vous pouvez utiliser des définitions de niveau de service (SLD) et des accords sur les niveaux de service (SLA). Ce modèle vous permet de définir des règles pour des SLD et des SLA par un moyen administré, défini, gouverné et utilisé, et ce manière efficace. Les types de règles utilisés dans ce modèle inclut les éléments suivants :

- **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** : dans l'exemple, nous présentons les moyens de mettre en application des règles de sécurité sur le contrôle d'accès à XACML. Ces moyens sont gouvernés au sein du point d'administration des règles à ce stade.

Le modèle IBM SOA Policy Gateway Pattern contient les canevas de système virtuelsuivants :

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

Les quatre canevas de système virtuel s'associent pour fournir un environnement de gouvernance de services multi-étapes. Le modèle IBM SOA Policy Gateway Pattern offre également la possibilité de mettre à dispositionplusieurs domaines DataPower configurés pour l'environnement de gouvernance au cours du déploiement du modèle. Combinées, les topologies de déploiement ont fourni :

- Un déploiement autonome
- Un déploiement pilote
- Un déploiement de production complet

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

Il est possible de configurer manuellement le canevas de système virtuel déployé pour inclure une surveillance avec ITCAM for SOA Version 7. Ceci offre une surveillance de base des événements et développe une prise en charge des règles pour inclure des règles de surveillance. Les règles de surveillance permettent à des situations d'événement d'être définies au sein du point de création de règles (PAP, Policy Authoring Point) et être jointes à une définition de service ; le dispositif de surveillance peut ainsi agir lorsqu'une situation d'événement se produit.

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. Des pratiques basées sur l'architecture orientée services (SOA, Service Orientated Architecture) permettent aux entreprises d'identifier et de se concentrer sur des services clés de leur activité. Lorsque vous ajoutez des règles, nous ajoutons des points de contrôle et d'agilité pour l'entreprise et les technologies de l'information. Le résultat est que l'architecture SOA plus consommables, en améliorant la valeur temps pour des utilisateurs métier avec des coûts réduits pour leurs projets, et en accélérant l'adoption de solutions SOA.

«SOA Policy Gateway Basic Runtime», à la page 21
SOA Policy Gateway Basic Runtime propose un moyen simple de fournir un environnement d'exécution qui peut être utilisé en mode autonome ou intégré à l'aide d'un modèle SOA Policy Gateway Governance Master déployé. Le modèle SOA Policy Gateway Basic Runtime prend en charge le déploiement d'un domaine DataPower qui est configuré pour communiquer avec le serveur d'exécution WSRR mis à disposition dans le modèle.

«Exemple SOA Policy Gateway Basic Runtime», à la page 18
Exemple SOA Policy Gateway Basic Runtime met à disposition un environnement d'exécution SOA Policy Gateway Basic Runtime 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», à la page 23
Le modèle SOA Policy Gateway Advanced Runtime inclut d'autres options haute disponibilité et doit être utilisé avec le modèle SOA Policy Gateway Governance Master.

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. Les rubriques de cette section vont vous aider de mieux comprendre ce qui est couvert par ce scénario, les raisons qui pousseront une entreprise à vouloir suivre ce scénario, les rôles utilisateur impliqués et une présentation de la fonction fournie avec le produit.

Avant de commencer

Vous pouvez utiliser le IBM SOA Policy Gateway Pattern IBM sur le dispositif IBM PureApplication System ou IBM Workload Deployer.

Procédure

Pour utiliser le IBM SOA Policy Gateway Pattern, procédez comme suit :

1. Téléchargez et installez IBM SOA Policy Gateway Pattern. Pour plus d'informations sur le téléchargement des packages à partir de Passport Advantage, voir «Téléchargement et installation des modèles», à la page 12.
2. Facultatif : Configurez un accès utilisateur. Pour plus d'informations, voir «Configuration de l'accès utilisateur», à la page 14.
3. Configurez et déployez ce modèle.
   a. Acceptez les licences des images de systèmes virtuels importés pour WSRR.
   b. Acceptez tous les contrat de licence sur DB2 Enterprise.
   c. Déployez le modèle :
      1) Décidez de la topologie de déploiement à employer. Pour plus d'informations, voir Centre de documentation d'IBM WebSphere Service Registry and Repository version 8.0 - Topologies de déploiement.
      2) Si vous utilisez une topologie de déploiement autonome, déployez un modèle d'exécution de base unique sans promotion configurée.
      3) Pour d'autres topologies, commencez par déployer le modèle SOA Policy Gateway Governance Master. Ceci fournit un environnement de gouvernance pour des services et règles.
      4) Une fois le modèle de maître de gouvernance (Governance Master) déployé, choisissez le type d'environnement d'exécution dont vous avez besoin. S'il s'agit d'un environnement de test ou de transfert, un environnement d'exécution de base (Basic) est suffisant. Dans le cas d'un environnement de production, optez pour l'environnement d'exécution avancé (Advanced). Les environnements d'exécution peuvent être enregistrés avec la configuration de promotion du profil d'activation de la gouvernance pour Governance Master. Les options de promotion incluent production, staging (transfert) ou no promotion pour une configuration de promotion manuelle.

      Pour plus d'informations, voir «Déploiement des modèles», à la page 68.
   d. Vérifiez le déploiement. Voir «Vérification du déploiement», à la page 74.

e. Sécurisez l'environnement WSRR. Pour plus d'informations sur la planification et la configuration de la sécurité WSRR, voir Centre de documentation d'IBM WebSphere Service Registry and Repository version 8.0.

f. Configurez le domaine DataPower mis à disposition. Pour plus d'informations, voir «Gestion de la sécurité», à la page 60.

4. Utilisez l'instance déployée. Pour plus d'informations, voir Chapitre 6, «Utilisation de l'instance déployée», à la page 99.

Téléchargement et installation des modèles

IBM SOA Policy Gateway Pattern à utiliser avec IBM Workload Deployer version 3.1.0.2 ou IBM PureApplication System est assemblé pour être téléchargé à partir de Passport Advantage.

Avant de commencer

Assurez-vous de disposer de 10 Go d'espace disponible pour le fichier `CI9G9ML.tar.gz` et de 10 à 14 Go supplémentaires pour les fichiers extraits.

Le fichier `CI9G9ML.tar.gz` doit être téléchargé dans un système fonctionnant sous Linux ou Microsoft Windows. Java™ Runtime Environment (JRE) version 6 doit également être installé avant de lancer l'installation du modèle. Vous pouvez télécharger cette version pour Linux à partir de l'adresse suivante : http://www.ibm.com/developerworks/java/jdk/linux/download.html.

Pourquoi et quand exécuter cette tâche

Le modèle IBM SOA Policy Gateway Pattern est assemblé dans le fichier `CI9G9ML.tar.gz`. 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 nom du fichier est `CI9G9ML.tar.gz`.
3. Ouvrez un terminal sous Linux ou une fenêtre d'invite de commande sous Windows pour accéder au répertoire dans lequel le fichier `CI9G9ML.tar.gz` a été téléchargé.
4. Extrayez le contenu du fichier `CI9G9ML.tar.gz` vers votre système de fichier local. Sous Linux, la commande d'extraction est : Sous Linux, la commande d'extraction est :

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

   Sous Windows, utilisez un logiciel d'extraction supplémentaire pour extraire le contenu du fichier `CI9G9ML.tar.gz`.
5. Assurez-vous que les fichiers extraits suivants possèdent les droits d'exécution sur les systèmes Linux :
   - `chmod a+x installer/installer`
   - `chmod a+x installer/deployer.cli/bin/deployer`

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

6. Changez pour le répertoire `installer` :

```
cd installer
```

7. Pour installer IBM SOA Policy Gateway Pattern dans le dispositif Cloud, 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 Cloud et nom_utilisateur et mot_de_passe sont les données d'identification de l'administrateur cloud. Par exemple :

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

8. 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.
9. 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 2.0.0.0 - Governance Master" ...
Import pattern "SOA Policy Gateway 2.0.0.0 - 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 du dispositif IBM Workload Deployer ou dans IBM PureApplication System.

Pour valider l'installation, voir «Vérifiez le modèle installé».

Vérifiez le modèle installé

Vous pouvez vérifier que le modèle est correctement installé et accepter toutes les licences requises pour utiliser le modèle.

Avant de commencer

Vérifiez que toutes les étapes de «Téléchargement et installation des modèles», à la page 12 sont terminées.

Pourquoi et quand exécuter cette tâche

Après l'installation du modèle, vous pouvez en vérifier l'installation. Avant de pouvoir utiliser une image virtuelle, vous devez accepter la licence requise pour celle-ci.

Procédure

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

1. Ouvrez une session sur la console IPAS ou la console IWD de l'hôte dans lequel le modèle a été installé.
2. Vérifiez les images virtuelles en accédant à `Catalog -> Virtual Images` et recherchez : DB2 9.7.5.0 et WebSphere Service Registry and Repository 8.0.0.1. Si une licence n'est pas acceptée, l'icône de l'image doit contenir un case rouge barrée d'une croix.
   a. Pour accepter une licence, cliquez sur l'image pour afficher ses détails. L'état en cours 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 en cours doit apparaître en mode lecture seule (Read-only) et le contrat de licence doit afficher Accepted une fois terminé.
3. Accédez à `Catalog -> Script Packages`, et recherchez :
   - SOA Policy Gateway 2.0.0.0 - DataPower Domain
   - SOA Policy Gateway 2.0.0.0 - Promotion
   - SOA Policy Gateway 2.0.0.0 - Sample
   - SOA Policy Gateway 2.0.0.0 - Security

   Ces packages de script sont tous présents dans une installation qui s'est correctement effectuée.
4. Accédez à `Patterns -> Virtual Systems`, et recherchez :
   - SOA Policy Gateway 2.0.0.0 - Advanced Runtime
   - SOA Policy Gateway 2.0.0.0 - Basic Runtime
   - SOA Policy Gateway 2.0.0.0 - Basic Runtime Sample
   - SOA Policy Gateway 2.0.0.0 - Governance Master

   Ces modèles sont tous présents 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 avec : Chapitre 5, «Utilisation du IBM SOA Policy Gateway Pattern», à la page 57. Sinon, répétez à partir de l'étape 7 de la rubrique «Téléchargement et installation des modèles», à la page 12.

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.

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 l'interface.
     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 le menu, cliquez sur **Catalogue** > **Images virtuelles** pour ouvrir la fenêtre Images virtuelles. Sélectionnez une image virtuelle de IBM SOA Policy Gateway Pattern dans le panneau de gauche, puis ajoutez les utilisateurs ou le groupe dans le panneau de droite.

Que faire ensuite

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

Information associée:

IBM PureApplication System : Gestion des utilisateurs et des groupes

IBM Workload Deployer : Gestion des utilisateurs et des groupes

Chapitre 4. Modèles, composant et packages de script

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

Il décrit la fonction offerte par chaque machine virtuelle d'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.

Composants

Les composants sont les éléments configurés sur une machine virtuelle. Chaque composant possède une série de propriétés (paramètres) utilisées pendant le déploiement et qui participent à la définition de la configuration du système virtuel. Lorsque vous chargez les images du IBM SOA Policy Gateway Pattern sur IBM Workload Deployer, les composants sont inclus.

Modèles

Le modèle IBM SOA Policy Gateway Pattern contient quatre modèles :

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

Pour plus d'informations sur l'utilisation d'IBM Workload Deployer pour accéder à des modèles existants ou créer un modèle personnalisé, voir http://publib.boulder.ibm.com/infocenter/worlodep/v3r0m0/topic/com.ibm.worlodep.doc/welcome.html.

Modèles

Lorsque les images virtuelles ont été chargées dans IBM Workload Deployer ou IBM PureApplication System et que l'accès approprié a été affecté aux utilisateurs, ces derniers peuvent commencer à utiliser les modèles des images.

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

SOA Policy Gateway Basic Runtime contient les composants requis suivants :

- DB2 Enterprise
- Serveur autonome WSRR

Exemple SOA Policy Gateway Basic Runtime

Exemple SOA Policy Gateway Basic Runtime contient les composants requis suivants :

- DB2 Enterprise
- Serveur autonome WSRR

SOA Policy Gateway Advanced Runtime

SOA Policy Gateway Advanced Runtime contient les composants requis suivants :

- Gestionnaire de déploiement WSRR
- DB2 Enterprise HADR Primary
- DB2 Enterprise HADR Standby
- Noeud personnalisé WSRR

SOA Policy Gateway Governance Master

SOA Policy Gateway Governance Master contient les composants requis suivants :

- Gestionnaire de déploiement WSRR
- DB2 Enterprise HADR Primary
- DB2 Enterprise HADR Standby
- Noeud personnalisé WSRR

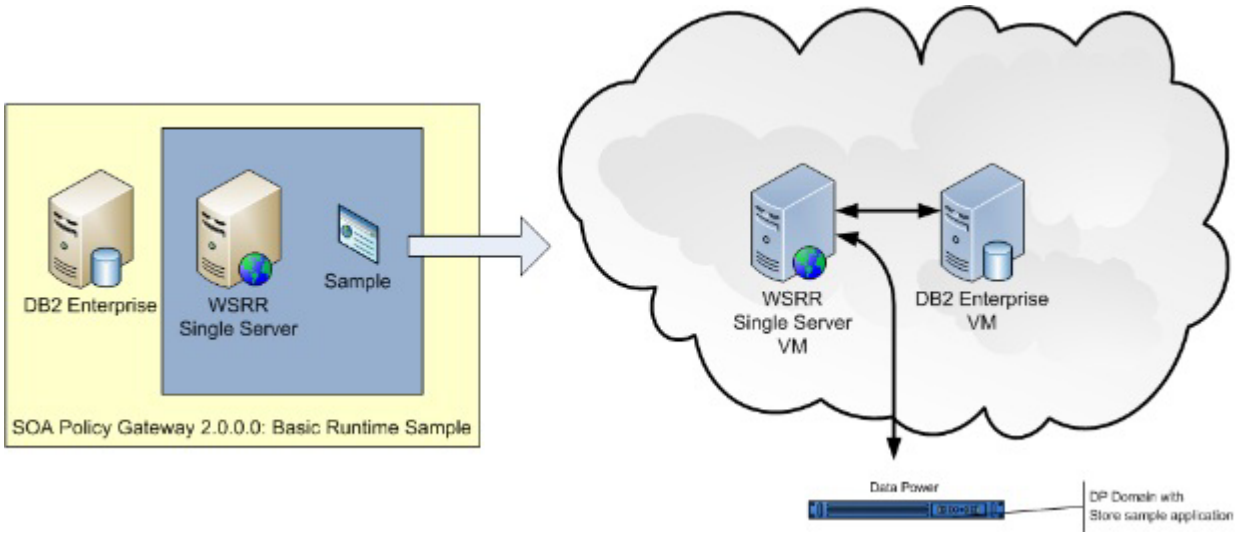
Exemple SOA Policy Gateway Basic Runtime

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

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

- Serveur autonome WSRR
- DB2 Enterprise

Le modèle Exemple SOA Policy Gateway Basic Runtime installe un modèle d'application dans l'environnement déployé. Il installe l'exemple de domaine au sein de DataPower qui implémente un service simple, 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 77. Il installe l'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.



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 SOA Policy Gateway Basic Runtime requiert les scripts suivants.

Sur le composant Serveur autonome WSRR :

- SOA Policy Gateway 2.0.0.0 - Sample

Afficher les paramètres des composants et des scripts :

- «Paramètres de configuration du composant DB2 Enterprise pour le modèle Exemple SOA Policy Gateway Basic Runtime», à la page 29
- «Paramètres de configuration du composant Serveur automome WSRR pour le modèle Exemple SOA Policy Gateway Basic Runtime», à la page 40
- «SOA Policy Gateway 2.0.0.0 - Paramètres de configuration du script Sample pour le modèle Exemple SOA Policy Gateway Basic Runtime», à la page 51

Concepts associés:

«Composant DB2 Enterprise», à la page 26
Le composant DB2 Enterprise fournit certaines options de configuration.

«Composant Serveur autonome WSRR», à la page 38
Le composant Serveur autonome WSRR fournit certaines options de configuration.

«Script : SOA Policy Gateway 2.0.0.0 - Sample», à la page 50
Le script Sample configure les paramètres du modèle d'application à utiliser avec le modèle Exemple SOA Policy Gateway Basic Runtime .

«Modèle d'application», à la page 77
Le modèle d'application est un domaine DataPower configurable et un ensemble d'artefacts WSRR permettant de présenter les fonctions du modèle.

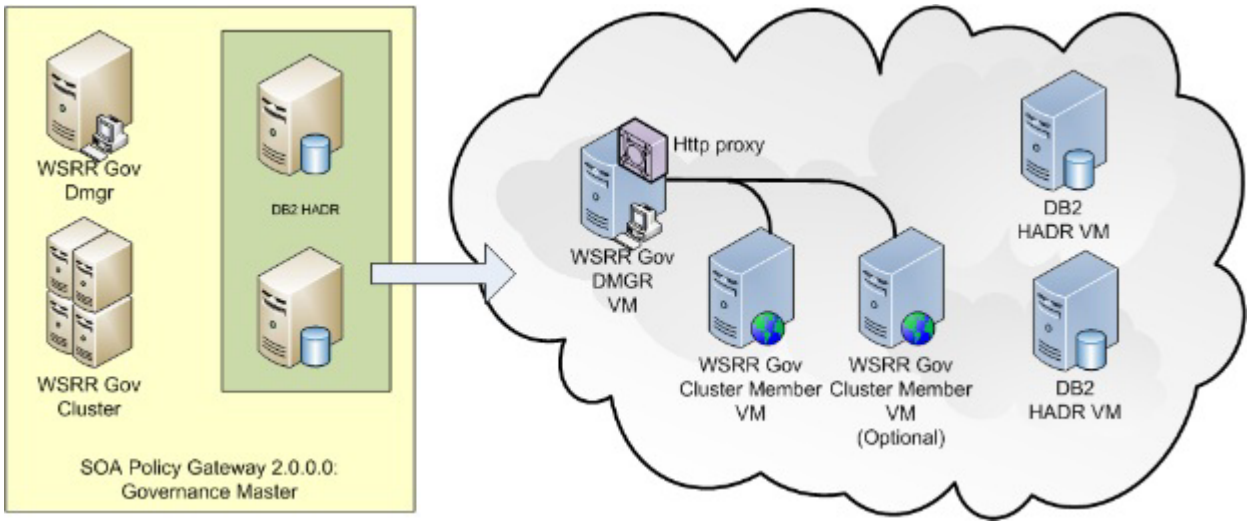
SOA Policy Gateway Governance Master

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. Seul le modèle SOA Policy Gateway Basic Runtime ou le modèle SOA Policy Gateway Advanced Runtime peut être configuré dans Governance Master.



Scripts et options avancées

Le modèle SOA Policy Gateway Governance Master requiert les scripts suivants :

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

Afficher les paramètres des composants et des scripts :

- «Paramètres de configuration du composant principal HADR DB2 Enterprise HADR pour le modèle SOA Policy Gateway Governance Master», à la page 33
- «Paramètres de configuration du composant de secours HADR DB2 Enterprise HADR pour le modèle SOA Policy Gateway Governance Master», à la page 37
- «Paramètres de configuration du composant gestionnaire de déploiement WSRR pour le modèle SOA Policy Gateway Governance Master», à la page 42
- «Paramètres de configuration du composant Noeuds personnalisés WSRR pour le modèle SOA Policy Gateway Governance Master», à la page 44

Utilisation du modèle Governance comme maître de gouvernance

Le modèle SOA Policy Gateway Governance Master est déployé avec le profil d'activation de gouvernance (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 la gouvernance. Les modèles SOA Policy Gateway Basic Runtime et SOA Policy Gateway Advanced Runtime peuvent être déployés au sein de cette intégration en tant que cibles de promotion. Pour plus d'informations sur comment effectuer cette configuration, voir «Scénario : ajout d'un environnement d'exécution supplémentaire au modèle», à la page 74.

Concepts associés:

«Composant principal HADR DB2 Enterprise», à la page 30
Le composant principal HADR DB2 Enterprise fournit certaines options de configuration.

«Composant de secours HADR DB2 Enterprise», à la page 34
Le composant de secours HADR DB2 Enterprise fournit certaines options de configuration.

«Composant Gestionnaire de déploiement WSRR», à la page 40
Le composant Gestionnaire de déploiement WSRR fournit certaines options de configuration.

«Composant Noeuds personnalisés WSRR», à la page 43
Le composant Noeuds personnalisés WSRR fournit certaines options de configuration.

Information associée:

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

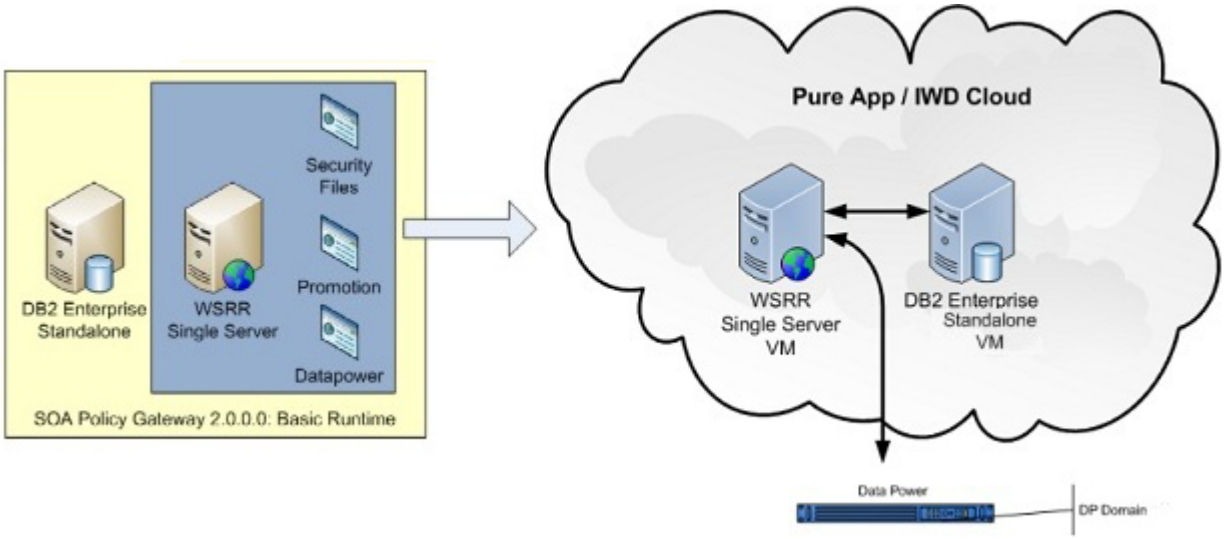
SOA Policy Gateway Basic Runtime

SOA Policy Gateway Basic Runtime propose un moyen simple de fournir un environnement d'exécution qui peut être utilisé en mode autonome ou intégré à l'aide d'un modèle SOA Policy Gateway Governance Master déployé. Le modèle

SOA Policy Gateway Basic Runtime prend en charge le déploiement d'un domaine DataPower qui est configuré pour communiquer avec le serveur d'exécution WSRR mis à disposition dans le modèle.

