Patrón IBM SOA Policy Gateway

Contenido

Capítulo 1. Visión general de la política SOA

La gestión de políticas juega un papel clave en el gobierno de políticas de modo estructurado y coherente. Las políticas se pueden utilizar para habilitar un mejor gobierno en cualquier entorno orientado a servicios.

Una política es un elemento independiente que puede aplicarse a uno o varios recursos, incluidos los diferentes servicios. La asignación de la política y todos los metadatos asociados, especialmente en un entorno distribuido, puede tener lugar en una variedad de puntos de aplicación y puntos de decisión.

La arquitectura de política SOA

La arquitectura de política SOA describe la interacción del punto de administración de políticas (PAP), el punto de aplicación de políticas (PEP), el punto de decisión de política (PDP), el punto de información de política (PIP) y el punto de supervisión de política (PMP). En el patrón, WSRR proporciona el PAP, WebSphere DataPower proporciona el PEP y el PMP se proporciona a través del componente de supervisión DataPower.

La organización de la arquitectura básica de la política y la definición de esos puntos clave es la siguiente:

- **Punto de administración de políticas**. Proporciona funciones para crear una política, gestionar y gobernar la política y su asignación a recursos y administrar los resultados de la política durante el tiempo de ejecución. El PAP incluye un repositorio para almacenar políticas. El PAP está proporcionado por WSRR.
- **Punto de aplicación de políticas**. Un punto de aplicación de políticas es un punto funcional que se ejecuta en el middleware. Ejecuta las siguientes acciones:
  - Aplica políticas.
  - Recibe actualizaciones de aplicación de la política y las prepara o convierte para poder utilizarlas.
  - Proporciona métricas de aplicación al Punto de supervisión de políticas.
  - Proporciona resultados y análisis de la aplicación de políticas al Punto de administración de políticas y a los Puntos de aplicación de políticas.
  - Cambia las ubicaciones donde se aplican las políticas y entran en vigor, dependiendo de la etapa del ciclo de vida:
    - Durante el diseño, WSRR es el punto de aplicación.
    - Durante la ejecución, generalmente las políticas son aplicadas por el sistema intermedio subyacente (middleware) que conecta proveedores de servicios con consumidores.

  En este patrón, el PEP viene proporcionado por WebSphere DataPower.
- **Punto de decisión de política**. Un punto de decisión de política evalúa las solicitudes de los participantes por comparación con políticas relevantes o contratos y atributos. El PDP entrega una decisión de autorización, elegibilidad o validación para proporcionar resultados calculados.
- **Punto de información de política**. Un punto de información de política proporciona información externa al punto de decisión de políticas, tal como información sobre atributos LDAP o los resultados de una base de datos, junto con información que se debe evaluar para tomar una decisión de política.

- **Punto de supervisión de políticas**. Un componente funcional que proporciona supervisión detallada de políticas para la arquitectura global; por ejemplo, la visión general de la política en el entorno distribuido. Ejecuta las siguientes acciones:
  - Recibir actualizaciones de supervisión de políticas y prepararlas o convertirlas para poder utilizarlas.
  - Capturar el análisis de estadísticas y la recopilación en tiempo real para su visualización.
  - Correlacionar, analizar y visualizar los datos proporcionados por los diferentes recopiladores en tiempo real, incluidos los puntos de aplicación de políticas.
  - Una consola de gestión que permite ver la gestión de la red distribuida de los puntos de aplicación de la política, y el estado de su aplicación.
  - Registrar, agregar medidas y resaltar los sucesos importantes, según lo especificado por la política de supervisión.
  - Proporcionar análisis de supervisión de políticas al Punto de administración de políticas y a los Puntos de aplicación de políticas.

  En este patrón, el PMP viene proporcionado por el componente de supervisión DataPower.

El consumidor y el proveedor ambos interactúan con el middleware, que a su vez interactúa con el repositorio y el software de supervisión.

¿Cómo funciona conjuntamente la arquitectura de la política SOA?

El flujo de patrón de la política SOA se muestra en Figura 1 en la página 3.