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

- Serveur autonome WSRR
- DB2 Enterprise



Scripts et options avancées

Le modèle SOA Policy Gateway Basic Runtime requiert les scripts suivants.

Sur le composant Serveur autonome WSRR :

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

Afficher les paramètres des composants et des scripts :

- «Paramètres de configuration du composant Serveur automome WSRR pour le modèle SOA Policy Gateway Basic Runtime», à la page 39
- «Paramètres de configuration du composant DB2 Enterprise pour le modèle SOA Policy Gateway Basic Runtime», à la page 27
- «SOA Policy Gateway 2.0.0.0 - Paramètres de configuration du script Secruity pour le modèle SOA Policy Gateway Basic Runtime», à la page 54
- «SOA Policy Gateway 2.0.0.0 - Paramètres de configuration du script Promotion pour le modèle SOA Policy Gateway Basic Runtime», à la page 48
- «SOA Policy Gateway 2.0.0.0 - Paramètres de configuration du script DataPower Domain pour le modèle SOA Policy Gateway Basic Runtime», à la page 46

Promotion de SOA Policy Gateway Basic Runtime dans une phase d'exécution de gouvernance

Lorsqu'un modèle Basic Runtime est configuré avec un modèle Governance Master, voici ce qui se produit :

- La sécurité inter-cellule est configurée
- Le fichier `promotion.xml` de Governance Master est mis à jour avec les données de déploiement pour le déploiement du modèle Basic Runtime.

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

- production
- staging
- other ou Unset

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 la gouvernance.

Concepts associés:

«Modèle d'application», à la page 77
Le modèle d'application est un domaine DataPower configurable et un ensemble d'artefacts WSRR permettant de présenter les fonctions du modèle.

«Composant DB2 Enterprise», à la page 26
Le composant DB2 Enterprise fournit certaines options de configuration.

«Composant Serveur autonome WSRR», à la page 38
Le composant Serveur autonome WSRR fournit certaines options de configuration.

«Script : SOA Policy Gateway 2.0.0.0 - Security», à la page 53
Le script Security copie les informations de sécurité, contenues dans un fichier ZIP, qui sont nécessaires pour communiquer avec un dispositif DataPower sur la machine Dmgr ou WSRR à partir d'un serveur de fichiers externe qui prend en charge le programme de copie sécurisée (SCP) de Linux.

«Script : SOA Policy Gateway 2.0.0.0 - Promotion», à la page 48
Le script Promotion permet à un modèle SOA Policy Gateway Basic Runtime ou SOA Policy Gateway Advanced Runtime 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 le maître de gouvernance.

«Script : SOA Policy Gateway 2.0.0.0 - DataPower Domain», à la page 45
Le script DataPower Domain met à disposition le domaine DataPower durant le déploiement. Le script configure la connexion entre un domaine DataPower unique et l'exécution de WSRR. Un autre script DataPower Domain est requis pour chaque domaine DataPower qui est connecté à l'exécution de WSRR.

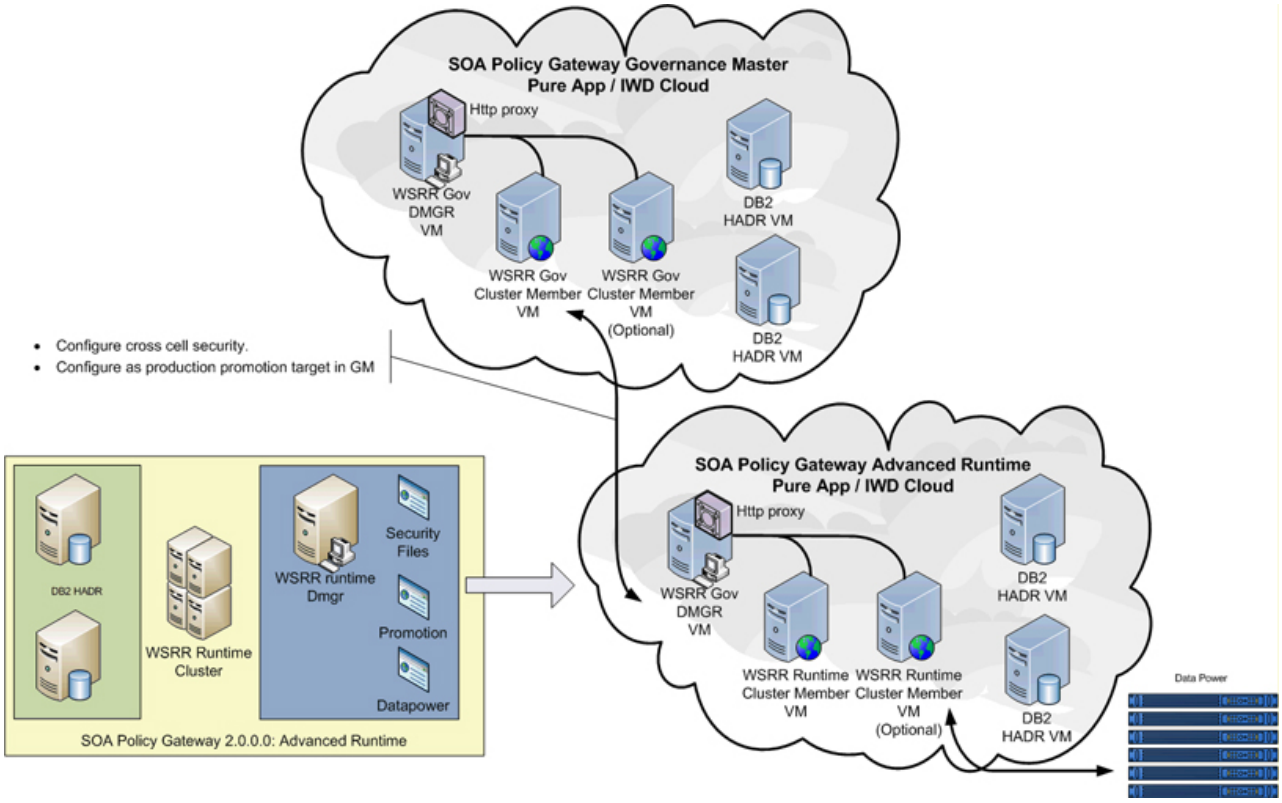
SOA Policy Gateway Advanced Runtime

Le modèle SOA Policy Gateway Advanced Runtime inclut d'autres options haute disponibilité et doit être utilisé avec le modèle SOA Policy Gateway Governance Master.

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

- HADR principal DB2
- HADR de secours DB2
- Gestionnaire de déploiement WSRR

- Noeuds personnalisés WSRR



Scripts et options avancées

Le modèle SOA Policy Gateway Governance Master nécessite les scripts suivants sur le composant du gestionnaire de déploiement de WSRR :

- SOA Policy Gateway 2.0.0.0 - Security
- SOA Policy Gateway 2.0.0.0 - Promotion
- SOA Policy Gateway 2.0.0.0 - DataPower Domain (un par domaine DataPower)

Afficher les paramètres des composants et des scripts :

- «Paramètres de configuration du composant principal HADR DB2 Enterprise HADR pour le modèle SOA Policy Gateway Advanced Runtime», à la page 31
- «Paramètres de configuration du composant de secours HADR DB2 Enterprise HADR pour le modèle SOA Policy Gateway Advanced Runtime», à la page 35
- «Paramètres de configuration du composant gestionnaire de déploiement WSRR pour le modèle SOA Policy Gateway Advanced Runtime», à la page 41
- «Paramètres de configuration du composant Noeuds personnalisés WSRR pour le modèle SOA Policy Gateway Advanced Runtime», à la page 43
- «SOA Policy Gateway 2.0.0.0 - Paramètres de configuration du script Security pour le modèle SOA Policy Gateway Advanced Runtime», à la page 55
- «SOA Policy Gateway 2.0.0.0 - Paramètres de configuration du script Promotion pour le modèle SOA Policy Gateway Advanced Runtime», à la page 49
- «SOA Policy Gateway 2.0.0.0 - Paramètres de configuration du script DataPower Domain pour le modèle SOA Policy Gateway Advanced Runtime», à la page 47

Promotion de SOA Policy Gateway Advanced Runtime dans une phase d'exécution de gouvernance

Lorsqu'un modèle Advanced Runtime est configuré avec un modèle Governance Master, voici ce qui se produit :

- La sécurité inter-cellule est configurée
- Le fichier `promotion.xml` de Governance Master est mis à jour avec les données issues du déploiement du modèle Advanced Runtime.

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

- production
- staging
- autre ou «Unset»

Ces options s'alignent avec les niveaux fournis par le profil d'activation de gouvernance (Governance Enablement Profile) dans WSRR. Si le profile de gouvernance de Governance Master a été altéré, utilisez «autre» comme niveau de promotion. 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 la gouvernance.

Concepts associés:

«Composant principal HADR DB2 Enterprise», à la page 30
Le composant principal HADR DB2 Enterprise fournit certaines options de configuration.

«Composant de secours HADR DB2 Enterprise», à la page 34
Le composant de secours HADR DB2 Enterprise fournit certaines options de configuration.

«Composant Gestionnaire de déploiement WSRR», à la page 40
Le composant Gestionnaire de déploiement WSRR fournit certaines options de configuration.

«Composant Noeuds personnalisés WSRR», à la page 43
Le composant Noeuds personnalisés WSRR fournit certaines options de configuration.

«Script : SOA Policy Gateway 2.0.0.0 - Security», à la page 53
Le script Security copie les informations de sécurité, contenues dans un fichier ZIP, qui sont nécessaires pour communiquer avec un dispositif DataPower sur la machine Dmgr ou WSRR à partir d'un serveur de fichiers externe qui prend en charge le programme de copie sécurisée (SCP) de Linux.

«Script : SOA Policy Gateway 2.0.0.0 - Promotion», à la page 48
Le script Promotion permet à un modèle SOA Policy Gateway Basic Runtime ou SOA Policy Gateway Advanced Runtime 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 le maître de gouvernance.

«Script : SOA Policy Gateway 2.0.0.0 - DataPower Domain», à la page 45
Le script DataPower Domain met à disposition le domaine DataPower durant le déploiement. Le script configure la connexion entre un domaine DataPower unique et l'exécution de WSRR. Un autre script DataPower Domain est requis pour chaque domaine DataPower qui est connecté à l'exécution de WSRR.

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 9.7.5 sont décrits dans le tableau suivant :

Tableau 2. Paramètres configurables

Nom du paramètre	Description
Unités centrales virtuelles	Nombre de processeurs virtuels alloués pour la machine virtuelle représentée par cet élément.
Taille de mémoire (Mo)	Taille de la mémoire allouée à cette machine virtuelle, en mégaoctets.
Mot de passe (db2inst1)	Le mot de passe de l'ID utilisateur db2inst1 du système d'exploitation. 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.
Confirmation du mot de passe	Vérifie le mot de passe de db2inst1.

Tableau 2. Paramètres configurables (suite)

Nom du paramètre	Description
Mot de passe (db2fenc1)	Le mot de passe de l'ID utilisateur servant à exécuter des fonctions UDF et des procédures mémorisées en dehors de l'espace adresse utilisé par la base de données DB2. L'utilisateur isolé est un utilisateur disposant de droits restreints pour exécuter certaines procédures mémorisées (des procédures mémorisées "isolées"). Les limites imposées à l'utilisateur par le système d'exploitation permettent d'éviter que les procédures mémorisées isolées n'écrasent les fichiers de l'instance.
Confirmation du mot de passe	Vérifie le mot de passe de db2fenc1.
Mot de passe (dasusr1)	L'ID de l'utilisateur du serveur d'administration DB2 exécutant le serveur d'administration DB2 sur votre système. L'utilisateur par défaut est dasusr1 et le groupe par défaut est dasadm1. 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.
Confirmation du mot de passe	Vérifie le mot de passe de dasusr1.
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.

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

Paramètres de configuration du composant DB2 Enterprise pour le modèle SOA Policy Gateway Basic Runtime

Les paramètres obligatoires sans valeur par défaut doivent être configurés avant le déploiement du modèle.

Tableau 3. Paramètres configurables

Nom du paramètre	Obligatoire	Valeur par défaut	Description
Unités centrales virtuelles	Oui	1	Nombre de processeurs virtuels alloués pour la machine virtuelle représentée par cet élément.
Taille de mémoire (Mo)	Oui	2048	Taille de la mémoire allouée à cette machine virtuelle, en mégaoctets.
Mot de passe (db2inst1)	Oui		Le mot de passe de l'ID utilisateur db2inst1 du système d'exploitation. 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.
Confirmation du mot de passe	Oui		Vérifie le mot de passe de db2inst1.

Tableau 3. Paramètres configurables (suite)

Nom du paramètre	Obligatoire	Valeur par défaut	Description
Mot de passe (db2fenc1)	Oui		Le mot de passe de l'ID utilisateur servant à exécuter des fonctions UDF et des procédures mémorisées en dehors de l'espace adresse utilisé par la base de données DB2. L'utilisateur isolé est un utilisateur disposant de droits restreints pour exécuter certaines procédures mémorisées (des procédures mémorisées "isolées"). Les limites imposées à l'utilisateur par le système d'exploitation permettent d'éviter que les procédures mémorisées isolées n'écrasent les fichiers de l'instance.
Confirmation du mot de passe	Oui		Vérifie le mot de passe de db2fenc1.
Mot de passe (dasusr1)	Oui		L'ID de l'utilisateur du serveur d'administration DB2 exécutant le serveur d'administration DB2 sur votre système. L'utilisateur par défaut est dasusr1 et le groupe par défaut est dasadm1. 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.
Confirmation du mot de passe	Oui		Vérifie le mot de passe de dasusr1.
Mot de passe (superutilisateur)	Oui		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	Oui		Vérifie le mot de passe du superutilisateur.
Mot de passe (utilisateur virtuel)	Oui		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	Oui		Vérifie le mot de passe de l'utilisateur virtuel.

Paramètres de configuration du composant DB2 Enterprise pour le modèle Exemple SOA Policy Gateway Basic Runtime

Dans l'Exemple SOA Policy Gateway Basic Runtime, les valeurs par défaut sont préconfigurées pour tous les paramètres.

Tableau 4. Paramètres configurés

Nom du paramètre	Obligatoire	Valeur par défaut	Description
Unités centrales virtuelles	Oui	1	Nombre de processeurs virtuels alloués pour la machine virtuelle représentée par cet élément.
Taille de mémoire (Mo)	Oui	2048	Taille de la mémoire allouée à cette machine virtuelle, en mégaoctets.
Mot de passe (db2inst1)	Oui	mot de passe	Le mot de passe de l'ID utilisateur db2inst1 du système d'exploitation. 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.
Confirmation du mot de passe	Oui	mot de passe	Vérifie le mot de passe de db2inst1.
Mot de passe (db2fenc1)	Oui	mot de passe	Le mot de passe de l'ID utilisateur servant à exécuter des fonctions UDF et des procédures mémorisées en dehors de l'espace adresse utilisé par la base de données DB2. L'utilisateur isolé est un utilisateur disposant de droits restreints pour exécuter certaines procédures mémorisées (des procédures mémorisées "isolées"). Les limites imposées à l'utilisateur par le système d'exploitation permettent d'éviter que les procédures mémorisées isolées n'écrasent les fichiers de l'instance.
Confirmation du mot de passe	Oui	mot de passe	Vérifie le mot de passe de db2fenc1.
Mot de passe (dasusr1)	Oui	mot de passe	L'ID de l'utilisateur du serveur d'administration DB2 exécutant le serveur d'administration DB2 sur votre système. L'utilisateur par défaut est dasusr1 et le groupe par défaut est dasadm1. 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.
Confirmation du mot de passe	Oui	mot de passe	Vérifie le mot de passe de dasusr1.

Tableau 4. Paramètres configurés (suite)

Nom du paramètre	Obligatoire	Valeur par défaut	Description
Mot de passe (superutilisateur)	Oui	mot de passe	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	Oui	mot de passe	Vérifie le mot de passe du superutilisateur.
Mot de passe (utilisateur virtuel)	Oui	mot de passe	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	Oui	mot de passe	Vérifie le mot de passe de l'utilisateur virtuel.

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 5. Paramètres configurables

Nom du paramètre	Description
Unités centrales virtuelles	Nombre de processeurs virtuels alloués pour la machine virtuelle représentée par cet élément.
Taille de mémoire (Mo)	Taille de la mémoire allouée à cette machine virtuelle, en mégaoctets.
Mot de passe (db2inst1)	Le mot de passe de l'ID utilisateur db2inst1 du système d'exploitation. 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.
Confirmation du mot de passe	Vérifie le mot de passe de db2inst1.
Mot de passe (db2fenc1)	Le mot de passe de l'ID utilisateur servant à exécuter des fonctions UDF et des procédures mémorisées en dehors de l'espace adresse utilisé par la base de données DB2. L'utilisateur isolé est un utilisateur disposant de droits restreints pour exécuter certaines procédures mémorisées (des procédures mémorisées "isolées"). Les limites imposées à l'utilisateur par le système d'exploitation permettent d'éviter que les procédures mémorisées isolées n'écrasent les fichiers de l'instance.
Confirmation du mot de passe	Vérifie le mot de passe de db2fenc1.

Tableau 5. Paramètres configurables (suite)

Nom du paramètre	Description
Mot de passe (dasusr1)	Le mot de passe pour l'ID de l'utilisateur du serveur d'administration DB2 exécutant le serveur d'administration DB2 sur votre système. L'utilisateur par défaut est dasusr1 et le groupe par défaut est dasadm1. 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.
Confirmation du mot de passe	Vérifie le mot de passe de dasusr1.
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.

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

Paramètres de configuration du composant principal HADR DB2 Enterprise HADR pour le modèle SOA Policy Gateway Advanced Runtime

Les paramètres obligatoires sans valeur par défaut doivent être configurés avant le déploiement du modèle.

Tableau 6. Paramètres configurables

Nom du paramètre	Obligatoire	Valeur par défaut	Description
Unités centrales virtuelles	Oui	1	Nombre de processeurs virtuels alloués pour la machine virtuelle représentée par cet élément.
Taille de mémoire (Mo)	Oui	2048	Taille de la mémoire allouée à cette machine virtuelle, en mégaoctets.
Mot de passe (db2inst1)	Oui		Le mot de passe de l'ID utilisateur db2inst1 du système d'exploitation. 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.
Confirmation du mot de passe	Oui		Vérifie le mot de passe de db2inst1.

Tableau 6. Paramètres configurables (suite)

Nom du paramètre	Obligatoire	Valeur par défaut	Description
Mot de passe (db2fenc1)	Oui		Le mot de passe de l'ID utilisateur servant à exécuter des fonctions UDF et des procédures mémorisées en dehors de l'espace adresse utilisé par la base de données DB2. L'utilisateur isolé est un utilisateur disposant de droits restreints pour exécuter certaines procédures mémorisées (des procédures mémorisées "isolées"). Les limites imposées à l'utilisateur par le système d'exploitation permettent d'éviter que les procédures mémorisées isolées n'écrasent les fichiers de l'instance.
Confirmation du mot de passe	Oui		Vérifie le mot de passe de db2fenc1.
Mot de passe (dasusr1)	Oui		Le mot de passe pour l'ID de l'utilisateur du serveur d'administration DB2 exécutant le serveur d'administration DB2 sur votre système. L'utilisateur par défaut est dasusr1 et le groupe par défaut est dasadm1. 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.
Confirmation du mot de passe	Oui		Vérifie le mot de passe de dasusr1.
Mot de passe (superutilisateur)	Oui		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	Oui		Vérifie le mot de passe du superutilisateur.
Mot de passe (utilisateur virtuel)	Oui		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	Oui		Vérifie le mot de passe de l'utilisateur virtuel.

Paramètres de configuration du composant principal HADR DB2 Enterprise HADR pour le modèle SOA Policy Gateway Governance Master

Les paramètres obligatoires sans valeur par défaut doivent être configurés avant le déploiement du modèle.

Tableau 7. Paramètres configurables

Nom du paramètre	Obligatoire	Valeur par défaut	Description
Unités centrales virtuelles	Oui	1	Nombre de processeurs virtuels alloués pour la machine virtuelle représentée par cet élément.
Taille de mémoire (Mo)	Oui	2048	Taille de la mémoire allouée à cette machine virtuelle, en mégaoctets.
Mot de passe (db2inst1)	Oui		Le mot de passe de l'ID utilisateur db2inst1 du système d'exploitation. 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.
Confirmation du mot de passe	Oui		Vérifie le mot de passe de db2inst1.
Mot de passe (db2fenc1)	Oui		Le mot de passe de l'ID utilisateur servant à exécuter des fonctions UDF et des procédures mémorisées en dehors de l'espace adresse utilisé par la base de données DB2. L'utilisateur isolé est un utilisateur disposant de droits restreints pour exécuter certaines procédures mémorisées (des procédures mémorisées "isolées"). Les limites imposées à l'utilisateur par le système d'exploitation permettent d'éviter que les procédures mémorisées isolées n'écrasent les fichiers de l'instance.
Confirmation du mot de passe	Oui		Vérifie le mot de passe de db2fenc1.

Tableau 7. Paramètres configurables (suite)

Nom du paramètre	Obligatoire	Valeur par défaut	Description
Mot de passe (dasusr1)	Oui		Le mot de passe pour l'ID de l'utilisateur du serveur d'administration DB2 exécutant le serveur d'administration DB2 sur votre système. L'utilisateur par défaut est dasusr1 et le groupe par défaut est dasadm1. 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.
Confirmation du mot de passe	Oui		Vérifie le mot de passe de dasusr1.
Mot de passe (superutilisateur)	Oui		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	Oui		Vérifie le mot de passe du superutilisateur.
Mot de passe (utilisateur virtuel)	Oui		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	Oui		Vérifie le mot de passe de l'utilisateur virtuel.

Composant de secours HADR DB2 Enterprise

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

Tableau 8. Paramètres configurables

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

Tableau 8. Paramètres configurables (suite)

Nom du paramètre	Description
Taille de mémoire (Mo)	Taille de la mémoire allouée à cette machine virtuelle, en mégaoctets.
Mot de passe (db2inst1)	Le mot de passe de l'ID utilisateur db2inst1 du système d'exploitation. 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.
Confirmation du mot de passe	Vérifie le mot de passe de db2inst1.
Mot de passe (db2fenc1)	Le mot de passe de l'ID utilisateur servant à exécuter des fonctions UDF et des procédures mémorisées en dehors de l'espace adresse utilisé par la base de données DB2. L'utilisateur isolé est un utilisateur disposant de droits restreints pour exécuter certaines procédures mémorisées (des procédures mémorisées "isolées"). Les limites imposées à l'utilisateur par le système d'exploitation permettent d'éviter que les procédures mémorisées isolées n'écrasent les fichiers de l'instance.
Confirmation du mot de passe	Vérifie le mot de passe de db2fenc1.
Mot de passe (dasusr1)	Le mot de passe pour l'ID de l'utilisateur du serveur d'administration DB2 exécutant le serveur d'administration DB2 sur votre système. L'utilisateur par défaut est dasusr1 et le groupe par défaut est dasadm1. 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.
Confirmation du mot de passe	Vérifie le mot de passe de dasusr1.
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.

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

Paramètres de configuration du composant de secours HADR DB2 Enterprise HADR pour le modèle SOA Policy Gateway Advanced Runtime

Les paramètres obligatoires sans valeur par défaut doivent être configurés avant le déploiement du modèle.

Tableau 9. Paramètres configurables

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

Tableau 9. Paramètres configurables (suite)

Nom du paramètre	Obligatoire	Valeur par défaut	Description
Mot de passe (db2inst1)	Oui		Le mot de passe de l'ID utilisateur db2inst1 du système d'exploitation. 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.
Confirmation du mot de passe	Oui		Vérifie le mot de passe de db2inst1.
Mot de passe (db2fenc1)	Oui		Le mot de passe de l'ID utilisateur servant à exécuter des fonctions UDF et des procédures mémorisées en dehors de l'espace adresse utilisé par la base de données DB2. L'utilisateur isolé est un utilisateur disposant de droits restreints pour exécuter certaines procédures mémorisées (des procédures mémorisées "isolées"). Les limites imposées à l'utilisateur par le système d'exploitation permettent d'éviter que les procédures mémorisées isolées n'écrasent les fichiers de l'instance.
Confirmation du mot de passe	Oui		Vérifie le mot de passe de db2fenc1.
Mot de passe (dasusr1)	Oui		Le mot de passe pour l'ID de l'utilisateur du serveur d'administration DB2 exécutant le serveur d'administration DB2 sur votre système. L'utilisateur par défaut est dasusr1 et le groupe par défaut est dasadm1. 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.
Confirmation du mot de passe	Oui		Vérifie le mot de passe de dasusr1.
Mot de passe (superutilisateur)	Oui		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	Oui		Vérifie le mot de passe du superutilisateur.

Tableau 9. Paramètres configurables (suite)

Nom du paramètre	Obligatoire	Valeur par défaut	Description
Mot de passe (utilisateur virtuel)	Oui		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	Oui		Vérifie le mot de passe de l'utilisateur virtuel.

Paramètres de configuration du composant de secours HADR DB2 Enterprise HADR pour le modèle SOA Policy Gateway Governance Master

Les paramètres obligatoires sans valeur par défaut doivent être configurés avant le déploiement du modèle.

Tableau 10. Paramètres configurables

Nom du paramètre	Obligatoire	Valeur par défaut	Description
Unités centrales virtuelles	Oui	1	Nombre de processeurs virtuels alloués pour la machine virtuelle représentée par cet élément.
Taille de mémoire (Mo)	Oui	2048	Taille de la mémoire allouée à cette machine virtuelle, en mégaoctets.
Mot de passe (db2inst1)	Oui		Le mot de passe de l'ID utilisateur db2inst1 du système d'exploitation. 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.
Confirmation du mot de passe	Oui		Vérifie le mot de passe de db2inst1.
Mot de passe (db2fenc1)	Oui		Le mot de passe de l'ID utilisateur servant à exécuter des fonctions UDF et des procédures mémorisées en dehors de l'espace adresse utilisé par la base de données DB2. L'utilisateur isolé est un utilisateur disposant de droits restreints pour exécuter certaines procédures mémorisées (des procédures mémorisées "isolées"). Les limites imposées à l'utilisateur par le système d'exploitation permettent d'éviter que les procédures mémorisées isolées n'écrasent les fichiers de l'instance.
Confirmation du mot de passe	Oui		Vérifie le mot de passe de db2fenc1.

Tableau 10. Paramètres configurables (suite)

Nom du paramètre	Obligatoire	Valeur par défaut	Description
Mot de passe (dasusr1)	Oui		Le mot de passe pour l'ID de l'utilisateur du serveur d'administration DB2 exécutant le serveur d'administration DB2 sur votre système. L'utilisateur par défaut est dasusr1 et le groupe par défaut est dasadm1. 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.
Confirmation du mot de passe	Oui		Vérifie le mot de passe de dasusr1.
Mot de passe (superutilisateur)	Oui		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	Oui		Vérifie le mot de passe du superutilisateur.
Mot de passe (utilisateur virtuel)	Oui		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	Oui		Vérifie le mot de passe de l'utilisateur virtuel.

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 11. Paramètres configurés

Nom du paramètre	Description
Unités centrales virtuelles	Nombre de processeurs virtuels alloués pour la machine virtuelle représentée par cet élément.
Taille de mémoire (Mo)	Taille de la mémoire allouée à cette machine virtuelle, en mégaoctets.
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	Nom d'utilisateur de l'administrateur d'environnement WebSphere.

Tableau 11. Paramètres configurés (suite)

Nom du paramètre	Description
Mot de passe de l'administrateur WebSphere	Mot de passe de l'administrateur de l'environnement WebSphere.
Confirmation du mot de passe	Vérifie l'entrée de l'utilisateur pour le mot de passe administrateur WebSphere.
Mémoire physique de réserve	Cette machine virtuelle a réservé la mémoire physique à un usage exclusif.

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

Paramètres de configuration du composant Serveur automome WSRR pour le modèle SOA Policy Gateway Basic Runtime

Les paramètres obligatoires sans valeur par défaut doivent être configurés avant le déploiement du modèle.

Tableau 12. Paramètres configurables

Nom du paramètre	Obligatoire	Valeur par défaut	Description
Unités centrales virtuelles	Oui	1	Nombre de processeurs virtuels alloués pour la machine virtuelle représentée par cet élément.
Taille de mémoire (Mo)	Oui	4096	Taille de la mémoire allouée à cette machine virtuelle, en mégaoctets.
Mémoire physique de réserve	Oui	False	Cette machine virtuelle a réservé la mémoire physique à un usage exclusif.
Nom de cellule	Oui	SOAPolicyBasicCell	Nom de cellule WebSphere sur la machine virtuelle du modèle Basic Runtime.
Nom du noeud	Oui	SOAPolicyBasicNode	Nom du noeud WebSphere sur la machine virtuelle du modèle Basic Runtime.
Mot de passe (superutilisateur)	Oui		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	Oui		Vérifie l'entrée de l'utilisateur pour Mot de passe (superutilisateur).
Nom d'utilisateur administrateur WebSphere	Oui	virtuser	Nom d'utilisateur de l'administrateur d'environnement WebSphere.
Mot de passe de l'administrateur WebSphere	Oui		Mot de passe de l'administrateur de l'environnement WebSphere.
Confirmation du mot de passe	Oui		Vérifie l'entrée de l'utilisateur pour le mot de passe administrateur WebSphere.

Paramètres de configuration du composant Serveur automome WSRR pour le modèle Exemple SOA Policy Gateway Basic Runtime

Dans l'Exemple SOA Policy Gateway Basic Runtime, les valeurs par défaut sont préconfigurées pour tous les paramètres.

Tableau 13. Paramètres configurés

Nom du paramètre	Obligatoire	Valeur par défaut	Description
Unités centrales virtuelles	Oui	1	Nombre de processeurs virtuels alloués pour la machine virtuelle représentée par cet élément.
Taille de mémoire (Mo)	Oui	4096	Taille de la mémoire allouée à cette machine virtuelle, en mégaoctets.
Mémoire physique de réserve	Oui	False	Cette machine virtuelle a réservé la mémoire physique à un usage exclusif.
Mot de passe (superutilisateur)	Oui	mot de passe	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	Oui	mot de passe	Vérifie l'entrée de l'utilisateur pour Mot de passe (superutilisateur).
Nom d'utilisateur administrateur WebSphere	Oui	virtuser	Nom d'utilisateur de l'administrateur d'environnement WebSphere.
Mot de passe de l'administrateur WebSphere	Oui	mot de passe	Mot de passe de l'administrateur de l'environnement WebSphere.
Confirmation du mot de passe	Oui	mot de passe	Vérifie l'entrée de l'utilisateur pour le mot de passe administrateur WebSphere.

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 14. Paramètres configurables

Nom du paramètre	Description
Unités centrales virtuelles	Nombre de processeurs virtuels alloués pour la machine virtuelle représentée par cet élément.
Taille de mémoire (Mo)	Taille de la mémoire allouée à cette machine virtuelle, en mégaoctets.
Unités centrales physiques de réserve	Cette machine virtuelle a réservé les unités centrales physiques à un usage exclusif.
Mémoire physique de réserve	Cette machine virtuelle a réservé la mémoire physique à un usage exclusif.
Nom de la cellule	Nom de cellule WebSphere pour le modèle d'exécution avancée Advanced Runtime.

Tableau 14. Paramètres configurables (suite)

Nom du paramètre	Description
Nom du noeud	Nom de noeud pour le noeud WebSphere 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	Nom d'utilisateur de l'administrateur d'environnement WebSphere.
Mot de passe de l'administrateur WebSphere	Mot de passe de l'administrateur de l'environnement WebSphere.
Confirmation du mot de passe	Vérifie l'entrée de l'utilisateur pour le mot de passe administrateur WebSphere.

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

Paramètres de configuration du composant gestionnaire de déploiement WSRR pour le modèle SOA Policy Gateway Advanced Runtime

Les paramètres obligatoires sans valeur par défaut doivent être configurés avant le déploiement du modèle.

Tableau 15. Paramètres configurables

Nom du paramètre	Obligatoire	Valeur par défaut	Description
Unités centrales virtuelles	Oui	1	Nombre de processeurs virtuels alloués pour la machine virtuelle représentée par cet élément.
Taille de mémoire (Mo)	Oui	2048	Taille de la mémoire allouée à cette machine virtuelle, en mégaoctets.
Unités centrales physiques de réserve	Oui	Faux	Cette machine virtuelle a réservé les unités centrales physiques à un usage exclusif.
Mémoire physique de réserve	Oui	Faux	Cette machine virtuelle a réservé la mémoire physique à un usage exclusif.
Nom de la cellule	Oui	SOAPolicyAdvancedCell	Nom de cellule WebSphere pour le modèle d'exécution avancée Advanced Runtime.
Nom du noeud	Oui	SOAPolicyAdvancedNode	Nom de noeud pour le noeud WebSphere résidant sur la machine virtuelle Gestionnaire de déploiement dans le modèle d'exécution avancée Advanced Runtime.
Mot de passe (superutilisateur)	Oui		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.

Tableau 15. Paramètres configurables (suite)

Nom du paramètre	Obligatoire	Valeur par défaut	Description
Confirmation du mot de passe	Oui		Vérifie l'entrée de l'utilisateur pour Mot de passe (superutilisateur).
Nom d'utilisateur administrateur WebSphere	Oui	virtuser	Nom d'utilisateur de l'administrateur d'environnement WebSphere.
Mot de passe de l'administrateur WebSphere	Oui		Mot de passe de l'administrateur de l'environnement WebSphere.
Confirmation du mot de passe	Oui		Vérifie l'entrée de l'utilisateur pour le mot de passe administrateur WebSphere.

Paramètres de configuration du composant gestionnaire de déploiement WSRR pour le modèle SOA Policy Gateway Governance Master

Les paramètres obligatoires sans valeur par défaut doivent être configurés avant le déploiement du modèle.

Tableau 16. Paramètres configurables

Nom du paramètre	Obligatoire	Valeur par défaut	Description
Unités centrales virtuelles	Oui	1	Nombre de processeurs virtuels alloués pour la machine virtuelle représentée par cet élément.
Taille de mémoire (Mo)	Oui	2048	Taille de la mémoire allouée à cette machine virtuelle, en mégaoctets.
Unités centrales physiques de réserve	Oui	Faux	Cette machine virtuelle a réservé les unités centrales physiques à un usage exclusif.
Mémoire physique de réserve	Oui	Faux	Cette machine virtuelle a réservé la mémoire physique à un usage exclusif.
Nom de la cellule	Oui	SOAPolicyGMCell	Nom de cellule WebSphere pour le modèle d'exécution avancée Advanced Runtime.
Nom du noeud	Oui	SOAPolicyGMNode	Nom de noeud pour le noeud WebSphere résidant sur la machine virtuelle Gestionnaire de déploiement dans le modèle d'exécution avancée Advanced Runtime.
Mot de passe (superutilisateur)	Oui		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	Oui		Vérifie l'entrée de l'utilisateur pour Mot de passe (superutilisateur).

Tableau 16. Paramètres configurables (suite)

Nom du paramètre	Obligatoire	Valeur par défaut	Description
Nom d'utilisateur administrateur WebSphere	Oui	virtuser	Nom d'utilisateur de l'administrateur d'environnement WebSphere.
Mot de passe de l'administrateur WebSphere	Oui		Mot de passe de l'administrateur de l'environnement WebSphere.
Confirmation du mot de passe	Oui		Vérifie l'entrée de l'utilisateur pour le mot de passe administrateur WebSphere.

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 17. Paramètres configurables

Nom du paramètre	Description
Unités centrales virtuelles	Nombre de processeurs virtuels alloués pour la machine virtuelle représentée par cet élément.
Taille de mémoire (Mo)	Taille de la mémoire allouée à cette machine virtuelle, en mégaoctets.
Unités centrales physiques de réserve	Cette machine virtuelle a réservé les unités centrales physiques à un usage exclusif.
Mémoire physique de réserve	Cette machine virtuelle a réservé la mémoire physique à un usage exclusif.
Nom de la cellule	La valeur du nom de cellule dans la configuration du composant Noeuds personnalisés est ignoré. Le nom de cellule indiqué dans la configuration du composant Gestionnaire de déploiement est utilisé.
Nom du noeud	Nom de noeud pour le noeud WebSphere résidant sur la machine virtuelle Nœud personnalisé 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 le Mot de passe (superutilisateur).
Nom d'utilisateur administrateur WebSphere	Nom d'utilisateur de l'administrateur d'environnement WebSphere.
Mot de passe de l'administrateur WebSphere	Mot de passe de l'administrateur de l'environnement WebSphere.
Confirmation du mot de passe	Vérifie l'entrée de l'utilisateur pour le mot de passe administrateur WebSphere.

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

Paramètres de configuration du composant Noeuds personnalisés WSRR pour le modèle SOA Policy Gateway Advanced Runtime

Les paramètres obligatoires sans valeur par défaut doivent être configurés avant le déploiement du modèle.

Tableau 18. Paramètres configurables

Nom du paramètre	Obligatoire	Valeur par défaut	Description
Unités centrales virtuelles	Oui	2	Nombre de processeurs virtuels alloués pour la machine virtuelle représentée par cet élément.
Taille de mémoire (Mo)	Oui	4096	Taille de la mémoire allouée à cette machine virtuelle, en mégaoctets.
Unités centrales physiques de réserve	Oui	Faux	Cette machine virtuelle a réservé les unités centrales physiques à un usage exclusif.
Mémoire physique de réserve	Oui	Faux	Cette machine virtuelle a réservé la mémoire physique à un usage exclusif.
Nom du noeud	Oui	SOAPolicyAdvancedNode	Nom de noeud pour le noeud WebSphere résidant sur la machine virtuelle Nœud personnalisé dans le modèle d'exécution avancée Advanced Runtime.
Mot de passe (superutilisateur)	Oui		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	Oui		Vérifie l'entrée de l'utilisateur pour le Mot de passe (superutilisateur).
Nom d'utilisateur administrateur WebSphere	Oui	utilisateur virtuel	Nom d'utilisateur de l'administrateur d'environnement WebSphere.
Mot de passe administrateur WebSphere	Oui		Mot de passe de l'administrateur de l'environnement WebSphere.
Confirmation du mot de passe	Oui		Vérifie l'entrée de l'utilisateur pour le mot de passe administrateur WebSphere.

Paramètres de configuration du composant Noeuds personnalisés WSRR pour le modèle SOA Policy Gateway Governance Master

Les paramètres obligatoires sans valeur par défaut doivent être configurés avant le déploiement du modèle.

Tableau 19. Paramètres configurables

Nom du paramètre	Obligatoire	Valeur par défaut	Description
Unités centrales virtuelles	Oui	2	Nombre de processeurs virtuels alloués pour la machine virtuelle représentée par cet élément.
Taille de mémoire (Mo)	Oui	4096	Taille de la mémoire allouée à cette machine virtuelle, en mégaoctets.

Tableau 19. Paramètres configurables (suite)

Nom du paramètre	Obligatoire	Valeur par défaut	Description
Unités centrales physiques de réserve	Oui	Faux	Cette machine virtuelle a réservé les unités centrales physiques à un usage exclusif.
Mémoire physique de réserve	Oui	Faux	Cette machine virtuelle a réservé la mémoire physique à un usage exclusif.
Nom du noeud	Oui	SOAPolicyGMNode	Nom de noeud pour le noeud WebSphere résidant sur la machine virtuelle Nœud personnalisé dans le modèle d'exécution avancée Advanced Runtime.
Mot de passe (superutilisateur)	Oui		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	Oui		Vérifie l'entrée de l'utilisateur pour le Mot de passe (superutilisateur).
Nom d'utilisateur administrateur WebSphere	Oui	utilisateur virtuel	Nom d'utilisateur de l'administrateur d'environnement WebSphere.
Mot de passe administrateur WebSphere	Oui		Mot de passe de l'administrateur de l'environnement WebSphere.
Confirmation du mot de passe	Oui		Vérifie l'entrée de l'utilisateur pour le mot de passe administrateur WebSphere.

Packages de script

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

Script : SOA Policy Gateway 2.0.0.0 - DataPower Domain

Le script DataPower Domain met à disposition le domaine DataPower durant le déploiement. Le script configure la connexion entre un domaine DataPower unique et l'exécution de WSRR. Un autre script DataPower Domain est requis pour chaque domaine DataPower qui est connecté à l'exécution de WSRR.

Paramètres

Tableau 20. Paramètres configurables

Nom du paramètre	Description
DataPower_hostname	Nom d'hôte du dispositif DataPower dans lequel le modèle d'application doit être installé.
DataPower_XML_mgmt_port	Numéro de port utilisé pour l'interface de gestion XML de DataPower, généralement 5550.
Datapower_admin_id	ID utilisateur de l'administrateur disposant des droits appropriés pour utiliser l'interface de gestion XML.
DataPower_admin_password	Mot de passe pour DataPower_admin_id.
Confirmation du mot de passe	Vérifie l'entrée de l'utilisateur pour DataPower_admin_password.
New_DataPower_domain	Nouveau nom de domaine à créer pour le dispositif DataPower. Il ne doit pas correspondre à un domaine existant sinon le package de script va échouer ou quitter. La valeur ne peut pas contenir d'espace.
securityFileCleanUp	Détermine si le fichier `DomainZipFile.zip` et le certificat WSRR téléchargé vers DataPower sont supprimés de l'instance WSRR dans laquelle les packages de script sont exécutés. S'il n'est pas supprimé, ce fichier représente un risque pour la sécurité au cas où les certificats seraient maintenus sur l'instance.

SOA Policy Gateway 2.0.0.0 - Paramètres de configuration du script DataPower Domain pour le modèle SOA Policy Gateway Basic Runtime

Les paramètres obligatoires sans valeur par défaut doivent être configurés avant le déploiement du modèle.

Tableau 21. Paramètres configurables

Nom du paramètre	Obligatoire	Valeur par défaut	Description
DataPower_hostname	Oui		Nom d'hôte du dispositif DataPower dans lequel le modèle d'application doit être installé.
DataPower_XML_mgmt_port	Oui	5550	Numéro de port utilisé pour l'interface de gestion XML de DataPower, généralement 5550.
Datapower_admin_id	Oui		ID utilisateur de l'administrateur disposant des droits appropriés pour utiliser l'interface de gestion XML.
DataPower_admin_password	Oui		Mot de passe pour DataPower_admin_id.
Confirmation du mot de passe	Oui		Vérifie l'entrée de l'utilisateur pour DataPower_admin_password.

Tableau 21. Paramètres configurables (suite)

Nom du paramètre	Obligatoire	Valeur par défaut	Description
New_DataPower_domain	Oui		Nouveau nom de domaine à créer pour le dispositif DataPower. Il ne doit pas correspondre à un domaine existant sinon le package de script va échouer ou quitter. La valeur ne peut pas contenir d'espace.
Remove_security_files	Oui	true	Détermine si le fichier `DomainZipFile.zip` et le certificat WSRR téléchargé vers DataPower sont supprimés de l'instance WSRR dans laquelle les packages de script sont exécutés. S'il n'est pas supprimé, ce fichier représente un risque pour la sécurité au cas où les certificats seraient maintenus sur l'instance.

SOA Policy Gateway 2.0.0.0 - Paramètres de configuration du script DataPower Domain pour le modèle SOA Policy Gateway Advanced Runtime

Les paramètres obligatoires sans valeur par défaut doivent être configurés avant le déploiement du modèle.

Tableau 22. Paramètres configurables

Nom du paramètre	Obligatoire	Valeur par défaut	Description
DataPower_hostname	Oui		Nom d'hôte du dispositif DataPower dans lequel le modèle d'application doit être installé.
DataPower_XML_mgmt_port	Oui	5550	Numéro de port utilisé pour l'interface de gestion XML de DataPower, généralement 5550.
Datapower_admin_id	Oui		ID utilisateur de l'administrateur disposant des droits appropriés pour utiliser l'interface de gestion XML.
DataPower_admin_password	Oui		Mot de passe pour DataPower_admin_id.
Confirmation du mot de passe	Oui		Vérifie l'entrée de l'utilisateur pour DataPower_admin_password.
New_DataPower_domain	Oui		Nouveau nom de domaine à créer pour le dispositif DataPower. Il ne doit pas correspondre à un domaine existant sinon le package de script va échouer ou quitter. La valeur ne peut pas contenir d'espace.

Tableau 22. Paramètres configurables (suite)

Nom du paramètre	Obligatoire	Valeur par défaut	Description
Remove_security_files	Oui	true	Détermine si le fichier `DomainZipFile.zip` et le certificat WSRR téléchargé vers DataPower sont supprimés de l'instance WSRR dans laquelle les packages de script sont exécutés. S'il n'est pas supprimé, ce fichier représente un risque pour la sécurité au cas où les certificats seraient maintenus sur l'instance.

Script : SOA Policy Gateway 2.0.0.0 - Promotion

Le script Promotion permet à un modèle SOA Policy Gateway Basic Runtime ou SOA Policy Gateway Advanced Runtime 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 le maître de gouvernance.

Paramètres

Tableau 23. Paramètres configurables

Nom du paramètre	Description
WSRR_GOV_DMGR_hostname	Nom d'hôte de Dmgr pour le cluster WSRR.
WSRR_GOV_DMGR_cellname	Nom de cellule WebSphere pour le cluster WSRR.
WSRR_GOV_admin_user	ID administrateur pour la cellule de gouvernance de WebSphere WSRR.
WSRR_GOV_admin_password	Mot de passe de l'ID administrateur pour la cellule de gouvernance de WebSphere WSRR.
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, issu du maître de gouvernance Governance Master et utilisé 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.