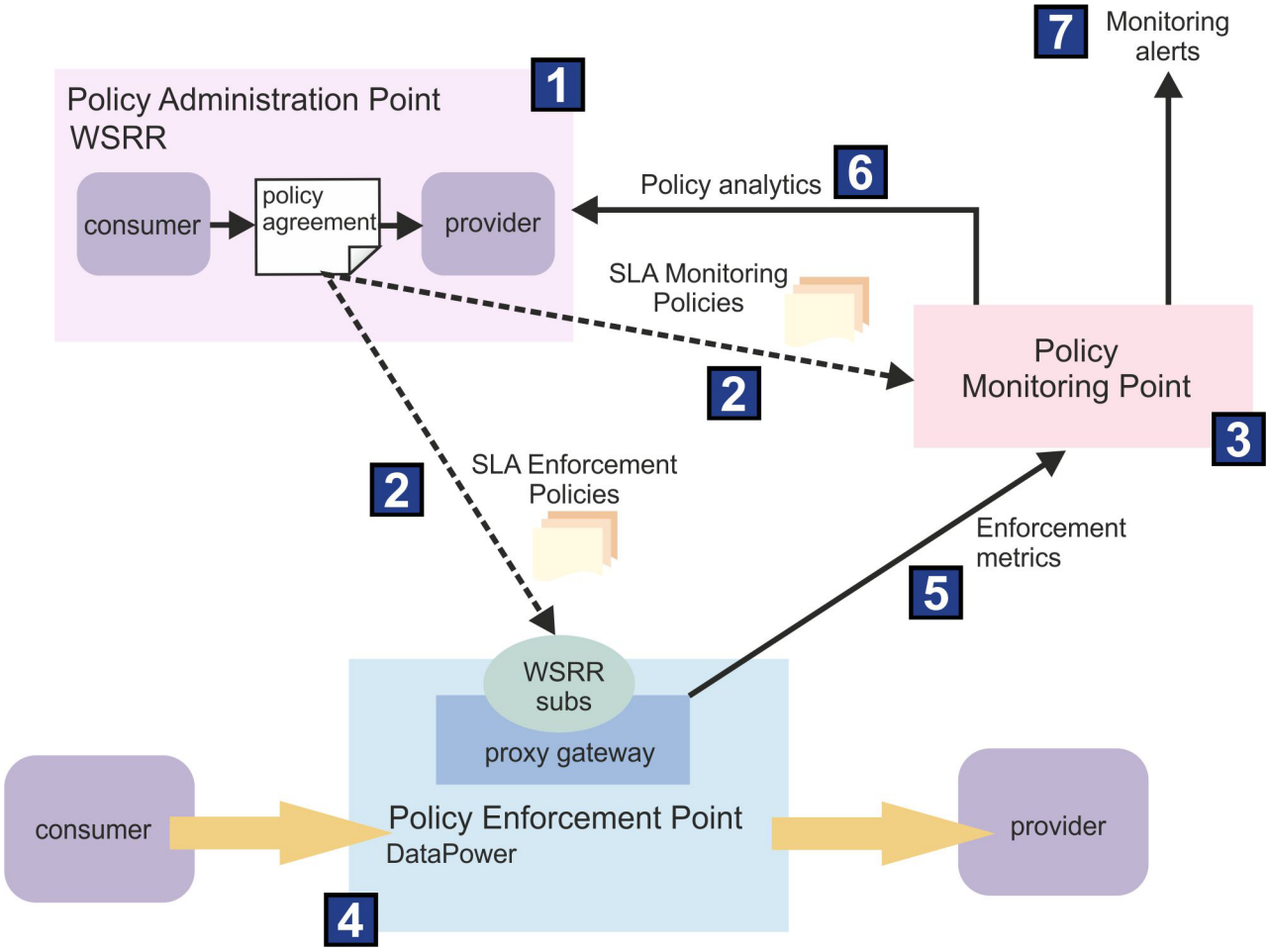


Figura 1. Política de Acuerdo de nivel de servicio (SLA): el modelo de despliegue de SOA

1 Las políticas se crean y después se adjuntan a servicios que necesitan esa política. Normalmente tiene el siguiente orden:

1. El conjunto de servicios se carga o crea en el repositorio de servicios. Esta acción forma parte del punto de administración de políticas.
2. El conjunto de políticas necesarias se crea en el punto de administración de políticas utilizando el ciclo de vida de políticas:
   - Se adjuntan políticas a los servicios que necesitan esas políticas, a nivel de nivel, operación o punto final, según sea necesario.

2 Publicación/suscripción automatizada de políticas desde el punto de administración de políticas a los puntos de aplicación de políticas y el punto de supervisión de política:

1. Como parte de la configuración, el servicio de supervisión se suscribe a la política de supervisión de WSRR. Esta acción se produce una sola vez.
2. Como parte de la configuración, se crean pasarelas de proxy en cada dispositivo de WebSphere DataPower (o dispositivo virtual) que tenga transacciones de servicio con aplicación de políticas. Esta acción se lleva a cabo una sola vez y se añade o se modifica, según sea necesario.