SOA Policy Gateway 2.0.0.0 - Paramètres de configuration du script Promotion pour le modèle SOA Policy Gateway Basic Runtime

Les paramètres obligatoires sans valeur par défaut doivent être configurés avant le déploiement du modèle.

Tableau 24. Paramètres configurables

Nom du paramètre	Obligatoire	Valeur par défaut	Description
WSRR_GOV_DMGR_hostname	Oui		Nom d'hôte de Dmgr pour le cluster WSRR.
WSRR_GOV_DMGR_cellname	Oui		Nom de cellule WebSphere pour le cluster WSRR.

Tableau 24. Paramètres configurables (suite)

Nom du paramètre	Obligatoire	Valeur par défaut	Description
WSRR_GOV_admin_user	Oui		ID administrateur pour la cellule de gouvernance de WebSphere WSRR.
WSRR_GOV_admin_password	Oui		Mot de passe de l'ID administrateur pour la cellule de gouvernance de WebSphere WSRR.
Confirmation du mot de passe	Oui		Vérifie l'entrée de l'utilisateur pour WSRR_GOV_admin_password.
Promotion_environment	Oui		Doit avoir la valeur staging, production ou Unset. Ces valeurs sont sensibles à la casse et doivent correspondre parfaitement.
LTPA_key_password	Oui		Une clé LTPA est exportée et utilisée au cours de l'exécution du package de script, issu du maître de gouvernance Governance Master et utilisé 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	Oui		Vérifie l'entrée de l'utilisateur pour LTPA_key_password.

SOA Policy Gateway 2.0.0.0 - Paramètres de configuration du script Promotion pour le modèle SOA Policy Gateway Advanced Runtime

Les paramètres obligatoires sans valeur par défaut doivent être configurés avant le déploiement du modèle.

Tableau 25. Paramètres configurables

Nom du paramètre	Obligatoire	Valeur par défaut	Description
WSRR_GOV_DMGR_hostname	Oui		Nom d'hôte de Dmgr pour le cluster WSRR.
WSRR_GOV_DMGR_cellname	Oui		Nom de cellule WebSphere pour le cluster WSRR.
WSRR_GOV_admin_user	Oui		ID administrateur pour la cellule de gouvernance de WebSphere WSRR.
WSRR_GOV_admin_password	Oui		Mot de passe de l'ID administrateur pour la cellule de gouvernance de WebSphere WSRR.
Confirmation du mot de passe	Oui		Vérifie l'entrée de l'utilisateur pour WSRR_GOV_admin_password.

Tableau 25. Paramètres configurables (suite)

Nom du paramètre	Obligatoire	Valeur par défaut	Description
Promotion_environment	Oui		Doit avoir la valeur staging, production ou Unset. Ces valeurs sont sensibles à la casse et doivent correspondre parfaitement.
LTPA_key_password	Oui		Une clé LTPA est exportée et utilisée au cours de l'exécution du package de script, issu du maître de gouvernance Governance Master et utilisé 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	Oui		Vérifie l'entrée de l'utilisateur pour LTPA_key_password.

Script : SOA Policy Gateway 2.0.0.0 - Sample

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

Paramètres

Remarque : Tout paramètre qui nécessite la valeur Unset est sensible à la casse.

Tableau 26. Paramètres configurables

Nom du paramètre	Description
SCP_host	Nom d'hôte du serveur SCP contenant le fichier `DomainZipFile.zip`.
SCP_user	Nom d'utilisateur à utiliser pour la connexion au serveur SCP.
SCP_password	Mot de passe à utiliser pour ouvrir une session sur le serveur SCP.
Confirmation du mot de passe	Vérifie l'entrée de l'utilisateur pour SCP_password.
SCP_zip_location	Emplacement de l'identificateur URI du fichier `DomainZipFile.zip`. Par exemple, `/files/DomainZipFile.zip`.
CLIENT_PUBLIC_KEY_file	Nom du fichier de certificats PEM utilisé pour la connexion au port de l'interface de gestion XML du dispositif DataPower. Utilisez la valeur «Unset» pour une authentification de serveur uniquement et pour ne pas utiliser SSL.
CLIENT_PUBLIC _KEY_password	Mot de passe pour le certificat public utilisé pour se connecter au port de l'interface de gestion XML des dispositifs DataPower. La valeur est «Unset» si aucun mot de passe n'est utilisé.
Confirmation du mot de passe	Vérifie l'entrée de l'utilisateur pour CLIENT_PUBLIC_KEY_password.

Tableau 26. Paramètres configurables (suite)

Nom du paramètre	Description
CLIENT_PRIVATE_KEY_file	Nom du fichier de clé PEM utilisé pour la connexion au port de l'interface de gestion XML du dispositif DataPower. Ceci est obligatoire pour une authentification mutuelle. Utilisez la valeur «Unset» pour une authentification de serveur uniquement et pour ne pas utiliser SSL.
CLIENT_PRIVATE_KEY_password	Mot de passe pour le fichier de clé utilisé pour la connexion au port de l'interface de gestion XML du dispositif DataPower. Ceci est obligatoire pour une authentification mutuelle. La valeur est «Unset» si aucun mot de passe n'est utilisé.
Confirmation du mot de passe	Vérifie l'entrée de l'utilisateur pour CLIENT_PRIVATE_KEY_password.
CLI_FILE_file	Nom du fichier d'interface CLI contenu dans le fichier `DomainZipFile.zip`. Cette interface CLI est exécutée à l'issue de l'installation du domaine et de la configuration du serveur WSRR.
Confirmation du mot de passe	Vérifie l'entrée utilisateur pour LTPA_KEY_password.
DataPower_hostname	Nom d'hôte du dispositif DataPower dans lequel le modèle d'application doit être installé.
DataPower_XML_mgmt_port	Port utilisé pour l'interface de gestion XML DataPower.
DataPower_admin_id	ID utilisateur de l'administrateur disposant des droits appropriés pour utiliser l'interface de gestion XML.
DataPower_admin_password	Mot de passe pour DataPower_admin_id.
Confirmation du mot de passe	Vérifie l'entrée de l'utilisateur pour DataPower_admin_password.
SOAPolicySample_DataPower_domain	Exemple de nom de domaine. Il ne doit pas correspondre à un domaine existant du dispositif DataPower.
SamplePolicySample_starting_port	L'application nécessite 5 ports libres qui seront utilisés en séquence à partir de cette valeur. Par exemple, si la valeur est 62000, les ports 62000-62004 seront utilisés. Aucune vérification n'est effectuée puisque si les ports sont libres par le script.
LDAP_hostname	L'exemple utilise un serveur LDAP ; il s'agit du nom d'hôte de ce serveur.
LDAP_port	Port non sécurisé du serveur LDAP. Généralement 389.
LDAP_password	Mot de passe utilisé lors de la liaison avec LDAP_DN.
Confirmation du mot de passe	Vérifie l'entrée de l'utilisateur pour LDAP_password.
LDAP_DN	Nom distinctif utilisé pour la liaison à LDAP. Par exemple, cn=root,dc=ibm.com.

SOA Policy Gateway 2.0.0.0 - Paramètres de configuration du script Sample pour le modèle Exemple SOA Policy Gateway Basic Runtime

Les paramètres obligatoires sans valeur par défaut doivent être configurés avant le déploiement du modèle.

Remarque : Tout paramètre qui nécessite la valeur Unset est sensible à la casse.

Tableau 27. Paramètres configurables

Nom du paramètre	Obligatoire	Valeur par défaut	Description
SCP_host	Oui		Nom d'hôte du serveur SCP contenant le fichier `DomainZipFile.zip`.
SCP_user	Oui		Nom d'utilisateur à utiliser pour la connexion au serveur SCP.
SCP_password	Oui		Mot de passe à utiliser pour ouvrir une session sur le serveur SCP.
Confirmation du mot de passe	Oui		Vérifie l'entrée de l'utilisateur pour SCP_password.
SCP_zip_location	Oui		Emplacement de l'identificateur URI du fichier `DomainZipFile.zip`. Par exemple, `/files/DomainZipFile.zip`.
CLIENT_PUBLIC_KEY_file	Oui		Nom du fichier de certificats PEM utilisé pour la connexion au port de l'interface de gestion XML du dispositif DataPower. Utilisez la valeur «Unset» pour une authentification de serveur uniquement et pour ne pas utiliser SSL.
CLIENT_PUBLIC _KEY_password	Oui		Mot de passe pour le certificat public utilisé pour se connecter au port de l'interface de gestion XML des dispositifs DataPower. La valeur est «Unset» si aucun mot de passe n'est utilisé.
Confirmation du mot de passe	Oui		Vérifie l'entrée de l'utilisateur pour CLIENT_PUBLIC_KEY_password.
CLIENT_PRIVATE_KEY_file	Oui		Nom du fichier de clé PEM utilisé pour la connexion au port de l'interface de gestion XML du dispositif DataPower. Ceci est obligatoire pour une authentification mutuelle. Utilisez la valeur «Unset» pour une authentification de serveur uniquement et pour ne pas utiliser SSL.
CLIENT_PRIVATE_KEY_password	Oui		Mot de passe pour le fichier de clé utilisé pour la connexion au port de l'interface de gestion XML du dispositif DataPower. Ceci est obligatoire pour une authentification mutuelle. La valeur est «Unset» si aucun mot de passe n'est utilisé.
Confirmation du mot de passe	Oui		Vérifie l'entrée de l'utilisateur pour CLIENT_PRIVATE_KEY_password.

Tableau 27. Paramètres configurables (suite)

Nom du paramètre	Obligatoire	Valeur par défaut	Description
DataPower_hostname	Oui		Nom d'hôte du dispositif DataPower dans lequel le modèle d'application doit être installé.
DataPower_XML_mgmt_port	Oui	5550	Port utilisé pour l'interface de gestion XML DataPower.
DataPower_admin_id	Oui		ID utilisateur de l'administrateur disposant des droits appropriés pour utiliser l'interface de gestion XML.
DataPower_admin_password	Oui		Mot de passe pour DataPower_admin_id.
Confirmation du mot de passe	Oui		Vérifie l'entrée de l'utilisateur pour DataPower_admin_password.
SOAPolicySample_DataPower_domain	Oui	SOAPolicySample	Exemple de nom de domaine. Il ne doit pas correspondre à un domaine existant du dispositif DataPower.
SOAPolicySample_starting_port	Oui	62001	L'application nécessite 5 ports libres qui seront utilisés en séquence à partir de cette valeur. Par exemple, si la valeur est 62000, les ports 62000-62004 seront utilisés. Aucune vérification n'est effectuée puisque si les ports sont libres par le script.
LDAP_hostname	Oui		L'exemple utilise un serveur LDAP ; il s'agit du nom d'hôte de ce serveur.
LDAP_port	Oui	389	Port non sécurisé du serveur LDAP. Généralement 389.
LDAP_password	Oui		Mot de passe utilisé lors de la liaison avec LDAP_DN.
Confirmation du mot de passe	Oui		Vérifie l'entrée de l'utilisateur pour LDAP_password.
LDAP_DN	Oui		Nom distinctif utilisé pour la liaison à LDAP. Par exemple, cn=root,dc=ibm.com.

Script : SOA Policy Gateway 2.0.0.0 - Security

Le script Security copie les informations de sécurité, contenues dans un fichier ZIP, qui sont nécessaires pour communiquer avec un dispositif DataPower sur la machine Dmgr ou WSRR à partir d'un serveur de fichiers externe qui prend en charge le programme de copie sécurisée (SCP) de Linux.

Le fichier de sécurité copié contient les éléments suivants :

- Certificat d'accès DPC
- Certificat public d'accès DPC
- Clé privée DPC

- Script d'interface CLI DP
- Dossier de chaîne de certificats

Le script d'interface de ligne de commande (CLI) pour DataPower vous permet de configurer un domaine déployé durant la phase de déploiement du modèle.

Remarque : Il convient de supprimer les certificats de sécurité confidentiels du serveur de fichiers externe à l'issue du déploiement.

Paramètres

Tableau 28. Paramètres configurables

Nom du paramètre	Description
SCP_host	Nom d'hôte du serveur SCP contenant le fichier `DomainZipFile.zip`.
SCP_user	Nom d'utilisateur à utiliser pour la connexion au serveur SCP.
SCP_password	Mot de passe à utiliser pour ouvrir une session sur le serveur SCP.
Confirmation du mot de passe	Vérifie l'entrée de l'utilisateur pour SCP_password.
SCP_zip_location	Emplacement de l'identificateur URI du fichier `DomainZipFile.zip` ; par exemple, `/files/DomainZipFile.zip`.
CLIENT_PUBLIC_KEY_file	Nom du fichier certificat de PEM utilisé pour la connexion au port de l'interface de gestion XML du dispositif DataPower.
CLIENT_PUBLIC_KEY_password	Mot de passe pour le certificat client utilisé pour la connexion au port de l'interface de gestion XML du dispositif DataPower. Ceci est obligatoire, si disponible, pour l'authentification mutuelle. Cette valeur peut être «Unset» si aucun mot de passe n'est utilisé.
CLIENT_PRIVATE_KEY_file	Nom du fichier de clé PEM utilisé pour la connexion au port de l'interface de gestion XML du dispositif DataPower. Ceci est obligatoire pour une authentification mutuelle.
CLIENT_PRIVATE_KEY_password	Mot de passe pour le fichier de clé utilisé pour la connexion au port de l'interface de gestion XML du dispositif DataPower. Ceci est obligatoire pour une authentification mutuelle. Cette valeur peut être «Unset» si aucun mot de passe n'est utilisé.
CLI_file	Nom du fichier d'interface CLI contenu dans le fichier `DomainZipFile.zip`. Cette interface CLI est exécutée à l'issue de l'installation du domaine et de la configuration du serveur WSRR.

SOA Policy Gateway 2.0.0.0 - Paramètres de configuration du script Secruity pour le modèle SOA Policy Gateway Basic Runtime

Les paramètres obligatoires sans valeur par défaut doivent être configurés avant le déploiement du modèle.

Tableau 29. Paramètres configurables

Nom du paramètre	Obligatoire	Valeur par défaut	Description
SCP_host	Oui		Nom d'hôte du serveur SCP contenant le fichier `DomainZipFile.zip`.
SCP_user	Oui		Nom d'utilisateur à utiliser pour la connexion au serveur SCP.
SCP_password	Oui		Mot de passe à utiliser pour ouvrir une session sur le serveur SCP.

Tableau 29. Paramètres configurables (suite)

Nom du paramètre	Obligatoire	Valeur par défaut	Description
Confirmation du mot de passe	Oui		Vérifie l'entrée de l'utilisateur pour SCP_password.
SCP_zip_location	Oui		Emplacement de l'identificateur URI du fichier `DomainZipFile.zip` ; par exemple, `/files/DomainZipFile.zip`.
CLIENT_PUBLIC_KEY_file	Oui		Nom du fichier certificat de PEM utilisé pour la connexion au port de l'interface de gestion XML du dispositif DataPower.
CLIENT_PUBLIC_KEY_password	Oui		Mot de passe pour le certificat client utilisé pour la connexion au port de l'interface de gestion XML du dispositif DataPower. Ceci est obligatoire, si disponible, pour l'authentification mutuelle. Cette valeur peut être «Unset» si aucun mot de passe n'est utilisé.
CLIENT_PRIVATE_KEY_file	Oui		Nom du fichier de clé PEM utilisé pour la connexion au port de l'interface de gestion XML du dispositif DataPower. Ceci est obligatoire pour une authentification mutuelle.
CLIENT_PRIVATE_KEY_password	Oui		Mot de passe pour le fichier de clé utilisé pour la connexion au port de l'interface de gestion XML du dispositif DataPower. Ceci est obligatoire pour une authentification mutuelle. Cette valeur peut être «Unset» si aucun mot de passe n'est utilisé.
CLI_file	Oui	Unset	Nom du fichier d'interface CLI contenu dans le fichier `DomainZipFile.zip`. Cette interface CLI est exécutée à l'issue de l'installation du domaine et de la configuration du serveur WSRR.

SOA Policy Gateway 2.0.0.0 - Paramètres de configuration du script Security pour le modèle SOA Policy Gateway Advanced Runtime

Les paramètres obligatoires sans valeur par défaut doivent être configurés avant le déploiement du modèle.

Tableau 30. Paramètres configurables

Nom du paramètre	Obligatoire	Valeur par défaut	Description
SCP_zip_location	Oui		Emplacement de l'identificateur URI du fichier `DomainZipFile.zip` ; par exemple, `/files/DomainZipFile.zip`.

Tableau 30. Paramètres configurables (suite)

Nom du paramètre	Obligatoire	Valeur par défaut	Description
SCP_host	Oui		Nom d'hôte du serveur SCP contenant le fichier `DomainZipFile.zip`.
SCP_user	Oui		Nom d'utilisateur à utiliser pour la connexion au serveur SCP.
SCP_password	Oui		Mot de passe à utiliser pour ouvrir une session sur le serveur SCP.
Confirmation du mot de passe	Oui		Vérifie l'entrée de l'utilisateur pour SCP_password.
CLIENT_PUBLIC_KEY_file	Oui		Nom du fichier certificat de PEM utilisé pour la connexion au port de l'interface de gestion XML du dispositif DataPower.
CLIENT_PUBLIC_KEY_password	Oui		Mot de passe pour le certificat client utilisé pour la connexion au port de l'interface de gestion XML du dispositif DataPower. Ceci est obligatoire, si disponible, pour l'authentification mutuelle. Cette valeur peut être «Unset» si aucun mot de passe n'est utilisé.
CLIENT_PRIVATE_KEY_file	Oui		Nom du fichier de clé PEM utilisé pour la connexion au port de l'interface de gestion XML du dispositif DataPower. Ceci est obligatoire pour une authentification mutuelle.
CLIENT_PRIVATE_KEY_password	Oui		Mot de passe pour le fichier de clé utilisé pour la connexion au port de l'interface de gestion XML du dispositif DataPower. Ceci est obligatoire pour une authentification mutuelle. Cette valeur peut être «Unset» si aucun mot de passe n'est utilisé.
CLI_file	Oui	Unset	Nom du fichier d'interface CLI contenu dans le fichier `DomainZipFile.zip`. Cette interface CLI est exécutée à l'issue de l'installation du domaine et de la configuration du serveur WSRR.

Chapitre 5. Utilisation du IBM SOA Policy Gateway Pattern

IBM SOA Policy Gateway Pattern fournit une définition de modèle pour un déploiement reproductible de la topologie qui constitue le produit. Chaque modèle fournit une fonction spécifique dans IBM SOA Policy Gateway Pattern et contient plusieurs images permettant de prendre en charge chaque modèle. Les modèles doivent être configurés avant un déploiement selon les besoins métier.

Dans le cadre du processus de déploiement, configurez les paramètres de l'élément. Pour plus d'informations, voir «Déploiement des modèles», à la page 68.

Tâches associées:

Chapitre 3, «Guide d'initiation à IBM SOA Policy Gateway Pattern», à la page 11
Ce modèle utilise WebSphere DataPower pour contrôler des messages utilisant des règles gouvernées et des définitions de service dans WSRR. Les rubriques de cette section vont vous aider de mieux comprendre ce qui est couvert par ce scénario, les raisons qui pousseront une entreprise à vouloir suivre ce scénario, les rôles utilisateur impliqués et une présentation de la fonction fournie avec le produit.

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. Déterminez quelles sont les exigences et ressources de gouvernance requises.

Pour déployer votre environnement, préparez le dispositif DataPower pour une administration à distance et pour collecter les actifs requis permettant de communiquer en toute sécurité avec le dispositif. Vous pouvez tester l'environnement en déployant le modèle Exemple SOA Policy Gateway Basic Runtime. Ceci permet de confirmer que l'environnement est correctement configuré pour un déploiement et de présenter la mise en application des règles. Après la validation de l'environnement, la configuration souhaitée de gouvernance et d'exécution du modèle IBM SOA Policy Gateway Pattern est déterminée en se fondant sur les meilleure pratique de WSRR. Le déploiement du modèle démarre avec Governance Master, suivi par les modèles Runtime correspondant à la configuration souhaitée.

Préparation et déploiement du modèle IBM SOA Policy Gateway Pattern

Préparation de DataPower et collecte des fichiers de sécurité :

1. Préparez le dispositif DataPower pour une administration à distance. Pour plus d'informations, voir «Configuration de DataPower pour les modèles IBM SOA Policy Gateway Pattern», à la page 59.
2. Si le dispositif DataPower est sécurisé, lisez la section relative à la sécurité de DataPower, puis collectez les fichiers de sécurité DataPower nécessaires pour communiquer avec lui.
3. Confirmez qu'un système DataPower de l'environnement de cloud peut communiquer avec le dispositif et que ce dernier peut communiquer avec un système déployé.

Vous pouvez utiliser le modèle Exemple SOA Policy Gateway Basic Runtime pour montrer les fonctions du modèle avant de créer un déploiement de production. S'il est nécessaire d'utiliser Basic Runtime Sample, procédez comme suit :

1. Fournissez un serveur SCP sous Linux accessible à partir d'un système déployé au sein du cloud. SCP est la commande de copie sécurisée. Le serveur SCP offre un moyen d'héberger les fichiers de sécurité externes au modèle pour qu'il ne soit pas nécessaire d'avoir à modifier le modèle pour chaque configuration de sécurité.
2. Fournissez un serveur LDAP destiné à héberger les ID de sécurité utilisés par le modèle d'application implémenté dans DataPower. Pour plus d'informations, voir «Configuration de LDAP pour l'exemple», à la page 66.
3. Déployez le modèle Exemple SOA Policy Gateway Basic Runtime pour valider l'infrastructure. Pour plus d'informations, voir «Déploiement du modèle Exemple SOA Policy Gateway Basic Runtime», à la page 69.
4. Si vous avez terminé avec l'exemple, le serveur LDAP n'est alors plus nécessaire.

Préparation pour un déploiement en production :

1. Décidez de l'échelle à adopter pour le déploiement. Déterminez les tailles de clusters pour Governance Master et pour les déploiements des environnements d'exécution.

   Remarque : Lorsqu'un cluster est déployé, il n'est pas possible de l'étendre avec un autre membre de cluster.
2. Définissez le nom de cellule et l'ID administrateur et le mot de passe de Governance Master.
3. Hébergez le fichier `DomainZipFile.zip` de sécurité de DataPower sur un serveur SCP. Pour plus d'informations, voir «Création de la sécurité `DomainZipFile.zip`», à la page 60.

Déployez Governance Master pour l'environnement de production :

1. Déployez un modèle SOA Policy Gateway Governance Master. Attendez que le déploiement soit terminé avant de déployer des modèles d'exécution dans un environnement de production. Pour plus d'informations, voir «Déploiement du modèle SOA Policy Gateway Governance Master», à la page 70.