3. Como parte de la configuración, cada pasarela proxy del dispositivo se suscribe a políticas de WSRR para servicios de los que es responsable. Esta acción se lleva a cabo una sola vez y se añade o se modifica, según sea necesario.
4. Como parte de la configuración, WebSphere DataPower se configura de modo que las políticas se puedan compartir con otros dispositivos de un clúster. Esta acción se lleva a cabo una sola vez y se añade o se modifica, según sea necesario.
5. El punto de supervisión de políticas descarga las políticas de supervisión a medida que se publican.
6. El punto de supervisión de políticas convierte las políticas en la representación interna denominada políticas de situación.
7. WebSphere DataPower descarga los WSDL para los servicios de los que es responsable.
8. WebSphere DataPower descarga las políticas para los servicios de los que es responsable, cuando se lo notifica WSRR.
9. WebSphere DataPower convierte las políticas internas en la representación WebSphere DataPower interna con el formato de objetos SLM.


Supervisión de políticas SOA con creación de informes y notificación de operaciones:

1. Las políticas de supervisión están activas en la Política de situaciones de punto de supervisión de políticas.
2. El punto de supervisión de políticas recibe información de supervisión y la coloca en los espacios de trabajo.


Aplicación de políticas SOA:

1. La aplicación de políticas está activa en los diferentes dispositivos WebSphere DataPower.
2. WebSphere DataPower recibe las transacciones de servicios y aplica políticas para dicho servicio de consumidor y para el proveedor de servicios.


El punto de aplicación de políticas envía estadísticas de aplicación de políticas SOA al punto de supervisión de políticas.


El punto de supervisión de políticas envía sucesos de supervisión al punto de administración de políticas:

1. Los sucesos se configuran en el punto de administración de políticas que requiere supervisión desde el punto de supervisión de políticas. Esta acción se lleva a cabo una sola vez y se añade o se modifica, según sea necesario.
2. A medida que la evaluación de las políticas situación da como resultado True, se transfieren sucesos desde el punto de creación de políticas al punto de supervisión de políticas.


Supervisión de alertas:

- Se ejecutan periódicamente políticas de situación y se emprenden acciones operativas según lo especificado en la política. El valor predeterminado es cada 5 minutos.

Ciclo de vida de política SOA

Las políticas se gobiernan utilizando el ciclo de vida de política SOA. El ciclo de vida se inicia con definición de la política, luego se despliega durante la producción y finalmente se deja de utilizar cuando ya no es necesaria.

Para obtener más información sobre las transiciones y estados del ciclo de vida de política SOA, consulte Information Center de IBM® WebSphere Service Registry and Repository, Versión 8.0 - Ciclo de vida de la política SOA.

Estándares de políticas

Los grupos comunitarios técnicos de la web, W3C y OASIS han creado estándares para definir las políticas aplicables a los servicios web.

- **WS-Policy**: el dominio Web Services Mediation Policy 1.0 define un conjunto de aserciones de política para describir los requisitos de mediación de un servicio.
- **Web Services Policy 1.5 - Framework**: define una infraestructura y un modelo para expresar políticas que hacen referencia a prestaciones específicas del dominio, requisitos y características generales de las entidades de un sistema basado en servicios web.

Ejemplos de especificaciones que definen aserciones de política específicas del dominio:

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

Para obtener más información sobre WS-MediationPolicy, consulte ftp://public.dhe.ibm.com/software/solutions/soa/pdfs/WSMediationPolicy1.7-20130506.pdf.

El modelo de datos WS-Policy incluye las siguientes entidades:

- **Política**: una colección no ordenada de “alternativas de política”.
- **Alternativa de política**: una alternativa de política es una colección de “aserciones de política”.
- **Aserción de política**: representa una preferencia individual, por ejemplo, un requisito o una prestación.
- **Parámetros de política**: es la carga útil opaca de una “aserción de política”.
- **Asunto de política**: entidad a la que se puede vincular una expresión de política. Esta entidad se utiliza en un documento WS-PolicyAttachment.