Déployez les modèles d'exécution dans l'environnement de production.

1. Décidez si un environnement en cluster ou autonome est nécessaire.
2. Si plusieurs domaines DataPower sont nécessaires, clonez le modèle Basic Runtime ou Advanced Runtime, et ajoutez les packages de script DataPower au clone pour chaque domaine requis.

   Remarque : Une fois cette configuration terminée, il ne sera plus possible d'ajouter des domaines DataPower supplémentaires.
   Pour plus d'informations, voir «Déploiement avec plusieurs domaines DataPower», à la page 76.
3. Configurez le modèle d'exécution avec les informations du modèle Governance Master. Pour plus d'informations, voir «Informations sur le déploiement de SOA Policy Gateway Governance Master», à la page 71.
4. Décidez si l'environnement d'exécution doit être staging, production ou autre (other).

5. Déployez le modèle Basic Runtime ou Advanced Runtime. Pour plus d'informations, voir «Déploiement du modèle SOA Policy Gateway Advanced Runtime», à la page 72 ou «Déploiement du modèle SOA Policy Gateway Basic Runtime», à la page 71.
6. Attendez que le déploiement complet soit terminé avant de déployer un autre environnement d'exécution.

.

Lorsque le déploiement des environnements d'exécution est terminé :

1. Le serveur de fichier SCP n'est plus nécessaire.
2. WSRR et la sécurité WebSphere peuvent être mis à jour à partir de la configuration de sécurité par défaut. Pour plus d'informations, voir «Gestion de la sécurité», à la page 60.
3. Le domaine DataPower est maintenant prêt pour une configuration de passerelle.

Configuration de DataPower pour les modèles IBM SOA Policy Gateway Pattern

Exécutez les étapes suivantes de configuration de DataPower avant d'exécuter 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 indique actif.
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

Les clients nécessitent différents niveaux de sécurité entre WSRR et DataPower, notamment dans le domaine du protocole SSL. Le modèle IBM SOA Policy Gateway Pattern prend en charge 3 niveaux de communication SSL entre les scripts de configuration et DataPower lors de l'utilisation des modèles SOA Policy Gateway Basic Runtime, Exemple SOA Policy Gateway Basic Runtime et SOA Policy Gateway Advanced Runtime.

Si SSL n'est pas obligatoire

Si vous n'avez pas besoin d'utiliser SSL, la clé publique et les clés privées pour le client curl ne sont pas fournies et laissées à la valeur «Unset».

Remarque : Si aucune couche SSL n'est utilisée, aucune des données envoyées à DataPower n'est chiffrée, y compris les informations d'utilisateur et de mot de passe. Ceci présente une vulnérabilité en matière de sécurité. Les mots de passe utilisés dans des apples SOMA à DataPower ne prennent pas en charge le chiffrement et sont par conséquent transportés vers le dispositif DataPower en mode non chiffé. En conséquence, une authentification côté serveur constitue un minimum pour assurer une sécurité.

Authentification mutuelle entre les applications DataPower et les scripts des modèles Basic (modèle de base) et Advanced (modèle avancé).

Si vous voulez que l'authentification mutuelle s'effectue entre les applications DataPower et les scripts dans les modèles Basic et Advanced :

- La clé publique et les clés privées pour le client curl doivent être fournies.

Gestion 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 véritable environnement de sécurité, vous devez les sécuriser avec des techniques de sécurité WebSphere normalisées.

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

Création de la sécurité `DomainZipFile.zip`

Créez le fichier de sécurité `DomainZipFile.zip` pour le modèle SOA Policy Gateway Basic Runtime, le modèle SOA Policy Gateway Advanced Runtime et Exemple SOA Policy Gateway Basic Runtime.

Procédure

Créez le fichier `DomainZipFile.zip` à l'aide des règles suivantes :

1. La structure du fichier `DomainZipFile.zip` doit être comme suit :

   Remarque : Seule la structure de répertoires est nécessaire, les noms de fichier individuels peuvent suivre la désignation de votre choix. Notez cependant que tous les fichiers de certificats et de clés doivent être au format PEM.

   Remarque : L'utilisation du nom d'hôte de DataPower dans le chemin permet à différents certificats d'être utilisés pour différents dispositifs DataPower.

Tableau 31. Fichiers requis pour les modèles Basic et Advanced

Nom de fichier, emplacement relatif au répertoire root	Remarques
`CurlClientPublicKeyFile.crt`	Requis uniquement en cas d'utilisation d'une authentification mutuelle (Mutual Authentication). Format PEM uniquement.
`CurlClientPrivateKeyFile.key`	Requis uniquement en cas d'utilisation d'une authentification mutuelle (Mutual Authentication).
`/dataPowerHostName/certificate1.crt`	Les certificats DataPower à télécharger sur WSRR. Cela nécessite que le format de la chaîne de certificats complète soit PEM. Certificats DataPower à télécharger dans WSRR. Il doit inclure le contenu suivant uniquement : `------BEGINCERTIFICATE---- to -----END CERTIFICATE-----` L'extension de fichier doit être `.crt` ou `.pem`.
`/dataPowerHostName/certificate2.crt`	L'extension de fichier doit être `.crt` ou `.pem`.
`/dataPowerHostName/certificate3.crt`	L'extension de fichier doit être `.crt` ou `.pem`.

2. Pour le modèle SOA Policy Gateway Advanced Runtime uniquement, ajoutez le fichier `cli` à exécuter (facultatif) :

Tableau 32. Fichiers supplémentaires requis pour le modèle Advanced

Nom de fichier, emplacement relatif au répertoire root	Remarques
`/cli.cli`	Fichier CLI unique qui doit être exécuté à l'issue de la configuration du domaine DataPower.

3. Placez `DomainZipFile.zip` à l'emplacement de votre serveur SCP. En raison de la nature confidentielle de ces fichiers, nous recommandons de les supprimer après la configuration. Les scripts de configuration de modèles supprimeront tous les fichiers extraits du fichier `DomainZipFile.zip` ainsi que la copie du fichier `DomainZipFile.zip` qui est créé à l'aide de SCP à partir de votre environnement SCP.
4. Notez les informations du serveur SCP suivantes :
   - Le nom d'hôte SCP (point de contrôle de service)
   - Le chemin d'accès SCP au fichier `DomainZipFile.zip`
   - L'utilisateur et le mot de passe SCP

Utilisation du fichier `DomainZipFile`

Cas d'utilisation du fichier `DomainZipFile` pour différents niveaux de sécurité dans des modèles.

Le fichier `DomainZipFile.zip` peut s'utiliser dans les modèles Basic Runtime, Basic Runtime Sample et Advanced Runtime.

Il n'est pas nécessaire d'utiliser une couche SSL pour connecter les packages de script de modèles au dispositif DataPower. Si vous n'utilisez pas SSL, vous n'avez pas besoin de créer de fichier `DomainZipFile.zip`, sauf si un script d'interface CLI est nécessaire pour personnaliser le domaine DataPower créé par le modèle. Dans ce cas, si vous n'utilisez pas au minimum une authentification de serveur, les données ne seront pas chiffrées. Il s'agit d'un risque de sécurité car les informations des utilisateurs et de mots de passe sont transmises à DataPower au cours du scriptage du client sur une connexion http, et cette opération est protégée par les certificats du fichier `DomainZipFile.zip`.

Si l'hôte DataPower n'est pas configuré pour valider le certificat du client, vous n'avez pas à utiliser d'authentification mutuelle entre le client de script et le dispositif DataPower. Nous recommandons d'utiliser au minimum une authentification de serveur.

Les scénarios de cas d'utilisation de cette rubrique décrivent différents niveaux de sécurité.

Le produit prend en charge les scénarios suivants :

Cas n°1 : aucune couche SSL n'est requise

Cas n°2 : aucune couche SSL n'est requise, mais un script d'interface CLI est nécessaire pour personnaliser le domaine

Cas n°3 : une authentification de serveur du certificat de DataPower Certificate par le client de script est obligatoire

Cas n°4 : une authentification mutuelle avec le dispositif DataPower est obligatoire

Cas n°1 : aucune couche SSL n'est requise

Pour des raisons de sécurité déjà mentionnées, nous recommandons de n'utiliser cette option que pour des scénarios de développement. Si vous ne souhaitez pas utiliser de couche Secure Sockets Layer (SSL), procédez comme suit :

1. Définissez les paramètres pour SCP_host à «Unset». Si vous utilisez les modèles Basic Runtime ou Advanced Runtime, SCP_host est dans le script de package SOA Policy Gateway 2.0.0.0 - Security. Si vous utilisez le modèle Basic Runtime Sample, SCP_host est dans le script SOA Policy Gateway 2.0.0.0. Ceci définit le script dans le modèle pour qu'il ne récupère pas le fichier `DomainZipFile.zip` à l'aide de SCP.
2. Définissez les paramètres suivants à «Unset» dans les mêmes packages de script à partir de l'étape 1 :
   - CLIENT_PUBLIC_KEY_file
   - CLIENT_PUBLIC_KEY_password
   - Confirmation du mot de passe
   - CLIENT_PRIVATE_KEY_file
   - CLIENT_PRIVATE_KEY_password
   - Confirmation du mot de passe

Cas n°2 : aucune couche SSL n'est requise, mais un script d'interface CLI est nécessaire pour personnaliser le domaine

Pour des raisons de sécurité déjà mentionnées, nous recommandons de n'utiliser cette option que pour des scénarios de développement. Vous ne souhaitez pas utiliser SSL, mais un script d'interface CLI est nécessaire :

1. Définissez les paramètres pour SCP_host à «Unset». Si vous utilisez les modèles Basic Runtime ou Advanced Runtime, SCP_host est dans le script de package SOA Policy Gateway 2.0.0.0 - Security. Si vous utilisez le modèle Basic Runtime Sample, SCP_host est dans le script SOA Policy Gateway 2.0.0.0. Ceci définit le script dans le modèle pour qu'il ne récupère pas le fichier `DomainZipFile.zip` à l'aide de SCP.
2. Définissez les paramètres suivants à Unset dans les mêmes packages de script à partir de l'étape 1 :
   - CLIENT_PUBLIC_KEY_file

- CLIENT_PUBLIC_KEY_password
- Confirmation du mot de passe
- CLIENT_PRIVATE_KEY_file
- CLIENT_PRIVATE_KEY_password
- Confirmation du mot de passe

Remarque : Si SCP_host est défini à «Unset», vous n'avez pas besoin de fichier `DomainZipFile.zip`, sauf si vous avez un script d'interface CLI à exécuter dans les modèles Basic Runtime et Advanced Runtime.

3. Mettez le fichier du script d'interface CLI que vous souhaitez utiliser dans la racine du fichier `DomainZipFile.zip`. Voici un exemple de structure du fichier `DomainZipFile.zip` :

   ```
   /cli.cli
   ```

   Ce fichier est exécuté à la fin du package de script de DataPower Domain. `cli.cli` est un exemple de nom de fichier. Le nom de fichier ne doit contenir aucun espace.

Cas n°3 : une authentification de serveur du certificat de DataPower Certificate par le client de script est obligatoire

Vous devez fournir tous les certificats de la chaîne DataPower Certificate qui protègent l'interface de gestion XML (XML Management Interface). Pour les localiser, procédez comme suit :

1. Examinez le profil de proxy SSL pour l'interface XML Management et localisez le profil CryptoProfile. Crypto Profile doit contenir les données d'identification qui détiennent les certificats utilisés pour protéger l'interface XML Management.
2. Ajoutez ces certificats au fichier `DomainZipFile.zip`.

   Le format est :

   - dataPowerHostName/certificateChainMember1.crt
   - dataPowerHostName/certificateChainMember2.pem
   - dataPowerHostName/certificateChainMember(n).crt

   Si vous utilisez le scénario multi-domaine, le fichier peut avoir deux répertoires `dataPowerHostName` différents avec les fichiers suivants pour chacune des chaînes de certificats DataPower Certificate :

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

   Remarque : Le fichier des chaînes de certificats de DataPower Certificate doit être du type `.crt` ou `.pem` et ne doit contenir que le certificat proprement dit. Les noms de fichier `.crt` ou `.pem` utilisés ici sont des exemples. Le nom de fichier ne doit contenir aucun espace.
3. Facultatif : si seulement une authentification de serveur suffit pour le script de package Authentication for the SOA Policy Gateway 2.0.0.0 - Security utilisé par les modèles Basic Runtime et Advanced Runtime, ou le script SOA Policy

Gateway 2.0.0.0 - Sample dans le modèle Basic Runtime Sample, utilisez «Unset» comme valeur pour les paramètres suivants de ces scripts:

- CLIENT_PUBLIC_KEY_file
- CLIENT_PUBLIC_KEY_password
- Confirmation du mot de passe
- CLIENT_PRIVATE_KEY_file
- CLIENT_PRIVATE_KEY_password
- Confirmation du mot de passe

4. Facultatif : si un script d'interface CLI est obligatoire :

   Mettez le fichier du script d'interface CLI que vous souhaitez utiliser dans la racine du fichier `DomainZipFile.zip`. Voici un exemple de structure du fichier `DomainZipFile.zip` :

   ```
   /cli.cli
   ```

   Ce fichier est exécuté à la fin du package de script de DataPower Domain. `cli.cli` est un exemple de nom de fichier. Le nom de fichier ne doit contenir aucun espace.

Cas n°4 : une authentification mutuelle avec le dispositif DataPower est obligatoire

Dans ce cas, le client et le serveur DataPower nécessitent la validation des autres certificats. Ceci est uniquement nécessaire si l'hôte DataPower Host est configuré dans le profil de proxy SSL pour l'interface de gestion XML (XML Management Interface) afin de valider les certificats des clients.

1. Ajoutez ces certificat au fichier `DomainZipFile.zip`.

   Le format est :

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

   Remarque : Le fichier des chaînes de certificats de DataPower Certificate doit être du type `.crt` ou `.pem` et ne doit contenir que le certificat proprement dit. Les noms de fichier `.crt` ou `.pem` utilisés ici sont des exemples. Le nom de fichier ne doit contenir aucun espace.

   Le certificat client et le fichier de clés client peuvent contenir les données du certificat ou du fichier de clés avant la ligne du fichier qui contient : `-----BEGIN CERTIFICATE-----`.

2. Facultatif : si une authentification de serveur suffit pour le script de package Authentication for the SOA Policy Gateway 2.0.0.0 - Security utilisé par les modèles Basic Runtime et Advanced Runtime, ou le script SOA Policy Gateway 2.0.0.0 - Sample dans le modèle Basic Runtime Sample, utilisez «Unset» comme valeur pour les paramètres suivants de ces scripts:

   - CLIENT_PUBLIC_KEY_file
   - CLIENT_PRIVATE_KEY_file
   - CLIENT_PRIVATE_KEY_password

- Confirmation du mot de passe

3. S'il n'existe pas de mot de passe pour le fichier de clé publique, la valeur du paramètre suivant peut être «Unset» :
   - CLIENT_PUBLIC_KEY_password
   - Confirmation du mot de passe
4. Les commandes curl utilisées par les packages de script supposent que le type de fichier est `.pem`, en conséquence **--key-type** et **--cert-type** sont définis à PEM par défaut. Les fichiers de certificats et de clés peuvent contenir ce contenu avant `-----BEGIN CERTIFICATE-----` dans le fichier de certificats ou de clés particulier.
5. Facultatif : si un script d'interface CLI est requis en utilisant les modèles Basic Runtime ou Advanced Runtime :

   Mettez le fichier du script d'interface CLI que vous souhaitez utiliser dans la racine du fichier `DomainZipFile.zip`. Voici un exemple de structure du fichier `DomainZipFile.zip` :

   ```
   /cli.cli
   ```

   Ce fichier est exécuté à la fin du package de script de DataPower Domain. `cli.cli` est un exemple de nom de fichier. Le nom de fichier ne doit contenir aucun espace.

En sélectionnant un cas, vous avez configuré le niveau de sécurité approprié, en ayant utilisé ou non le fichier `DomainZipFile.zip`.

Les certificats DataPower peuvent être téléchargés dans WSRR

Vous pouvez fournir un répertoire des certificats dans le répertoire `dataPowerHostName` du fichier `DomainZipFile.zip`. Celui-ci peut être téléchargé sur le serveur WSRR Dmgr ou le serveur autonome WSRR.

Fourniture de votre propre mécanisme de téléchargement du fichier `DomainZipFile.zip`

Vous pouvez fournir votre propre fichier `DomainZipFile.zip` sans utiliser le serveur SCP dans le package de script de sécurité.

Procédure

Pour utiliser d'autres moyens pour placer le fichier dans l'environnement, vous devez procéder comme suit :

1. Le paramètre **`SCP_host`** doit être défini à Unset (Désactivé).
2. Vous devez créer un package de script personnalisé pour créer le fichier `DomainZipFile.zip` dans le répertoire `/tmp` avant d'exécuter l'un des scripts de modèle de passerelle SOA (SOA Gateway Pattern).
3. Pour les modèles avancés (Advanced), créez le fichier `DomainZipFile.zip` dans le répertoire `/tmp/security/RetrieveDomainFiles`.
4. Pour les exemples de modèle de base (Basic), créez le fichier `DomainZipFile.zip` dans le répertoire `/installSample/Retrieve_Domain_Files`.

   Remarque : En cas d'absence du `DomainZipFile.zip`, le script peut échouer si les paramètres indiquent que des certificat ou des clés sont utilisés.

Valeurs CN dans des certificats

Les certificats fournis comme partie intégrante du fichier `DomainZipFile.zip` doivent prendre en compte la valeur CN qui figure dans le certificat.

Une vérification du nom d'hôte est toujours active lorsque vous décidez d'utiliser la couche SSL (couche Secure Sockets Layer) ; ainsi, vous devez prendre en compte ce qui suit si le certificat est utilisé dans le module de script :

- Pour des certificats client (clé publique et privée), vous n'avez aucun moyen de connaître l'hôte précis où se trouvera le serveur WSRR ou WSRR Dmgr où s'exécute le script. En conséquence, la valeur CN doit être suffisamment générique pour s'exécuter sur n'importe quel hôte client potentiel de l'environnement IBM Workload Deployer ; par exemple, `*nom_client*.votre_entreprise.com`.
- Les certificats pour les machines DataPower se trouvent dans des répertoires individuels du fichier `DomainZipFile.zip` ; par exemple :

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

- La valeur CN pour le certificat (le certificat final dans la chaîne pour l'hôte DataPower) doit être valide pour ce nom d'hôte ; par exemple, `dp1.votre_entreprise.com` ou `*dp*.votre_entreprise.com`.

Configuration de LDAP pour l'exemple

L'exemple nécessite un protocole LDAP (Lightweight Directory Access Protocol) avec certaines entrées spécifiques.

Pourquoi et quand exécuter cette tâche

Les éléments et propriétés doivent être définis lors de la configuration de LDAP.

Remarque : Ne changez pas ces mots de passe.

Comme alternative aux étapes de configuration manuelle, extrayez le contenu du fichier `.zip` suivant, contenant deux fichiers LDIF détenant les détails de configuration fournis dans cette tâche, puis utilisez ces fichiers pour mettre à jour le serveur LDAP : soaSamples.zip.

Procédure

Créez un LDAP avec les éléments suivants :

1. Définissez le suffixe :

```
dc=ibm.com
```

2. Définissez le domaine `dc=ibm.com` avec les propriétés suivantes :

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

3. Définissez les conteneurs :
   a. Définissez les groupes de conteneur :

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

   b. Définissez les utilisateurs de conteneurs :

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

4. Définissez les utilisateurs suivants :
   a. Utilisateur ConsumerA avec les propriétés suivantes :

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

   b. Utilisateur ConsumerB avec les propriétés suivantes :

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

   c. Utilisateur ConsumerX avec les propriétés suivantes :

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

5. Définissez les groupes suivants :
   a. Définissez le groupe MANAGER avec les propriétés suivantes :

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

   b. Définissez le groupe Clerk avec les propriétés suivantes :

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

   c. Définissez le groupe Customer avec les propriétés suivantes :

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

6. Veillez à collecter les informations suivantes sur LDAP avant d'exécuter l'exemple :
   - Le nom distinctif (DN), par exemple `cn=root`.
   - Le mot de passe, par exemple `passw0rd`.
   - Le port non sécurisé, par exemple 389.
   - Le nom d'hôte LDAP, par exemple `ldap.customer.com`.

Déploiement des modèles

Le déploiement des modèles avec IBM Workload Deployer 3.1.0.2 ou IBM SOA Policy Gateway Pattern dans le cloud fournit un environnement d'exécution à l'environnement IBM PureApplication System. Vous pouvez déployer les modèles prédéfinis disponibles avec les images IBM SOA Policy Gateway Pattern ou déployer des modèles 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.

Pourquoi et quand exécuter cette tâche

Le déploiement d'un modèle crée un système virtuel, ou un nouvel environnement d'exécution IBM SOA Policy Gateway Pattern mis à disposition, qui est exécuté dans le cloud.

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 qui est 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 Workload Deployer : Gestion des modèles de système virtuel

IBM PureApplication System : Gestion des modèles de système virtuel

Déploiement du modèle Exemple SOA Policy Gateway Basic Runtime

Le déploiement du modèle Exemple SOA Policy Gateway Basic Runtime crée une instance de système virtuel d'exécution du modèle.

Avant de commencer

Ces prérequis doivent être satisfaits avant de déployer le modèle :

- Configurez DataPower pour l'exemple, voir «Configuration de DataPower pour les modèles IBM SOA Policy Gateway Pattern», à la page 59.
- Configurez Security pour l'exemple, voir «Sécurité appliquée aux modèles IBM SOA Policy Gateway Pattern», à la page 59.
- Configurez le serveur SCP pour héberger les fichiers de sécurité.
- Configurez LDAP pour l'exemple, voir «Configuration de LDAP pour l'exemple» , à la page 66.

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 Exemple SOA Policy Gateway Basic Runtime, procédez comme suit :

1. Cliquez sur **Canevas** > **Systèmes virtuels**.
2. Dans la liste Modèles de systèmes virtuels, sélectionnez **SOA Policy Gateway 2.0.0.0 - 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. 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 le script :

      Remarque : Tous les mots de passe de ce modèle, à l'exception du paramètre DataPower_admin_id, utilisent le mot de passe par défaut `password`.

      - «Paramètres de configuration du composant DB2 Enterprise pour le modèle Exemple SOA Policy Gateway Basic Runtime», à la page 29.
      - «Paramètres de configuration du composant Serveur automome WSRR pour le modèle Exemple SOA Policy Gateway Basic Runtime», à la page 40

- «SOA Policy Gateway 2.0.0.0 - Paramètres de configuration du script Sample pour le modèle Exemple SOA Policy Gateway Basic Runtime», à la page 51

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

Que faire ensuite

Pour vérifier le déploiement, voir «Vérification du déploiement», à la page 74.

Déploiement du modèle SOA Policy Gateway Governance Master

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

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 Governance Master, procédez comme suit :

1. Cliquez sur **Modèles** > **Systèmes virtuels**.
2. Dans la liste Modèles de systèmes virtuels, sélectionnez **SOA Policy Gateway 2.0.0.0 - Governance Master**.
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. Configurer les modèles virtuels. Cliquez sur **Configurer les composants virtuels**, puis cliquez sur le nom du composant pour ouvrir l'éditeur pour le composant :
      - «Paramètres de configuration du composant principal HADR DB2 Enterprise HADR pour le modèle SOA Policy Gateway Governance Master», à la page 33
      - «Paramètres de configuration du composant gestionnaire de déploiement WSRR pour le modèle SOA Policy Gateway Governance Master», à la page 42
      - «Paramètres de configuration du composant Noeuds personnalisés WSRR pour le modèle SOA Policy Gateway Governance Master», à la page 44
      - «Paramètres de configuration du composant de secours HADR DB2 Enterprise HADR pour le modèle SOA Policy Gateway Governance Master», à la page 37
5. Cliquez sur **OK** pour déployer le modèle.

Que faire ensuite

Pour vérifier le déploiement, voir «Vérification du déploiement», à la page 74.

Informations sur le déploiement de SOA Policy Gateway Governance Master

Vous devez déployer Governance Master avant de déployer les modèles SOA Policy Gateway Basic Runtime ou SOA Policy Gateway Advanced Runtime.

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. Notez les points suivants :
   - 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).

   Remarque : 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 ou SOA Policy Gateway Advanced Runtime :
   - WSRR_GOV_DMGR_hostname
   - WSRR_GOV_DMGR_cellname
   - WSRR_GOV_admin_user
   - WSRR_GOV_admin_password

Déploiement du modèle SOA Policy Gateway Basic Runtime

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

Avant de commencer

Complétez ce qui suit avant de déployer le modèle Basic Runtime :

- Configurez DataPower pour le modèle IBM SOA Policy Gateway Pattern ; voir «Configuration de DataPower pour les modèles IBM SOA Policy Gateway Pattern», à la page 59.
- Configurez la sécurité pour IBM SOA Policy Gateway Pattern ; voir «Sécurité appliquée aux modèles IBM SOA Policy Gateway Pattern», à la page 59.
- Configurez le serveur SCP pour héberger les fichiers de sécurité.
- Récupérez les informations de déploiement de Governance Master ; voir «Informations sur le déploiement de SOA Policy Gateway Governance Master».

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 le modèle SOA Policy Gateway Basic Runtime ou le modèle SOA Policy Gateway Advanced Runtime. La raison en est que cela 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 le modèle SOA Policy Gateway Basic Runtime, procédez comme suit :

1. Cliquez sur **Modèles** > **Systèmes virtuels**.
2. Dans la liste Modèles de systèmes virtuels, sélectionnez **SOA Policy Gateway Basic Runtime 2.0.0.0**.
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. 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 :
      - «Paramètres de configuration du composant DB2 Enterprise pour le modèle SOA Policy Gateway Basic Runtime», à la page 27
      - «Paramètres de configuration du composant Serveur automome WSRR pour le modèle SOA Policy Gateway Basic Runtime», à la page 39
      - «SOA Policy Gateway 2.0.0.0 - Paramètres de configuration du script Secruity pour le modèle SOA Policy Gateway Basic Runtime», à la page 54
      - «SOA Policy Gateway 2.0.0.0 - Paramètres de configuration du script Promotion pour le modèle SOA Policy Gateway Basic Runtime», à la page 48
      - «SOA Policy Gateway 2.0.0.0 - Paramètres de configuration du script DataPower Domain pour le modèle SOA Policy Gateway Basic Runtime», à la page 46
5. Cliquez sur **OK** pour déployer le modèle.

Que faire ensuite

Pour vérifier le déploiement, voir «Vérification du déploiement», à la page 74.

Déploiement du modèle SOA Policy Gateway Advanced Runtime

Le déploiement du modèle SOA Policy Gateway Advanced Runtime crée une instance du système virtuel en cours d'exécution du modèle.

Avant de commencer

Complétez ce qui suit avant de déployer le modèle Advanced Runtime :

- Configurez DataPower pour le modèle IBM SOA Policy Gateway Pattern ; voir «Configuration de DataPower pour les modèles IBM SOA Policy Gateway Pattern», à la page 59.
- Configurez la sécurité pour IBM SOA Policy Gateway Pattern ; voir «Sécurité appliquée aux modèles IBM SOA Policy Gateway Pattern», à la page 59.
- Configurez le serveur SCP pour héberger les fichiers de sécurité.
- Récupérez les informations de déploiement de Governance Master ; voir «Informations sur le déploiement de SOA Policy Gateway Governance Master», à la page 71.

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 le modèle SOA Policy Gateway Basic Runtime ou le modèle SOA Policy Gateway Advanced Runtime. La raison en est que cela 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 le modèle SOA Policy Gateway Advanced Runtime, procédez comme suit :

1. Cliquez sur **Modèles** > **Systèmes virtuels**.
2. Dans la liste Modèles de systèmes virtuels, sélectionnez **SOA Policy Gateway 2.0.0.0 - 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. Facultatif : Choisissez l'environnement et planifiez le déploiement.
   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 :
      - «Paramètres de configuration du composant principal HADR DB2 Enterprise HADR pour le modèle SOA Policy Gateway Advanced Runtime», à la page 31
      - «Paramètres de configuration du composant gestionnaire de déploiement WSRR pour le modèle SOA Policy Gateway Advanced Runtime», à la page 41
      - «SOA Policy Gateway 2.0.0.0 - Paramètres de configuration du script Security pour le modèle SOA Policy Gateway Advanced Runtime», à la page 55

- «SOA Policy Gateway 2.0.0.0 - Paramètres de configuration du script Promotion pour le modèle SOA Policy Gateway Advanced Runtime», à la page 49
- «SOA Policy Gateway 2.0.0.0 - Paramètres de configuration du script DataPower Domain pour le modèle SOA Policy Gateway Advanced Runtime», à la page 47
- «Paramètres de configuration du composant Noeuds personnalisés WSRR pour le modèle SOA Policy Gateway Advanced Runtime», à la page 43
- «Paramètres de configuration du composant de secours HADR DB2 Enterprise HADR pour le modèle SOA Policy Gateway Advanced Runtime», à la page 35

5. Cliquez sur **OK** pour déployer.

Que faire ensuite

Pour vérifier le déploiement, voir «Vérification du déploiement».

Vérification du déploiement

Une fois que vous avez 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 119.
2. Facultatif : Si vous avez déployé le modèle Exemple SOA Policy Gateway Basic Runtime, 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 79.

Scénario : ajout d'un environnement d'exécution supplémentaire au modèle

Le profil d'activation de gouvernance 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. En d'autres termes, 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. Ceci est approprié 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 Capability Version pour une utilisation généralisée. 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 57.

Procédure

1. Déployez le SOA Policy Gateway Governance Master prédéfini. Pour plus d'informations, voir «Déploiement du modèle SOA Policy Gateway Governance Master», à la page 70.
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 : Personnalisation des environnements d'exécution.
3. Configurez les modèles SOA Policy Gateway Basic Runtime ou SOA Policy Gateway Advanced Runtime avec les détails de Governance Master. Pour plus d'informations, voir «Informations sur le déploiement de SOA Policy Gateway Governance Master», à la page 71.

   Remarque : La valeur d'environnement de promotion doit être définie à «Unset».
4. Déployez le modèle SOA Policy Gateway Basic Runtime ou SOA Policy Gateway Advanced Runtime prédéfini. Pour plus d'informations, voir «Déploiement du modèle SOA Policy Gateway Basic Runtime», à la page 71 et «Déploiement du modèle SOA Policy Gateway Advanced Runtime», à la page 72.

Clonage et personnalisation du modèle IBM SOA Policy Gateway Pattern

IBM SOA Policy Gateway Pattern ne peut pas être modifié. Si la topologie fournie dans les modèles du système virtuel du modèle IBM SOA Policy Gateway Pattern ne fournit pas la fonction dont vous avez besoin, vous pouvez cloner le modèle et ensuite le modifier pour créer d'autres modèles.

Pourquoi et quand exécuter cette tâche

Vous pouvez personnaliser les modèles des manières suivantes :

- Ajouter des domaines DataPower supplémentaires. Pour plus d'informations, voir «Déploiement avec plusieurs domaines DataPower», à la page 76.
- Augmenter la taille de cluster par défaut. Pour plus d'information, voir Centre de documentation d'IBM Workload Deployer version 3.1.

  Remarque : Lors du développement de la taille de cluster, augmentez également la taille de mémoire du gestionnaire de déploiement de WSRR
- Choisir le moyen d'obtenir le fichier de sécurité compressé sur le serveur. Pour plus d'informations, voir «Gestion de la sécurité», à la page 60.
- Définir et verrouiller vos propres valeurs par défaut ; par exemple, l'ID administrateur de DataPower. Pour plus d'informations sur les paramètres de verrouillage, voir Centre de documentation d'IBM Workload Deployer version 3.1.
- Vous permet d'utiliser votre propre mécanisme pour télécharger le fichier `DomainZipFile.zip`. Pour plus d'informations, voir «Fourniture de votre propre mécanisme de téléchargement du fichier `DomainZipFile.zip`», à la page 65.

Procédure

Pour cloner les modèles et les modifier pour créer d'autres modèles, procédez comme suit :

1. Dans le panneau de gauche de la fenêtre Modèle, sélectionnez le modèle à cloner.
2. Cliquez sur l'icône Cloner et entrez un nom pour le nouveau modèle. Vous pouvez également indiquer des informations supplémentaires, comme une description.
3. Sélectionnez le nouveau modèle et cliquez sur l'icône Editer pour modifier la configuration. Vous pouvez ajouter et supprimer des composants et les configurer, augmenter ou réduire le nombre de certains composants, ou modifier l'ordre dans lequel certains composants sont déployés.

Que faire ensuite

Vérifiez que vous disposez de tous les composants requis correctement configurés pour le type de modèle que vous avez créé. Vous pouvez déployer le modèle lorsque votre configuration est terminée.

Information associée:

IBM Workload Deployer : Gestion des modèles de système virtuel

IBM PureApplication System : Gestion des modèles de système virtuel

Déploiement avec plusieurs domaines DataPower

Vous pouvez cloner et personnaliser les modèles SOA Policy Gateway Basic Runtime et SOA Policy Gateway Advanced Runtime pour inclure plusieurs domaines DataPower.

Procédure

1. Clonez le modèle SOA Policy Gateway Basic Runtime ou SOA Policy Gateway Advanced Runtime. Pour plus d'informations, voir «Clonage et personnalisation du modèle IBM SOA Policy Gateway Pattern», à la page 75.
2. Pour éditer le modèle, cliquez sur **Edit** (Editer).
3. Développez la section **Scripts**.
4. Pour chaque domaine supplémentaire à ajouter, glissez-déposez le package de script **SOA Policy Gateway 2.0.0.0 DataPower Domain** sur le composant du gestionnaire de déploiement de WSRR pour le modèle Basic Runtime.
5. Cliquez sur **Done editing** (Edition terminée).
6. Déployez le modèle, en entrant les informations suivantes pour chaque domaine ajouté :
   - DataPower_hostname
   - DataPower_XML_mgmt_port
   - DataPower_admin_id
   - DataPower_admin_password
   - Confirmation du mot de passe
   - New_DataPower_domain
   - securityFileCleanUp

Remarque : Lorsque plusieurs domaines sont utilisés, le dernier domaine doit avoir la valeur securityFileCleanUp définie à **true** ; en revanche, cette valeur doit être définie à **false** pour tous les autres domaines.

Pour plus d'informations sur le déploiement des modèles, voir «Déploiement du modèle SOA Policy Gateway Basic Runtime», à la page 71 ou «Déploiement du modèle SOA Policy Gateway Advanced Runtime», à la page 72.

Modèle d'application

Le modèle d'application est un domaine DataPower configurable et un ensemble d'artefacts WSRR permettant de présenter les fonctions du modèle.

Le scénario de base du modèle d'application est une application d'inventaire pour un magasin (entrepôt). Il existe un service Web de magasin qui compte trois opérations :

- purchase
- findInventory
- returnProduct

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

- Validation par rapport à Store.wsdl. Ceci suppose que la validation DataPower est désactivée.
- Rejet s'il y a plus de 5 messages en 90 secondes. Il s'agit d'un seuil bas facilitant les démonstrations.

Les consommateurs de ce service disposent actuellement de deux accords sur les niveaux de licence (SLA) : Gold et Anonymous. Si le contexte du client dans l'en-tête HTTP est Gold, les acheminements s'effectuent immédiatement vers le noeud final de remplacement (Alternate endpoint). S'il sont anonymes, ce qui se traduit par non-Gold, l'accès s'effectue vers le noeud final de service simulé du magasin (Store Mock Service), qui présente une valeur tarifaire différente pour l'élément.

Le scénario exécute également l'autorisation pour l'opération findInventory, selon l'appartenance à un groupe d'utilisateurs. La figure 5, à la page 78 affiche le flux de l'application avec chaque zone représentant une passerelle DataPower différente.

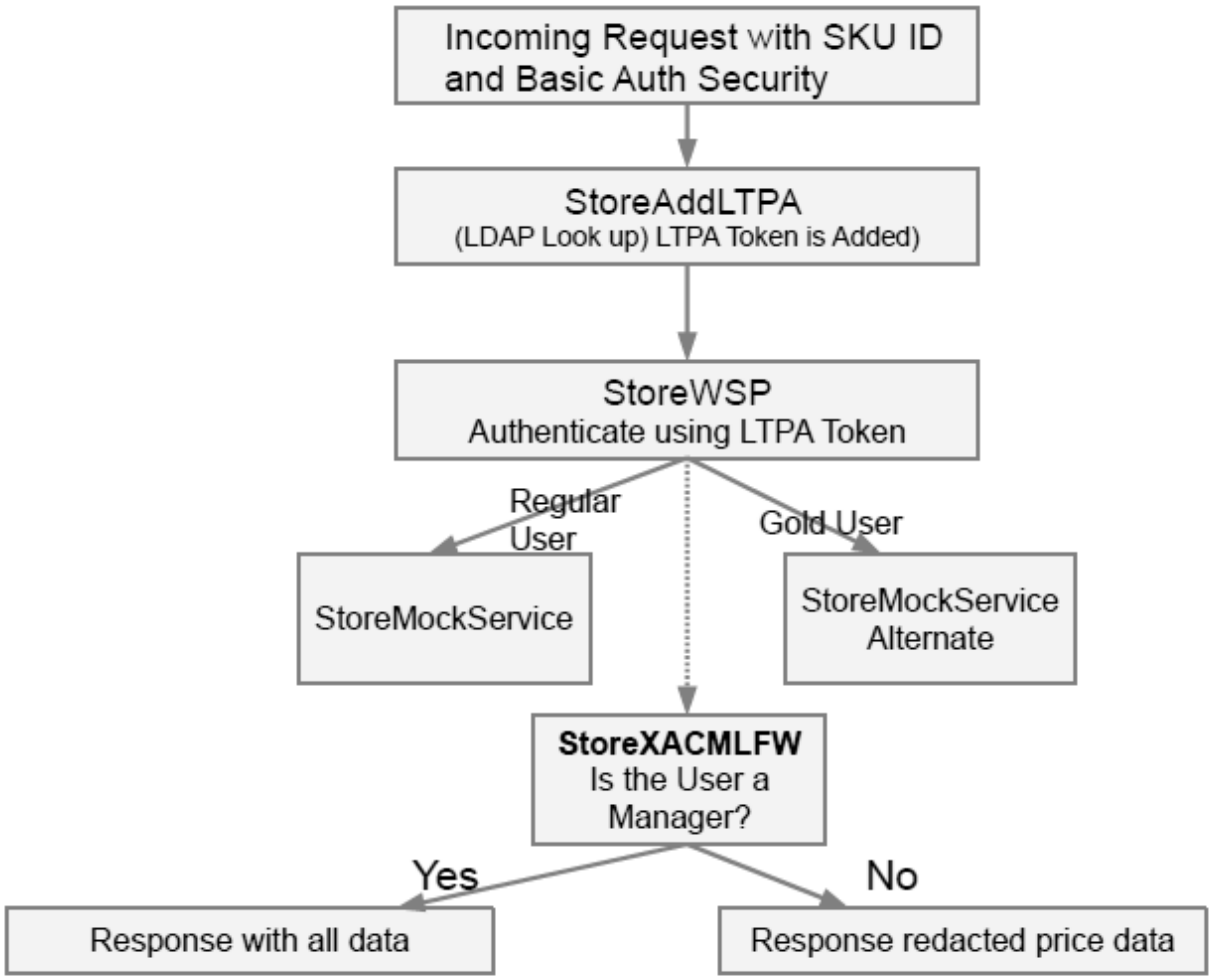


Figure 5. Le diagramme du flux du modèle d'application

Tâches associées:

«Clonage et personnalisation du modèle IBM SOA Policy Gateway Pattern», à la page 75
IBM SOA Policy Gateway Pattern ne peut pas être modifié. Si la topologie fournie dans les modèles du système virtuel du modèle IBM SOA Policy Gateway Pattern ne fournit pas la fonction dont vous avez besoin, vous pouvez cloner le modèle et ensuite le modifier pour créer d'autres modèles.

Présentation des artefacts WSRR de l'exemple

Les artefacts WSRR décrivent les opérations d'entreposage.

Il existe des fonctions métier de base relatives à l'entreposage et qui font partie de l'organisation plus étendue des entrepôts de Bob. La version de service, Store V1.0, représente le service de magasin. La définition de niveau de service du magasin (Store SLD) dispose de deux accords sur les niveaux de licence (SLA) : l'un concerne les utilisateurs Gold et les achemine vers un autre service préféré, l'autre concerne l'accord sur les niveaux de licence (SLA) des utilisateurs anonymes qui est destiné à tous les autres utilisateurs et qui consiste simplement à consigner dans un journal une notification sur DataPower indiquant qu'une requête a été

effectuée. Store SLD possède également deux autres exemples de règles joints ; 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.

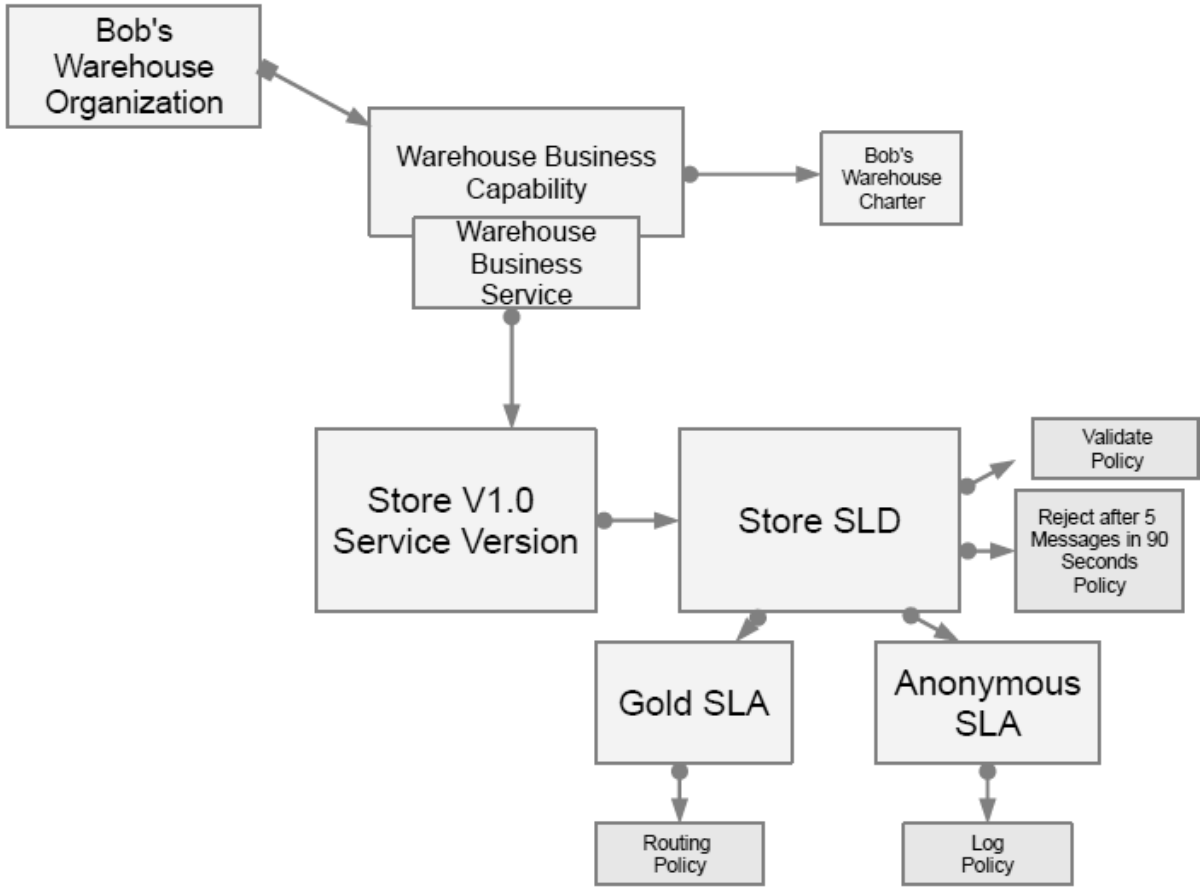


Figure 6. L'exemple de domaine

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 Exemple SOA Policy Gateway Basic Runtime déployé. Il existe six variations de test qui peuvent être exécutées sur le modèle d'application via la ligne de commande.

Pour déployer le modèle Basic Sample Runtime, voir «Déploiement du modèle Exemple SOA Policy Gateway Basic Runtime», à la page 69.

Remarque : La valeur de `SamplePolicySample_starting_port` utilisée dans les exemples XML suivants est issue des journaux associés au modèle Exemple SOA Policy Gateway Basic Runtime.

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 cela, développez la section **Virtual machines** (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. L'écran de test du modèle d'application implémenté dans DataPower s'affiche.
4. Les options sont les suivantes :
   - **Send Standard** - Envoie une requête findInventory au service du magasin. L'ID de contexte est un utilisateur «Silver». Un résultat correct est `Part: SKU10 Price: 461.73`.
   - **Send Routed** - Envoie une requête findInventory au service du magasin. L'ID de contexte est un utilisateur «Gold», en conséquence la requête est acheminée vers une implémentation du service. Un résultat correct est `Part: GOLDSKU10 Price: 461.73`.
   - **Send Invalid** - Envoie d'une requête avec un contenu non valide. Les règles de validation nécessitent DataPower pour valider une requête et un résultat correct doit être un message de réponse provenant de DataPower `"Internal Error (from client)"`.
   - **User ID = ConsumerA** - Pour des appels avec un ID utilisateur ConsumerA, la règle XACML est appliquée de telle sorte que seuls les Managers (gestionnaires) peuvent voir le prix. La valeur du prix dans le message de réponse doit être rédigée. Un résultat correct contient `Price: 0.0`.
   - **Many Standard Requests** - Si plus de 5 requêtes sont effectuées dans les 90 secondes, la règle de refus s'applique alors. Une réponse correcte montrant que règle a été appliquée est : `Rejected: "Rejected (from client)"`.
5. Ouvrez la console WSRR et explorez le service et les règles. Pour plus d'informations, voir «Connexion à WSRR - Business Space», à la page 100.