En el ejemplo siguiente, la Figura 2 en la página 6, se muestra una expresión de política de seguridad que utiliza las aserciones definidas en WS-Security y 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">  <!-- policy expression -->
(02)   <wsp:ExactlyOne>
(03)     <wsp:All>    <!-- policy alternative #1 -->
(04)       <sp:SignedParts>;   <!-- policy assertion -->
(05)         <sp:Body>   <!-- policy assertion parameter -->
(06)       </sp:SignedParts>
(07)     </wsp:All>
(08)     <wsp:All>    <!-- policy alternative #2 -->
(09)       <sp:EncryptedParts> <!-- policy assertion -->
(10)         <sp:Body/>   <!-- policy assertion parameter -->
(11)       </sp:EncryptedParts>
(12)     </wsp:All>
(13)   </wsp:ExactlyOne>
(14) </wsp:Policy>
```

Las líneas (03-07) representan una política alternativa para firmar el cuerpo del mensaje.

Las líneas (08-12) representan una segunda alternativa de política cifrar el cuerpo del mensaje.

Las líneas (02-13) muestran el operador de política `ExactlyOne`. Los operadores de política agrupan las aserciones de política en alternativas de política. Una interpretación válida de la política sería que una invocación de un servicio web firmara o cifrara el cuerpo del mensaje, pero no ambas cosas.

Figura 2. Uso de políticas de servicios web con aserciones de política de seguridad.

La Figura 3 muestra una definición de política.

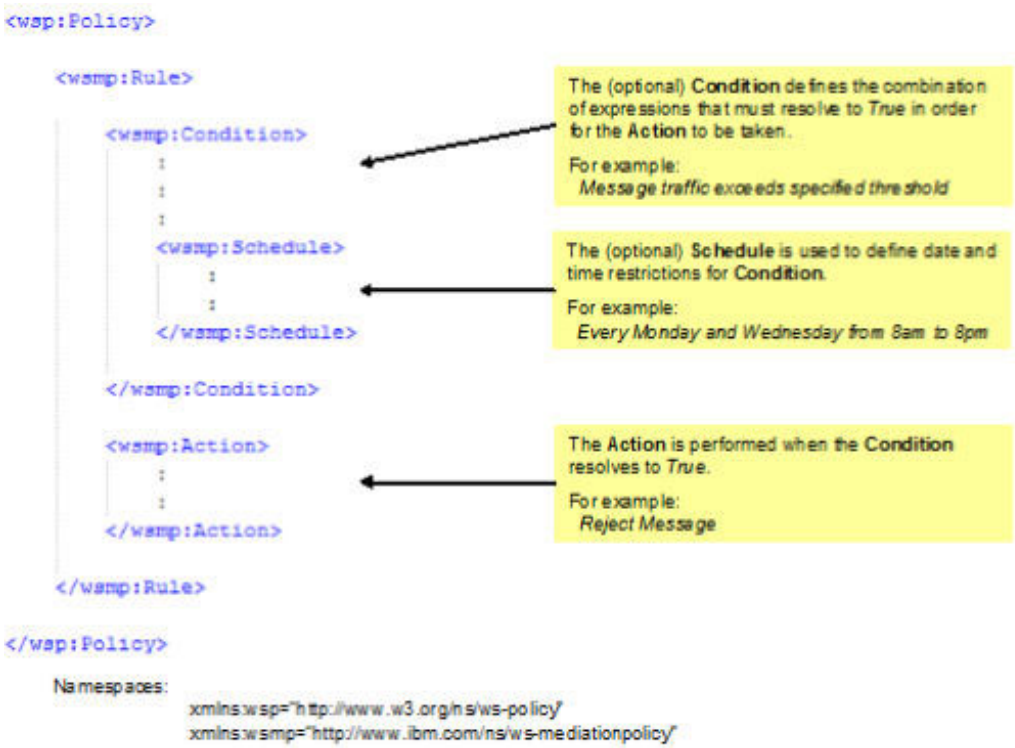


Figura 3. Visión general de la estructura de la política

Adjunto de política

El rol del documento PolicyAttachment es asociar un conjunto de políticas WS-Policy con un punto de conexión de servicio específico para su aplicación, tal como un punto de conexión de servicios web.

Por ejemplo, las plataformas de servicios web pueden dar soporte a puntos de conexión basados en:

- Elementos WSDL Element URI 1.1
- Elementos WS-Addressing

La sintaxis se define en la especificación de WS-PolicyAttachment:

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


    </wsp:AppliesTo>
    <wsp:Policy>


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

Figura 4. Especificación de WS-PolicyAttachment

WSRR expone interfaces REST para adquirir los adjuntos de políticas adecuados en un modelo de SLA. La información sobre el par de consumidor-proveedor al que se aplica la política se pasa al ESB con el formato WS-PolicyAttachment. La sintaxis se define en el WS-PolicyAttachment: Especificación de filtros de contenido de mensaje.

La política se puede especificar para un solo proveedor de servicio, para un par de proveedor-consumidor específico, o para consumidores anónimos. Los consumidores anónimos proporcionan un modo de definir una política predeterminada que solo se aplica a aquellos consumidores a los que no se aplican otras políticas.

En la Figura 4, el asunto de política específico del dominio al que se aplica la política (el proveedor) está contenido en la sección `<wsp:AppliesTo>`. Le sigue el filtro consumer-context al que se aplica la política (el consumidor). A continuación, en la sección `<wsp:Policy>`, se declaran o se hace referencia a la política, o políticas.

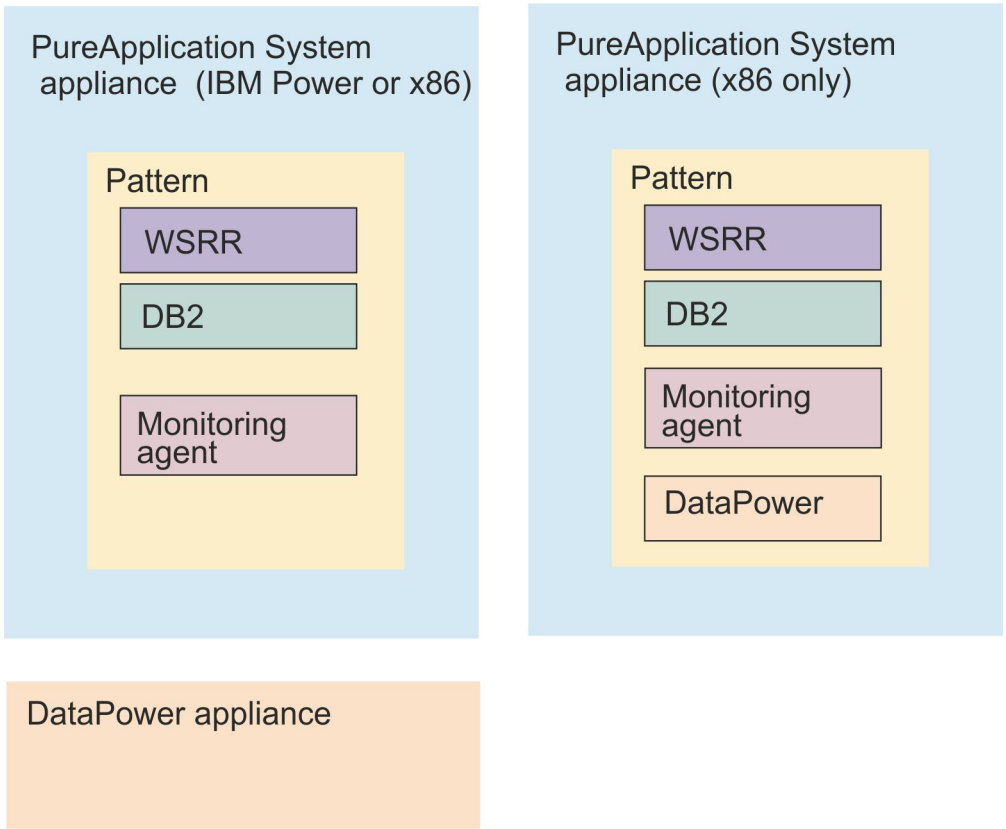
Capítulo 2. Visión general del patrón

El Patrón IBM SOA Policy Gateway es un conjunto de patrones de sistema virtual que proporcionan un punto de aplicación de políticas, un punto de administración de políticas y un punto de supervisión de políticas.

Puede instalar el Patrón IBM SOA Policy Gateway en un dispositivo IBM PureApplication System en arquitecturas IBM Power o x86.

El punto de administración de políticas es proporcionado por patrones de sistema virtual que suministran WSRR en una arquitectura de varios niveles, ofreciendo un entorno de producción y preparación. El punto de aplicación de políticas puede ser proporcionado por un dispositivo WebSphere DataPower. Como alternativa, en x86, PureApplication System puede desplegar una imagen DataPower virtual. En cualquier caso, se crea un dominio durante el despliegue de un patrón de sistema virtual. El punto de supervisión de políticas viene proporcionado por un complemento de supervisión del servicio de supervisión de PureApplication System.

El siguiente diagrama ilustra las prestaciones procedentes del Patrón IBM SOA Policy Gateway



Existen ejemplos de políticas en muchos, si no en todos los servicios de la Arquitectura orientada a servicios (SOA). Los productores y consumidores de servicios acuerdan las funciones, el rendimiento y las características del servicio

durante la fase de diseño. Para implementar estos acuerdos, puede utilizar definiciones de nivel de servicio (SLD) y acuerdos de nivel de servicio (SLA). Utilice el patrón para definir políticas para SLD y SLA de un modo administrado, definido y gobernado de forma eficaz. Los tipos de política que se utilizan en este patrón incluyen las siguientes políticas:

- **Políticas de mediación**:
  - Rechazo: rechazar o regular las solicitudes que llegan a un ritmo mayor que el definido.
  - Registro: crear un mensaje de registro con el punto de aplicación de políticas cuando se invoca un servicio.
  - Transformación.
  - Validación: validar la llamada de servicio por comparación con la definición de servicio.
  - Direccionamiento: basándose en el mensaje, hacer un direccionamiento hacia un punto final específico.
- **Políticas de seguridad**: el ejemplo muestra la aplicación de políticas de seguridad de control de accesos XACML. Estas políticas no están gobernadas dentro del punto de administración de políticas en este momento.
- **Políticas de supervisión**: Puede definir las políticas de supervisión en despliegues de PureApplication System.

El Patrón IBM SOA Policy Gateway contiene los siguientes patrones de sistemas virtuales:

- SOA Policy Gateway Basic Runtime Sample (solo x86)
- SOA Policy Gateway Governance Master
- SOA Policy Gateway Basic Runtime
- SOA Policy Gateway Basic Runtime External DataPower
- SOA Policy Gateway Advanced Runtime
- SOA Policy Gateway Advanced Runtime External DataPower
- System Monitoring for SOA Policy Gateway Pattern 2.5 (un servicio compartido)

Los patrones de sistema virtual trabajan conjuntamente para proporcionar un entorno de gobierno de servicios de varias etapas. El Patrón IBM SOA Policy Gateway también permite proporcionar varios dominios DataPower configurados al entorno de gobierno durante el despliegue del patrón.