Pour exécuter les scénarios de test du modèle d'application à l'aide de la ligne de commande :

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 ci-dessus 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://<votre_nom_hôte_DataPower>.com:<SamplePolicySample_starting_port+4>/Store/Store
```

Dans cet exemple, ConsumerX est un Manager et donc nous devons voir les informations complètes sur les prix 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://<votre_nom_hôte_DataPower>.com:<SamplePolicySample_starting_port+4>/Store/Store
```

Notez que la réponse a un prix réécrit qui est 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

L'accord sur les niveaux de licence de l'ID de contexte permet de déclencher la règle de routage. Dans ce cas, l'accord sur les niveaux de licence (SLA) des clients Gold a la valeur «Gold» dans l'accord sur les niveaux de licence (SLA). Voici le contenu d'un exemple de requête avec Gold comme ID de contexte (contextIdentifier) :

```
<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 ci-dessus 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://<votre_nom_hôte_DataPower>.com:<SamplePolicySample_starting_port+4>/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.wsl 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 nous exécutons la requête curl suivante :

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

Ceci produit 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>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 ait 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://<votre_nom_hôte_DataPower>.com:<SamplePolicySample_starting_port+4>/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 Manager (gestionnaire). En conséquence, les informations complètes sur les prix doivent être affichées comme suit 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

Dans le cas où l'ID de contexte n'est pas «Gold», aucun accord sur les niveaux de licence (SLA) n'est mappé et donc l'accord sur les niveaux de licence anonyme est utilisé. La règle de médiation pour l'accord sur les niveaux de licence anonyme consiste à consigner ou notifier. Ceci implique l'activation du mode débogage Debug pour l'exemple de domaine. Exécutez la commande suivante :

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

Dans ce cas, ConsumerX est un Manager, nous devons donc voir les informations complètes sur les prix 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">AFIAAgAkZmExODgzNTQtY2Q1ZC0zYjU0L
WEyMzItZGM3MmEzNWY0MTAzACRmYWVjYjA1Mi1jMWUxLTMyODEtOWY3Ni0wY2IxNm
RhMDc4MjkAAw==</KD4NS:KD4SoapHeaderV2></soapenv:Header><soapenv:Body><b:fin
dInventoryResponse xmlns:a="http://company.ibm.com/"
xmlns:b="http://company.ibm.com/store">
<findInventoryRes>
<sku>SKU10</sku>
<price>461.73</price>
<inventory>460</inventory>
<msrp>923.46</msrp>
<supplierID>IBM</supplierID>
</findInventoryRes>
</b:findInventoryResponse>
</soapenv:Body>
</soapenv:Envelope>
```

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 définie à debug (débogage) pour pouvoir voir ce message. Si ce n'est pas le cas, cliquez sur l'icône Troubleshooting (traitement des incidents) de la console Web de DataPower. Dans la section Logging (Consignation), changez la valeur Log level pour «debug», puis cliquez sur **Set Log Level**.

Pour trouver le journal, sélectionnez **Fichiers** et **Administration des fichiers** > **Gestion des fichiers**. Le journal se trouve dans le dossier `logtemp` et se nomme `default-log`. En raison de l'encapsulage du journal, vous devrez peut-être mettre le fichier journal dans une fenêtre de navigateur Web avant d'exécuter le test et actualiser la page dans le navigateur après l'exécution du test.

Tâches associées:

«Déploiement du modèle Exemple SOA Policy Gateway Basic Runtime», à la page 69
Le déploiement du modèle Exemple SOA Policy Gateway Basic Runtime crée une instance de système virtuel d'exécution du modèle.

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. S'il a été souhaité de déplacer le point de décision de règles (PDP) vers un autre dispositif DataPower, un profil de proxy SSL peut avoir été 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/envel
xmlns:xacml-context="urn:oasis:names:tc:xacml:2.0:context:schema:os" xmlns:ws="http://docs.oasis-open.org/wss/2004/01/oas
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>
```

En examinant le fichier `sendToPDP.xsl`, nous devrions constater les points suivants :

1. La feuille de style récupère le port pour XACMLFW à parir 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.

Examinons la feuille de style des règles pour la réécriture.

StorePrivateDataXACML.xml

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

Notez les points suivants :

- 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:s
```

- 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 les scripts `.xsl` utilisés dans l'application au niveau de plusieurs points.

Procédure

Pour modifier l'exemple de feuilles de style XSL, vous pouvez :

1. Modifier le mappage de données d'identification pour AZ.

   Ouvrez la feuille de style `rgxacml.xsl` et exécutez les instructions XSL suivantes :

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

   Les variables suivantes sont définies dans la feuille de style `soavars.xsl` :

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

   L'exemple contient un mot de passe non chiffré pour le serveur LDAP ; peut-être souhaitez-vous personnaliser la feuille de style fournie pour déchiffrer un mot de passe chiffré.

```
<!-- Spécifiez le nom descriptif de base pour débuter la recherche -->
<xsl:variable name="baseDN">dc=ibm.com</xsl:variable>
```

   `baseDN` est codé en dur `dc=ibm.com`. Si vous avez configuré votre LDAP avec un suffixe différent, baseDN, modifiez cette ligne pour personnaliser l'exemple.

2. Modifier la feuille de style de rédaction (Redaction).

   La feuille de style `noPriceInfo.xsl` contient le code suivant, qui met à zéro toutes les valeurs de prix. 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 **Add** (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.

Edition des documents de règles

Utilisez l'interface utilisateur de Business Space pour 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 101.

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», à la page 115.
2. Cliquez sur **Terminer**. La vue Parcourir s'affiche.
3. 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 117.

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.

Tâches associées:

«Création de règles», à la page 115
Lors de la création de règles de médiation dans l'interface utilisateur de Business Space, indiquez les conditions et actions relatives à la règle.

«Gérer le cycle de vie de la règle», à la page 117
Les règles peuvent être en transition entre des états de gouvernance à l'aide de l'interface utilisateur de Business Space.

Information associée:

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

L'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 78.
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. Ceci 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 (return) nécessitent Manager ou Clerk tandis que les achats (purchase) peuvent être effectués par des clients (Customer).

4. Définition la valeur ConsumerID (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 de back end (dorsale) 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-feux XML dans l'exemple

Les pare-feux 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 ne peuvent appeler qu'en utilisant une authentification de base (par exemple, aucune authentification LTPA ou similaire). La règle de traitement de la requête :

1. Identifie via l'authentification de base.
2. Authentifie via une recherche LDAP très 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

StoreMockServiceAlternate 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 politique de routage appliquée.

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-feux 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 stratégie 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 : Ce 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 manuellement 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 ressources sont utilisés dans l'exemple ; le premier 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>
</Sujet>
<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>
</Sujet>
</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 devez voir qu'il existe des mappages similaires pour Customer et Clerk. Vous devez 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.

Si vous examinez la feuille de style storeCallPDP.xsl style vous devez remarquer les choses suivantes :

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. L'examen de XACML pour Redaction, storePrivateDataXACML.xml, la structure 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']/*[loc
        response']/*[local-name()='Envelope']/*[local-name()='Body']/*[local-name()='Response']/*[local-name()='Result']/*[
        Decision']" />
      </xsl:variable>
      <xsl:message dp:priority="debug">
        <DECISION-FROM-RTSS>
          <xsl:value-of select="$decision" />
        </DECISION-FROM-RTSS>
      </xsl:message>
      <xsl:choose>
      <xsl:when test="$decision = 'Permit'">
        <xsl:message dp:priority="debug">****** 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 Exemple SOA Policy Gateway Basic Runtime

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

Tableau 33. Artefacts WSRR créés pour le modèle Exemple SOA Policy Gateway Basic Runtime

Objet	Description
Organisation	Entrepôt de Bob.

Tableau 33. Artefacts WSRR créés pour le modèle Exemple SOA Policy Gateway Basic Runtime (suite)

Objet	Description
Fonction métier	Entrepôt, appartenant à l'entreprise d'entreposage de Bob.
Version de service	Store 1.0 utilise le service Web du magasin (Store Web Service), la définition de niveau de service de magasin (Store SLD) et la fonction métier d'entrepôt (Warehouse Business Capability).
WSDL	Store.wsdl
XSD	Company.xsd
Politique	• Validate.xml • RouteForGold.xml • LogEveryTime.xml • RejectAfter5MsgIn90Seconds.xml
Annexes de politique	• Anonymous Users_GenericObject_Anonymous Users_LogEveryTime.xml - Joint la règle LogEveryTime à l'accord sur les niveaux de service (SLA) des utilisateurs anonymes. • Gold SLA_GenericObject_Gold SLA_RouteForGold.xml - Joint la règle RouteForGold à l'accord sur les niveaux de service (SLA) Gold. • Store_GenericObject_Store_urn :RejectAfter5MsgIn90Seconds.xml - Joint la règle RejectAfter5MsgIn90Seconds à la définition de niveau de service du magasin (Store SLD). • Store_GenericObject_Store_urn:Validate.xml - Joint la règle Validate à la définition de niveau de service du magasin (Store SLD).
SLD	Définition de niveau de service de magasin (Store SLD) - Utilisé par la version de service Store 1.0.
SLA	Accord sur les niveaux de service (SLA) Gold - Achemine vers le noeud final Gold si l'ID de contexte est «Gold».
Anonymous SLA	Utilisateurs anonymes - Utilise la notification de règle LogEveryTime et est exécuté si l'ID de contexte n'est pas «Gold».

Le modèle d'application utilise des artefacts WSRR

StoreWSP utilise un abonnement WSRR pour extraire des artefacts WSDL et de règles. Toutes les fois qu'une demande est traitée via StoreWSP, les actions suivantes sont menées :

1. La version de service Store 1.0 est connectée à la définition de niveau de service de magasin (Store SLD) qui dispose de deux politiques directes associées : Validate et RejectAfter5MsgIn90Seconds. L'ordre dans lequel les politiques sont exécutées est indéterminé.
   a. Si 5 requêtes se sont produites dans les dernières 90 secondes, la requête est refusée.
   b. La requête est validée par rapport à Store.wsdl avec son Company.xsd associé.
2. Le service Store 1.0 utilise la définition de niveau de service de magasin (Store SLD), qui dispose de deux accords sur les niveaux de licence (SLA) ; un SLA Gold destiné aux utilisateurs Gold et un SLA Anonymous Users (utilisateurs anonymes) pour tous les autres utilisateurs. Si l'attribut ID de contexte (ContextId) est «Gold», la requête est acheminée vers le pare-feu XML StoreMockServiceAlternate ; en revanche, s'il est «Silver» ou a tout autre valeur, l'accord de niveau de service (SLA) Anonymous Users (utilisateurs anonymes) prend le relais et la règle LogEveryTime est exécutée. Une notification est alors

inscrite dans le journal `default.log` de l'exemple de domaine. Elle ne peut être vue que si le mode de débogage (debug) a été activé pour le domaine. Le message est ensuite acheminé vers le pare-feu XML StoreMockService.

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

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

Tableau 34. Artefacts DataPower créés pour le modèle Exemple SOA Policy Gateway Basic Runtime

Type	Nom	Objet
Proxy service Web	StoreWSP	Service principal.
Pare-feux 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	La validation des données d'identification contient 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 opération 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.

L'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 35. 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.

Tableau 35. Feuilles de style du modèle d'application (suite)

Feuille de style	Objet
noPriceInfo.xsl	Cette feuille de style définit l'élément de prix à la valeur 0.0.
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 utilisant des feuilles de style XSL

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

Tableau 36. 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

Lorsque l'image IBM SOA Policy Gateway Pattern a été déployée, vous pouvez enregistrer vos propres définitions de service et associer vos propres règles aux définitions. Vous pouvez également afficher et gérer vos systèmes déployés. Pour afficher la liste des instances déployées, cliquez sur **Instances** > **Système virtuel**.

Affichage des détails de l'instance

Les détails d'une instance déployée peut être visualisés en sélectionnant une instance dans la liste des instances dans la fenêtre Instances du système virtuel. Les détails de l'instance du système virtuel sont affichés sur la droite. Les détails incluent la liste des machines virtuelles mises à disposition dans l'infrastructure de cloud pour ce déploiement, l'adresse IP, le statut de la machine virtuelle et le statut du rôle. Un rôle correspond à une unité de fonction exécutée par le middleware de l'application virtuelle sur une machine virtuelle. Vous pouvez également afficher les informations sur l'état de santé du rôle de la machine virtuelle. Par exemple, une coche rouge se trouve sur la flèche d'état vert lorsque l'UC est critique sur 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**. Développez une machine virtuelle en cours d'exécution pour afficher les journaux de script dans la section **Packages de script** et des liens pour accéder à la machine virtuelle à l'aide de la section **Consoles**.

Administration des instances déployées

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

Avant de commencer

Pour afficher une instance de système virtuel, vous devez d'abord avoir déployé 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. Dans la liste des instances de la fenêtre 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. Par exemple, vous pouvez :
   - Lancer et ouvrir une session sur la console d'administration pour le gestionnaire de déploiement, puis consultez les clusters créés.
   - Lancer le centre de processus, et télécharger ensuite le concepteur de processus pour créer des applications de processus.
   - Configurer IBM Integration Designer et vous connecter au centre de processus pour la création du processus.

Connexion à WSRR - Business Space

Utilisez l'interface utilisateur Business Space pour administrer les règles.

Pourquoi et quand exécuter cette tâche

Accédez à l'interface utilisateur Business Space à l'aide de l'adresse d'hôte du système WSRR.

Procédure

1. Cliquez sur **Instances** > **Systèmes virtuels** pour accéder à la fenêtre Instances de système virtuel.
2. Dans la liste des instances de la fenêtre Instances de système virtuel, sélectionnez l'instance qui a été déployée. Les détails de l'instance s'affichent.
3. Accédez au système WSRR à l'aide de l'interface utilisateur Business Space :
   - Dans la section **Consoles**, cliquez sur **WSRR Business Space** pour vous connecter à Business Space en cours d'exécution sur le système WSRR.
   - Vous pouvez également, dans un navigateur Web externe :
     a. Rechercher le nom d'hôte et les numéros de port pour WSRR. Développer la section **Machines virtuelles** et sélectionner 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**.
     b. Entrez l'adresse URL de Business Space :
        – Pour le serveur WSRR autonome avec la sécurité activée : `https://<nom_hôte>:9443/BusinessSpace`
        – Pour le cluster : `http://<nom_hôte>/BusinessSpace`

        où *<nom_hôte>* et *port* correspondent aux valeurs de nom d'hôte et de port du serveur WSRR.

Résultats

Business Space est affiché, et vous pouvez l'utiliser pour ajouter, éditer ou supprimer des règles.

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 Opérations.

Information associée:

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

Connexion à WSRR - Console Service Registry

Utilisez la console Service Registry pour classifier des versions de service.

Pourquoi et quand exécuter cette tâche

Accédez à l'interface utilisateur Service Registry à l'aide de l'adresse d'hôte du système WSRR.

Procédure

1. Cliquez sur **Instances** > **Systèmes virtuels** pour accéder à la fenêtre Instances de système virtuel.
2. Dans la liste des instances de la fenêtre Instances de système virtuel, sélectionnez l'instance qui a été déployée. Les détails de l'instance s'affichent.
3. Accédez au système WSRR :
   - Dans la section **Consoles**, cliquez sur **WSRR_Web_UI** pour vous connecter à l'espace métier Business Space en cours d'exécution sur le système WSRR.
   - Vous pouvez également, dans un navigateur Web externe :
     a. Rechercher le nom d'hôte et les numéros de port pour WSRR. Développer la section **Machines virtuelles** et sélectionner 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**.
     b. Entrez l'adresse URL de la console Service Registry : http://*nom_hôte*/ServiceRegistry

        où *nom_hôte* est le nom d'hôte du serveur WSRR.

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 100.

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'a pas encore été créé, vous devez le créé. 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 utilisateur de Gouvernance SOA. 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 (actions du registre de services) :

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**.

Configuration d'un modèle de post-déploiement

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

Changement des paramètres LDAP pour le modèle d'application

Si vous utilisez le modèle Exemple SOA Policy Gateway Basic Runtime et devez modifier les paramètres de sécurité pour votre serveur LDAP, par exemple, le mot de passe ou le nom d'utilisateur, vous devez modifier ces valeurs dans deux emplacements.

Emplacements dans lesquels ces modifications sont à réaliser :

- La section AAA Policy Authentication (Authentification de règle AAA) pour la règle AAA StoreAddLTPA - Pour rechercher cette règle, utilisez la fenêtre de recherche de l'interface utilisateur Web d'administration de DataPower et recherchez `AAA`. Sélectionnez la règle AAA et changez la valeur sous l'onglet Authentication (Authentification).
- Le fichier `soavars.xsl` - Utilisez la section File Management (Gestion des fichiers) de l'interface utilisateur de l'administrateur Web de DataPower. Ouvrez le domaine créé par le modèle Exemple SOA Policy Gateway Basic Runtime sur le dispositif DataPower et accédez au fichier `soavars.xsl` à partir du répertoire local. Modifiez les variables LDAPHost, LDAPPort, LDAPCN, LDAPPassword, le cas échéant.

  Remarque : Il sera peut-être nécessaire de redémarrer le domaine pour ces modifications soient prises en compte.

Valeurs de noms distinctifs (DN) 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 est plus stricte que la sécurité par défaut de WebSphere Application Server.

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 très spécifique qui fonctionne entre les valeurs par défaut de WebSphere Application Server et DataPower pourrait ne pas fonctionner pour le package de script «SOA Policy Gateway 2.0.0.0 - Security» ou le package de script «SOA Policy Gateway 2.0.0.0 - Sample» utilisé avec la IBM SOA Policy Gateway Pattern ; par exemple, un nom distinctif de `mon_serveur.votre_entreprise.com` pourrait être accepté selon les valeurs par défaut de WebSphere Application Server, mais pas par les packages de script. Pour ajouter ou supprimer les certificats DataPower utilisés avec le déploiement, voir «Suppression ou ajout de certificats DataPower au fichier de clés certifiées WSRR.», à la page 104.

Changement des clés LTPA

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

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 un environnement Advanced ND, dans ce WSRR procédez comme suit :
   a. Synchronisez tous les noeuds.
   b. Arrêtez le cluster WSRR.
   c. Arrêtez les agents de noeud.
   d. Arrêtez le Dmgr.
4. Si l'environnement est Advanced, il doit être redémarré en procédant 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 Standalone (autonome), vous devez l'arrêter et le redémarrer pour que le changement de clé LTPA prenne effet.

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

Cette tâche décrit comment ajouter ou supprimer des certificats DataPower. L'un des avantages de l'exécution de cette tâche est qu'elle simplifie la configuration future de la fonction de mise à jour de synchronisation entre WSRR et DataPower pour des mises à jour de règles.

Pourquoi et quand exécuter cette tâche

Les certificats DataPower composants des modèles utilisés pas l'outil curl. Les appels DataPower sont téléchargés dans le fichier de clés certifiées par défaut du noeud ou de la cellule. Ceci simplifie la configuration future de l'utilisation de la fonction de mise à jour synchronisée entre WSRR et DataPower pour les mises à jour de règles. Si cette fonction n'est pas nécessaire, cette procédure décrit comment supprimer des certificats DataPower. Cette procédure décrit également comment ajouter de nouveaux certificats DataPower si les certificats doivent être modifiés.

Procédure

1. Ouvrez une session dans WSRR Dmgr ou Stand Alone à l'adresse `http://hostname:9060/admin`. Entrez l'utilisateur et le mot de passe.
2. Accédez à **Security, SSL certficates and key management**.
3. Cliquez sur **Key Stores and Certificates**.
4. Cliquez sur **NodeDefaultTrustStore** si vous choisissez le modèle de base (Basic) ou **CellDefaultTruststore** si vous optez pour le modèle avancé (Advanced).
5. Cliquez sur **Certificats de signataire**.
6. Sélectionnez les cases à cocher des certificats que vous souhaitez supprimer.
7. Cliquez sur **Supprimer**.
8. Cliquez sur **Enregistrer**.
9. Facultatif : si vous devez ajouter de nouveaux certificats DataPower, cliquez sur **Ajouter** pour ajouter le nouveau certificat.

Configuration du point d'application de règles

Le dispositif 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

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 (Input) et la sortie (Output), ainsi que la stratégie AAA. Vous pouvez créer la règle durant le processus de création de l'action de stratégie AAA, ou l'avoir créé avant cela 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 ont été 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, nous vous avons présenté deux exemples ; 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 89.
– 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.

Que faire ensuite

Outre la création d'un domaine et la définition d'une configuration de serveur WSRR dans les modèles SOA Policy Gateway Advanced Runtime et SOA Policy Gateway Basic Runtime, il est possible d'étendre le modèle en exécutant un script d'interface CLI personnalisé. Le script CLI doit être dans la racine de la structure `DomainZipFile.zip`, par exemple `/cli.cli`. L'interface CLI peut exécuter des commandes CLI standard, mais tous les artefacts auxquels l'interface fait référence doivent exister ou être accessibles par le domaine DataPower créé par le modèle. Lorsque vous déployez une instance des modèles SOA Policy Gateway Advanced Runtime ou SOA Policy Gateway Basic Runtime, vous serez invité à entrer le nom du fichier CLI dans les paramètres du package de Securty (sécurité).

Utilisation du modèle SOA Policy Gateway Basic Runtime

Le modèle SOA Policy Gateway Basic Runtime consiste en trois fonctionnalités principales ; les fichiers requis entre les scripts de DataPower et du modèle WSRR sont extraits, un domaine est configuré sous DataPower et enfin, une promotion est configurée.

Une fois ceci terminé, les actions suivantes doivent se produire :

1. Le nouveau domaine existe sur le dispositif DataPower spécifié.
2. Une définition de serveur WSRR existe dans le domaine.
3. Le script d'interface CLI a été exécuté par rapport au domaine DataPower.
4. Un serveur WSRR est configuré.
5. Tous les certificats de signataire DataPower fournis par le client ont été téléchargés sur le NodeDefaultTruststore de la cellule WSRR.
6. La promotion entre la cellule WSRR du modèle SOA Policy Gateway Basic Runtime et la cellule SOA Policy Gateway Governance Master a été configurée.
7. Les certificats de signataire ont été échangés. Le certificat de signataire du Dmgr de gouvernance est placé dans le NodeDefaultTrustStore de la cellule

Basic, et le certificat de signataire du Dmgr de cellule Basic est placé dans le CellDefaultTrustStore de la cellule de gouvernance.