Para obtener más información sobre la política SOA, consulte Capítulo 1, “Visión general de la política SOA”, en la página 1.

Conceptos relacionados:

Capítulo 1, “Visión general de la política SOA”, en la página 1
La gestión de políticas juega un papel clave en el gobierno de políticas de modo estructurado y coherente. Las políticas se pueden utilizar para habilitar un mejor gobierno en cualquier entorno orientado a servicios.

“SOA Policy Gateway Basic Runtime External DataPower” en la página 23
El patrón SOA Policy Gateway Basic Runtime External DataPower es el mismo que el patrón Basic Runtime, pero requiere que se especifiquen dispositivos DataPower externos en el despliegue.

“SOA Policy Gateway Basic Runtime Sample (x86)” en la página 19
SOA Policy Gateway Basic Runtime Sample suministra un patrón de tiempo de ejecución básico con una interfaz y aplicación de ejemplo que muestra las políticas actualmente soportadas en este release.

Capítulo 3. Iniciación al Patrón IBM SOA Policy Gateway

Este patrón utiliza WebSphere DataPower para controlar los mensajes utilizando políticas gobernadas y definiciones de servicio en WSRR. Revise los temas de esta sección para saber cómo descargar e instalar el patrón, cómo verificarlo tras la instalación, aceptar licencias y los roles de usuario implicados.

Cómo descargar e instalar los patrones

El Patrón IBM SOA Policy Gateway para utilizar con IBM PureApplication System está empaquetado para su descarga desde Passport Advantage.

Antes de empezar

Descargue el Patrón IBM SOA Policy Gateway a un sistema provisional, que puede ser un sistema Linux o Microsoft Windows. A continuación, ejecute el instalador en el sistema provisional para instalar los patrones en IBM PureApplication System.

Asegúrese de que haya 16 GB de espacio disponible para el archivo `CIQ1LML.tar.gz` (destino Power) o el archivo `CIQ1VML.tar.gz` (destino x86), y 40 GB adicionales para los archivos extraídos. Java™ Runtime Environment (JRE) Versión 6 también debe estar instalado antes de iniciar la instalación del patrón. Puede descargar el JRE para Linux desde la dirección siguiente: http://www.ibm.com/developerworks/java/jdk/linux/download.html

Acerca de esta tarea

El Patrón IBM SOA Policy Gateway está empaquetado en el archivo `CIQ1LML.tar.gz` para un sistema de destino Power, o el archivo `CIQ1VML.tar.gz` para un sistema de destino x86. Este archivo contiene los archivos OVA (Open Virtual Archive), los archivos de paquetes script y los archivos de definiciones de patrones.

Procedimiento

Para descargar las imágenes del Patrón IBM SOA Policy Gateway desde Passport Advantage, realice los pasos siguientes:

1. Acceda al sitio web de Passport Advantage: Passport Advantage.
2. Descargue el archivo de archivado que contiene las imágenes, paquetes script y patrones que se deben utilizar. El nombre del archivo es `CIQ1LML.tar.gz` (destino Power) o `CIQ1VML.tar.gz` (destino x86).
3. Abra un terminal en Linux, o una ventana de indicador de mandatos en Windows y vaya al directorio donde se ha descargado el archivo archive.
4. Extraiga el contenido del archivo en su sistema de archivos local. En Linux, se utiliza el siguiente mandato de extracción:

```
tar xvzf archive_file
```

   En Windows, utilice software de extracción adicional para extraer el contenido del archivo archive.
5. Vaya al directorio `installer`:

```
cd installer
```

6. Para instalar el Patrón IBM SOA Policy Gateway en IBM PureApplication System, ejecute el instalador. El nombre del mandato es `installer.bat` en Microsoft Windows o `installer` en Linux. Escriba el mandato siguiente: `installer -h <host> -u <nombre de usuario> -p <contraseña>` donde `<host>` es IBM PureApplication System, y el nombre de usuario y contraseña son las credenciales del administrador de la nube. Por ejemplo:

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

7. Cuando se le solicite, acepte la licencia del Patrón IBM SOA Policy Gateway.
   a. En Microsoft Windows: después de aceptar el acuerdo de licencia, si una línea nueva en el terminal muestra >>>, escriba `quit()` y pulse la tecla Intro. Repita el paso 7.
8. Se importan los patrones. A medida que se instala cada patrón, se muestra un mensaje en el instalador para indicar que el patrón se ha instalado satisfactoriamente. Por ejemplo:

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

Resultados

Se han cargado los patrones y los scripts se han creado los patrones de sistema virtual.

Nota: Si un patrón de sistema virtual de la versión correcta utilizada en el Patrón IBM SOA Policy Gateway ya existe en el catálogo, no se sobrescribirá.

Qué hacer a continuación

Acepte las licencias en IBM PureApplication System, consulte .

Para validar la instalación, consulte “Verificación del patrón instalado”.

Verificación del patrón instalado

Puede verificar si el patrón se ha instalado correctamente.

Antes de empezar

Asegúrese de que todos los pasos de “Cómo descargar e instalar los patrones” en la página 13 se hayan completado.

Acerca de esta tarea

Después de instalar el patrón, puede verificar la instalación del patrón para asegurarse de que todos los componentes se han instalado correctamente.

Procedimiento

Para verificar la instalación del Patrón IBM SOA Policy Gateway, realice los pasos siguientes :

1. Abra la consola de carga de trabajo en el dispositivo donde se ha instalado el patrón.
2. Verifique las imágenes virtuales navegando a **Catálogo** > **Imágenes virtuales** y localice los siguientes elementos:
   - DB2 Enterprise 10.1.0.2

- WebSphere Service Registry and Repository 8.0.0.2
- WebSphere DataPower X152 Virtual Edition (solo sistemas x86)

3. Vaya a **Catálogo** > **Paquetes script**, y busque:
   - SOA Policy Gateway 2.5.0.0 - Dominio DataPower
   - SOA Policy Gateway 2.5.0.0 - Supervisión de DataPower (solo x86)
   - SOA Policy Gateway 2.5.0.0 - Supervisión de DataPower externa
   - SOA Policy Gateway 2.5.0.0 - Promoción
   - SOA Policy Gateway 2.5.0.0 - Ejemplo (solo x86)
   - SOA Policy Gateway 2.5.0.0 - Seguridad
   - SOA Policy Gateway 2.5.0.0 - Añadir consultas con nombre
   - SOA Policy Gateway 2.5.0.0 - Anular

   Estos paquetes script están todos incluidos en una instalación realizada correctamente.
4. Vaya a **Patrones** > **Sistemas virtuales**. En sistemas x86, localice:
   - SOA Policy Gateway 2.5.0.0 - Tiempo de ejecución avanzado
   - SOA Policy Gateway 2.5.0.0 - DataPower externo de tiempo de ejecución avanzado
   - SOA Policy Gateway 2.5.0.0 - Tiempo de ejecución básico
   - SOA Policy Gateway 2.5.0.0 - DataPower externo de tiempo de ejecución básico
   - SOA Policy Gateway 2.5.0.0 - Ejemplo de tiempo de ejecución básico
   - SOA Policy Gateway 2.5.0.0 - Maestro de gobierno

   En Power Systems, localice:
   - SOA Policy Gateway 2.5.0.0 - Tiempo de ejecución avanzado
   - SOA Policy Gateway 2.5.0.0 - Tiempo de ejecución básico
   - SOA Policy Gateway 2.5.0.0 - Maestro de gobierno

   Estos patrones están todos incluidos en una instalación realizada correctamente.
5. Vaya a **Nube** > **Tipos de patrón** y localice el siguiente elemento:
   - System Monitoring for SOA Policy Gateway Pattern 2.5.0.0

   Este patrón está presente en una instalación correcta.

Resultados

Ha verificado la instalación del Patrón IBM SOA Policy Gateway.

Qué hacer a continuación

Si la instalación se ha realizado satisfactoriamente, puede continuar para aceptar licencias, consulte “Aceptación de licencias”. Si la instalación no se ha realizado satisfactoriamente, repita el paso 7 y pasos subsiguientes del tema “Cómo descargar e instalar los patrones” en la página 13.

Aceptación de licencias