8. Les clés LTPA ont été échangées. La clé LTPA de la cellule de gouvernance est importée dans la cellule Basic.
9. Chaque hôte du cluster WSRR du maître de gouvernance est ajouté aux domaines de confiance de la cellule Basic. Chaque hôte du cluster WSRR de cellule Basic est ajouté aux domaines de confiance du maître de gouvernance.
10. Le fichier de propriétés de promotion est configuré si la cellule a été désignée comme environnement de transfert ou de production dans les entrées données.

Bien que d'autres étapes soient nécessaires pour compléter un environnement de sécurité entièrement sécurisé, la configuration effectuée à ce stade vous permet d'effectuer les opérations suivantes :

1. Créer des services et des règles et les gouverner au travers du cycle de vie SOA sous WSRR (si les environnements de production et de transfert ont été fournis), en utilisant le profil GEP (Governance Enablement Profile) par défaut.
2. Créer des proxys de services Web qui peuvent utiliser la définition de serveur WSRR pré-créée pour générer des abonnements.

Utilisation du modèle SOA Policy Gateway Advanced Runtime

Le modèle SOA Policy Gateway Advanced Runtime consiste en trois fonctionnalités principales ; les fichiers requis entre les scripts de DataPower et du modèle WSRR sont extraits, un domaine est configuré sous DataPower et enfin, une promotion est configurée.

Une fois ceci terminé, les actions suivantes doivent se produire :

1. Un nouveau domaine existe sur le dispositif DataPower spécifié.
2. Une définition de serveur WSRR existe dans le domaine.
3. Le script d'interface CLI a été exécuté par rapport au domaine DataPower.
4. Un environnement en cluster WSRR avec des noeuds 'n' doit avoir été créé et configuré.
5. Tous les certificats de signataire DataPower fournis par le client doivent avoir été téléchargés sur le CellDefaultTruststore de la cellule WSRR.
6. La promotion entre la cellule WSRR du modèle SOA Policy Gateway Advanced Runtime et la cellule SOA Policy Gateway Governance Master a été configurée :
   a. Les certificats de signataire ont été échangés. Le certificat de signataire du Dmgr de gouvernance est placé dans le CellDefaultTrustStore de la cellule Advanced, et le certificat de signataire du Dmgr de cellule Advanced est placé dans le CellDefaultTrustStore de la cellule de gouvernance.
   b. Les clés LTPA doivent avoir été échangées. La clé LTPA de la cellule de gouvernance est importée dans la cellule Advanced.
   c. Chaque hôte du cluster WSRR du maître de gouvernance est ajouté aux domaines de confiance de la cellule Advanced. Chaque hôte du cluster WSRR de cellule Advanced est ajouté aux domaines de confiance du maître de gouvernance.
   d. Le fichier de propriétés de promotion est configuré si la cellule a été désignée comme environnement de transfert ou de production dans les entrées données.

La configuration actuelle vous permet de procéder comme suit :

1. Créer des services et des règles et les gouverner au travers du cycle de vie des règles SOA sous WSRR (si les environnements de production et de transfert ont été fournis), en utilisant le profil GEP (Governance Enablement Profile) par défaut.
2. Créer des proxys de services Web qui peuvent utiliser la définition de serveur WSRR pré-créée pour générer des abonnements.

Ensuite, vous devez entreprendre les étapes supplémentaires permettant d'obtenir un environnement de production entièrement sécurisé. Pour plus d'informations, voir «Sécurité appliquée aux modèles IBM SOA Policy Gateway Pattern», à la page 59.

Objets DataPower créés dans les modèles Basic Runtime et Advanced Runtime

Présentation des objets DataPower créés dans les modèles SOA Policy Gateway Basic Runtime et SOA Policy Gateway Advanced Runtime et leur fonction.

Tableau 37. Objets du modèle DataPower

Objet	Description
Domaine	Domaine utilisable pour l'application des utilisateurs.
Serveur WSRR	WSRRSVR nommé. L'adresse URL, l'ID 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 du 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** (Proxy de services Web).
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).

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 (SOA Governance) n'a pas été créé, reportez-vous à «Configuration de Business Space pour la première utilisation», à la page 101 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 : Administration 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 : Administration d'un service existant.

Tâches associées:

«Connexion à WSRR - Business Space», à la page 100
Utilisez l'interface utilisateur Business Space pour administrer les règles.

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) lors de la création de règles de médiation.

Règles dans WSRR

WSRR permet de 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, les règles personnalisées et d'autres domaines de règles qui doivent être prises en charge à l'avenir. 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 lors de l'ajout 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», à la page 115.

Assertions de règles de médiation

Les accords sur les niveaux de licence (SLA, Service Level Agreement) doivent provenir d'une exigence exprimée par l'entreprise pour laquelle la qualité de service fournie par un service doit répondre 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, il convient de spécifier des exigences non fonctionnelles 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.

Nous pouvons écrire une règle qui implémente des contrôles d'exécution sur les performances du service et prend des mesures en cas de non respect de l'accord sur les niveaux de service (SLA), afin de garantir que le service satisfait son SLA. Par exemple, nous pouvons 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 a créé un noeud final secondaire sur un autre serveur qui est normalement 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. Nous pouvons écrire une règles 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 un grand nombre de consommateurs, chacun ayant un niveau de priorité différent. Dans un exemple simple, nous pouvons avoir à la fois des consommateurs "Gold" et "Bronze", mais nous garantissons uniquement une qualité de service spécifique à nos consommateurs "Gold". Dans cet exemple, nous pouvons vérifier que si le consommateur est "Gold", il est réacheminé vers notre 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, nous pouvons 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 même 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. Pour protéger la qualité de service du service, nous pouvons 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 date et heure indiquées 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** (Date de début) - Cet attribut facultatif indique la date à laquelle la planification devient effective, format xs:date. L'attribut StartDate est inclusif et s'il est maquant, la planification devient effective immédiatement ce jour même.

  Remarque : Cliquez sur le lien hypertexte xs:date pour vous informer sur cette norme de l'industrie.
- **StopDate** (Date de fin) - Cet attribut facultatif indique la date à laquelle la planification cesse d'être effective, format xs:date. 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 l'heure à laquelle la planification démarre quotidiennement, format xs:time. (Remarque : cliquez sur le lien hypertexte xs:time pour comprendre cette norme de l'industrie).
  - **StopTime** (Heure de fin) – Si l'attribut Daily est spécifié, l'attribut StopTime est obligatoire. Il indique l'heure à laquelle la planification s'arrête quotidiennement, format xs:time. L'attribut StopTime est exclusif et si l'heure

spécifiée est antérieure ou identique à l'heure de début (StartTime) quotidienne, la planification s'arrête le jour suivant à l'heure de fin (StopTime) 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 va en réalité se terminer 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 obligatoires : 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 38. 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 39. opérateurs

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

Tableau 39. opérateurs (suite)

Opérateur	Signification
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** (Intervalle) - 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, format xs:duration. 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.

  Remarque : Cliquez sur le lien hypertexte xs:duration 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, ceci 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 doit rejeter ce comportement. Les actions de la règle de médiation autorisées sont les suivantes :

- **QueueMessage** – Cette action indique que des transactions doivent être mises en file d'attente si la condition logique est satisfaite. Le traitement de message ne doit pas être 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 doivent être rejetées si la condition logique est satisfaite. Les transactions continueront 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 doit être produite si la condition logique est satisfaite. Pour WebSphere DataPower, un message doit être écrit dans le journal système de DataPower.
- **RouteMessage** - Cet élément facultatif indique que des messages doivent être acheminés vers une destination de noeud final spécifiée si la condition logique est satisfaite. Les messages continueront 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 doivent être validés par rapport à la grammaire spécifiée. Les messages doivent être 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 doivent être validés par rapport au schéma XML identifié par l'identificateur URI qu'il contient.
  - **WSDL** - Indique que des messages doivent être validés par rapport à la description de service Web (WSDL) identifié par l'identificateur URI qu'elle contient.
  - **SCOPE** – Indique quelle partie du message doit être validée. Le tableau suivant répertorie les valeurs possibles et leur signification :

Tableau 40. 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 doivent être rejetées si l'exécution échoue. L'information Stylesheet doit être spécifiée, tandis que les paramètres (Parameters) sont facultatifs et doivent être indiqués si nécessaire par la feuille de style particulière spécifiée.

– **Stylesheet** - Indique que l'opération de transformation doit utiliser 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

Lors de la création de règles de médiation dans l'interface utilisateur de Business Space, indiquez les conditions et actions relatives à la règle.

Avant de commencer

Pour plus d'informations sur l'accès à Business Space, voir «Connexion à WSRR - Business Space», à la page 100.

Vous devez créer l'espace de gouvernance SOA (SOA Governance) avant de pouvoir créer des règles. Si l'espace de gouvernance SOA n'a pas été créé, reportez-vous à «Configuration de Business Space pour la première utilisation», à la page 101 et suivez les étapes pour créer l'espace.

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 utilisateur 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 109 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 afficher le document de règles pour la règle que vous venez de créer, sélectionnez le document de règles dans le widget du navigateur de Service Registry 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 de Service Registry situé sur la droite.

Concepts associés:

«Règles», à la page 109
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) lors de la création de règles de médiation.

Information associée:

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

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 101.

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», à la page 117.
   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 du profil d'activation de la 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.

Pourquoi et quand exécuter cette tâche

Pour plus d'informations sur la gouvernance, voir «Cycle de vie de règles SOA», à la page 4.

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 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 de Service Registry situé sur la droite. 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 4
Les règles de médiation sont gouvernées à l'aide du cycle de vie de règles SOA. Ceci 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 avec pièces jointes aux 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 lors du déploiement de modèles dans IBM SOA Policy Gateway Pattern.

Echec de la connexion à DataPower 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 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.
- Examinez les étapes d'échec de connexion SSL ci-dessous pour vérifier que les certificats sont correctement installés dans le fichier `DomainZipFile.zip` et sur le dispositif DataPower.

Identification et résolution de l'échec d'authentification de client s'agissant d'une authentification mutuelle

Essayez les solutions suivantes :

- Vérifiez que le fichier `DomainZipFile.zip` contenait les certificats appropriés.
- Vérifiez que le profil Crytpo sur le port d'interface de gestion XML dispose des données d'identification de validation avec tous les certificats de la chaîne.
- Vérifiez que les mots de passe pour la clé publique du client et le certificat public du client sont corrects.

identification et résolution de l'échec d'authentification de serveur

Essayez les solutions suivantes :

- Vérifiez que l'ensemble des certificats de la chaîne sont présents dans le répertoire *yourDataPowerHostName* du fichier `DominZipFile.zip` que vous utilisez.

- Vérifiez que le profil de proxy SSL possède un profil Crypto inverse qui contient les données d'identification avec la chaîne de certificats.

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-feux 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 connexion à SCP

Essayez les solutions suivantes :

- Vérifiez que le nom d'hôte SCP est correct.
- Vérifiez que l'utilisateur SCP est correct.
- Vérifiez que le mot de passe SCP est correct.
- Testez manuellement le point de contrôle de service (SCP) à partir d'un noeud dans l'environnement IBM Workload Deployer ou IBM PureApplication System avec les informations fournies.

Identification et résolution de l'échec d'extraction du fichier `DomainZipFile.zip` à partir du SCP ou du débogage des artefacts manquants

Essayez les solutions suivantes :

- Vérifiez que le fichier `DomainZipFile.zip` existe dans l'identificateur URI.
- Vérifiez que le file mentionné dans le fichier journal d'erreur existe dans l'emplacement approprié du fichier `DomainZipFile.zip`. En particulier, vérifiez que les certificats requis se trouvent dans le répertoire approprié.

Identification et résolution de l'échec de promotion

De nombreux problèmes peuvent survenir dans une promotion, notamment l'échec de la connexion au maître de gouvernance 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 du maître de gouvernance et vérifiez qu'il existe une entrée de certificat pour le Dmgr ou que le serveur autonome de l'environnement d'exécution, SOA Policy Gateway Basic Runtime ou SOA Policy Gateway Advanced Runtime, existe.
  - Accédez à l'environnement d'exécution, SOA Policy Gateway Basic Runtime ou SOA Policy Gateway Advanced Runtime, 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 du maître de gouvernance (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 le maître de gouvernance :
  - 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 de défaillances SSL dues à des certificats DataPower manquants.

Si vous n'avez pas indiqué dans le fichier `DomainZipFile.zip` le nom d'hôte correct pour votre répertoire de certificats DataPower Certificates, les packages de script échoueront dans l'établissement de la connexion avec le serveur WSRR si une authentification de serveur ou mutuelle est activée sur l'hôte DataPower.

Identification et résolution des incidents de connexion WSRR/DataPower

Si vous voyez que le statut de WSDL dans un proxy de services Web (Web Service Proxy) indique un état Down (Arrêt) ou Synchronizing (Synchronisation) et qu'il ne change jamais pour Okay, procédez aux vérifications suivantes :

1. Vérifiez que Crypto Certificate est valide pour le serveur WSRR (WSRRSVR).
2. Vérifiez que DataPower dispose du serveur de noms de domaine (DNS) approprié et configuré pour reconnaître le nom d'hôte (Hostname) du serveur WSRR ou du Dmgr.
3. Si le serveur de noms de domaine (DNS) est incorrect, une solution de contournement temporaire consiste à changer l'adresse URL dans la définition du serveur WSRR pour pointer directement sur l'IP en substituant le nom d'hôte (HostName) par l'IP dans l'adresse URL.
4. Accédez à WSRR Subscription (Abonnement WSRR) et effectuez une synchronisation manuelle :
   a. Recherchez dans `default.log` des erreurs relatives à la connectivité du serveur WSRR.
5. Vérifiez que les certificats requis correspondent à ceux qui figurent dans les données d'identification pour le profil Crypto du profil de proxy SSL de l'interface XMLManagement des dispositifs DataPower.

Identification et résolution des problèmes dans l'instance déployée

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

Echec de la connexion à LDAP

Pour diagnostiquer des incidents LDAP dans l'exemple, tentez les solutions suivantes :

- Dans la section de dépannage Troubleshooting du panneau de commande de DataPower, vérifiez que le trace est en mode débogage (debug).
- Accédez à StoreAddLTPA, ouvrez les détails de la sonde (Probe) et activez celle-ci.
- Effectuez un test client.
- Affichez les journaux dans la sonde. Recherchez les messages d'incident LDAP Bind.
- Vérifiez le nom d'hôte LDAP.
- Vérifiez le nom distinctif LDAP ; par exemple, cn=root,dc=ibm.com.
- Vérifiez le mot de passe LDAP ; par exemple, passw0rd.
- Vérifiez que le port LDAP est 389 et non sécurisé.
- Vérifiez que les mots de passe d'entrée pour ConsumerX, ConsumerA et ConsumerB sont tous passw0rd. Vérifiez que l'importation du fichier LDIF a permis la transcription des mots de passe corrects.

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 :

- Le nom d'hôte de DataPower
- Le 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.

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.

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 nouveau 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.

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 Instances de système virtuel.

Chapitre 9. Appendices

Remarques

Ces informations concernent initialement des produits et services fournis aux Etats-Unis.

Le présent document peut contenir des informations ou références concernant certains produits, services ou fonctions IBM non annoncés dans ce pays. Adressez-vous à votre interlocuteur IBM local pour plus d'informations sur les produits et services actuellement disponibles dans votre région. Toute référence à un produit, logiciel ou service IBM n'implique pas que seul ce produit, logiciel ou service IBM puisse être utilisé. Tout autre produit, logiciel ou service fonctionnellement équivalent peut être utilisé s'il n'enfreint aucun droit d'IBM. Toutefois, il est de la responsabilité de l'utilisateur d'évaluer et de vérifier le fonctionnement de tout produit, programme ou service non fourni par IBM.

IBM peut détenir des brevets ou des demandes de brevet couvrant les produits mentionnés dans le présent document. La remise de ce document ne vous donne aucun droit de licence sur ces brevets ou demandes de brevet. Si vous désirez recevoir des informations concernant l'acquisition de licences, veuillez en faire la demande par écrit à l'adresse suivante :

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

Les informations sur les licences concernant les produits utilisant un jeu de caractères double octet peuvent être obtenues par écrit auprès du service Propriété Intellectuelle d'IBM à l'adresse suivante :

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

Le paragraphe suivant ne s'applique ni au Royaume-Uni, ni dans aucun pays dans lequel il serait contraire aux lois locales LE PRESENT DOCUMENT EST LIVRE «EN L'ETAT». IBM DECLINE TOUTE RESPONSABILITE, EXPLICITE OU IMPLICITE, RELATIVE AUX INFORMATIONS QUI Y SONT CONTENUES, Y COMPRIS EN CE QUI CONCERNE LES GARANTIES DE NON-CONTREFACON ET D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE. Certaines juridictions n'autorisent pas l'exclusion des garanties implicites, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

Le présent document peut contenir des inexactitudes ou des coquilles. Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. IBM peut modifier à tout moment et sans préavis les produits et logiciels décrits dans ce document.

Les références à des sites Web non IBM sont fournies à titre d'information uniquement et n'impliquent en aucun cas une adhésion aux données qu'ils

contiennent. Les éléments figurant sur ces sites Web ne font pas partie des éléments du présent produit IBM et l'utilisation de ces sites relève de votre seule responsabilité.

IBM pourra utiliser ou diffuser, de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part tout ou partie des informations qui lui seront fournies.

Les licenciés souhaitant obtenir des informations permettant : (i) l'échange des données entre des logiciels créés de façon indépendante et d'autres logiciels (dont celui-ci), et (ii) l'utilisation mutuelle des données ainsi échangées, doivent adresser leur demande à :

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

Ces informations peuvent être soumises à des conditions particulières, prévoyant notamment le paiement d'une redevance.

Le logiciel sous licence décrit dans ce document et tous les éléments sous licence disponibles s'y rapportant sont fournis par IBM conformément aux dispositions du contrat sur les produits et services IBM, des conditions internationales d'utilisation des logiciels IBM ou de tout autre accord équivalent.

Les données de performances indiquées dans ce document ont été déterminées dans un environnement contrôlé. Par conséquent, les résultats peuvent varier de manière significative selon l'environnement d'exploitation utilisé. Certaines mesures évaluées sur des systèmes en cours de développement ne sont pas garanties sur tous les systèmes disponibles. En outre, elles peuvent résulter d'extrapolations. Les résultats obtenus peuvent varier. Il incombe aux utilisateurs de ce document de vérifier si ces données sont applicables à leur environnement d'exploitation.

Les informations concernant des produits non IBM ont été obtenues auprès des fournisseurs de ces produits, par l'intermédiaire d'annonces publiques ou via d'autres sources disponibles. IBM n'a pas testé ces produits et ne peut confirmer l'exactitude de leurs performances, ni leur compatibilité. Elle ne peut recevoir aucune réclamation concernant des produits non IBM. Toute question concernant les performances de produits non IBM doit être adressée aux fournisseurs de ces produits.

Toute instruction relative aux intentions d'IBM pour ses opérations à venir est susceptible d'être modifiée ou annulée sans préavis, et doit être considérée uniquement comme un objectif.

Le présent document peut contenir des exemples de données et de rapports utilisés couramment dans l'environnement professionnel. Ces exemples mentionnent des noms fictifs de personnes, de sociétés, de marques ou de produits à des fins illustratives ou explicatives uniquement. Toute ressemblance avec des noms de personnes, de sociétés ou des données réelles serait purement fortuite.

LICENCE DE COPYRIGHT :

Les présentes informations contiennent des exemples de programmes d'application en langage source illustrant les techniques de programmation sur diverses plateformes d'exploitation. Vous avez le droit de copier, de modifier et de distribuer ces exemples de programmes sous quelque forme que ce soit et sans paiement d'aucune redevance à IBM, à des fins de développement, d'utilisation, de vente ou de distribution de programmes d'application conformes aux interfaces de programme d'application des plateformes pour lesquelles ils ont été écrits. Ces exemples n'ont pas été intégralement testés dans toutes les conditions. Par conséquent, IBM ne peut garantir la fiabilité, la serviçabilité ou le fonctionnement de ces programmes.

Si vous visualisez ces informations en ligne, il se peut que les photographies et illustrations en couleur n'apparaissent pas à l'écran.

Informations relatives à l'interface de programmation

La documentation sur l'interface de programmation, lorsqu'elle est fournie, aide les utilisateurs à créer des applications à utiliser avec le produit.

Cependant, cette documentation peut également comporter des informations de diagnostic, de modification et de personnalisation. Les informations de diagnostic, de modification et de personnalisation sont fournies à des fins de débogage de vos applications.

Important : N'utilisez pas les informations de diagnostic, de modification et d'optimisation en guise d'interface de programmation car elles peuvent être modifiées sans préavis.

Marques

IBM, le logo IBM et ibm.com sont des marques d'IBM Corp., aux Etats-Unis et/ou dans certains autres pays. La liste actualisée de toutes les marques d'IBM est disponible sur la page Web “Copyright and trademark information” (www.ibm.com/legal/copytrade.shtml). Les autres noms de produits et de services peuvent appartenir à IBM ou à des tiers.

Le présent produit comprend des logiciels développés dans le cadre du projet Eclipse (http://www.eclipse.org/).

Java ainsi que tous les logos et toutes les marques incluant Java sont des marques d'Oracle et/ou de ses filiales.

Envoi de commentaires à IBM

Si vous avez des commentaires, positifs ou négatifs, à propos de ce manuel, veuillez utiliser l'une des méthodes ci-dessous pour entrer en contact avec IBM.

N'hésitez pas à nous faire part de vos remarques sur ce que vous considérez comme des erreurs ou omissions, ainsi que sur l'exactitude, la structure, les rubriques ou l'exhaustivité du présent manuel.

Veuillez limiter vos commentaires aux informations contenues dans ce manuel et sur leur présentation.

Pour toute question technique sur les produits ou systèmes IBM, prenez contact avec votre interlocuteur IBM habituel ou votre partenaire commercial IBM.

Lorsque vous envoyez des commentaires à IBM, vous lui accordez le droit non exclusif d'utiliser ou de distribuer les informations fournies de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part.

Vous pouvez envoyer vos commentaires à IBM selon l'une des méthodes ci-dessous :

- Par courrier :

  User Technologies Department (MP095)
  IBM United Kingdom Laboratories
  Hursley Park
  WINCHESTER,
  Hampshire
  SO21 2JN
  United Kingdom
- Par télécopie :
  - Depuis tous les pays (sauf le Royaume-Uni), composez le code d'accès international, puis 44-1962-816151.
  - Depuis le Royaume-Uni, composez le 01962-816151.
- Par voie électronique, avec l'ID réseau approprié :
  - IBM Mail Exchange: GBIBM2Q9 at IBMMAIL
  - IBMLink : HURSLEY(IDRCF)
  - Internet : idrcf@hursley.ibm.com

Quelle que soit la méthode utilisée, n'oubliez pas de mentionner :

- le titre et la référence de la publication,
- la rubrique sur laquelle portent vos commentaires,
- vos nom, adresse, numéros de téléphone et de télécopie, votre ID réseau.