Debe aceptar licencias para componentes instalados recientemente antes de poder trabajar con los patrones.

Antes de empezar

Asegúrese de que todos los pasos de “Cómo descargar e instalar los patrones” en la página 13 se hayan completado.

Acerca de esta tarea

Para poder utilizar una imagen virtual cualquiera, debe aceptar la licencia necesaria correspondiente a ella.

Procedimiento

Para aceptar licencias, complete estos pasos:

1. Abra la consola de carga de trabajo en el dispositivo donde se ha instalado el patrón.
2. Seleccione **Catálogo** > **Imágenes virtuales**.
3. Localice las siguientes imágenes en la lista de **Imágenes virtuales** y confirme que la licencia se ha aceptado en el panel detalles, si no, pulse 'aceptar' para ver y aceptar la licencia. Para sistemas x86:
   - WebSphere DataPower XI52 Virtual Edition, Versión 6.0.0.0 - Número de referencia de imagen: XI52.6.0.0.0231528 (2013/06/16 14:14:19)
   - WebSphere Service Registry and Repository 8.0.0.2 - Número de referencia de imagen: 201309062038
   - DB2 Enterprise 10.1.0.2 - Número de referencia de imagen: 39
   - IBM OS Image for Red Hat Linux Systems, versión 2.0.0.3 - Número de referencia de imagen: 136

   Para sistemas Power:
   - WebSphere Service Registry and Repository 8.0.0.2 - Número de referencia de imagen: 201309080001
   - DB2 Enterprise 10.1.0.2 - Número de referencia de imagen: 50
   - IBM OS Image for AIX Systems versión 2.0.0.2 - Número de referencia de imagen: 126
4. Para aceptar una licencia, pulse la imagen para ver sus detalles. Se visualiza el estado. Pulse **Aceptar** para el Acuerdo de licencia, y luego pulse cualquiera de las licencias que deban aceptarse antes de utilizar la imagen virtual. El estado muestra **Solo lectura** y el Acuerdo de licencia muestra **Aceptado** cuando se completa. Si no se acepta una licencia, el icono de imagen contiene un recuadro rojo con una cruz.

Resultados

Ha aceptado las licencias para el Patrón IBM SOA Policy Gateway.

Qué hacer a continuación

Si la instalación se ha realizado satisfactoriamente y ha aceptado todas las licencias, puede continuar trabajando con el patrón, consulte Capítulo 5, “Trabajar con el Patrón IBM SOA Policy Gateway”, en la página 45. Si la instalación no se ha realizado satisfactoriamente, repita el paso 7 y pasos subsiguientes del tema “Cómo descargar e instalar los patrones” en la página 13.

Configuración del acceso de usuario

Para que los usuarios puedan acceder a las imágenes y patrones en el dispositivo, en primer lugar, el administrador de dispositivos debe permitir el acceso de usuario. Puede crear primero los usuarios y después añadir los usuarios al grupo o puede crear primero el grupo y luego crear los usuarios y añadirlos al grupo.

Acerca de esta tarea

Los usuarios administrativos, normalmente el administrador de dispositivos, pueden añadir otros usuarios para que accedan y administren los patrones. Esto se hace utilizando la consola del sistema.

Procedimiento

Para configurar el acceso de los usuarios, efectué los pasos siguientes:

1. Seleccione una de las opciones siguientes para configurar los usuarios y, opcionalmente, los grupos de usuarios:
   - Añada y configure un usuario desde la ventana Usuarios de la consola.
     a. En el menú pulse **Sistema** > **Usuarios**.
     b. Pulse el icono **Añadir**.
     c. Proporcione un nombre de usuario corto, así como el nombre real del usuario, la dirección de correo electrónico, y las contraseñas y pulse **Aceptar**.
     d. Seleccione el usuario que ha añadido en el panel Usuarios para configurar el acceso. Configure el acceso y las acciones del usuario que ha seleccionado.
     e. Añada el usuario a uno o varios grupos en el campo **Grupos de usuarios**.
   - Cree un grupo de usuarios.
     a. En el menú pulse **Sistema** > **Grupos de usuarios**.
     b. Pulse el icono **Añadir**. Proporcione un nombre y una descripción para el grupo.
     c. Seleccione el grupo que ha añadido en el panel Grupos de usuarios para configurar el acceso.
     d. Añada los miembros en el campo **Grupo de miembros** y proporcione los permisos que se aplicarán al grupo.
2. Opcional: Si ya ha añadido las imágenes virtuales, proporcione acceso a las imágenes virtuales a los usuarios o al grupo. Cambie a la consola de carga de trabajo y pulse **Patrones** > **Sistemas virtuales** para abrir la ventana de patrones de sistemas virtuales. Seleccione una imagen virtual de Patrón IBM SOA Policy Gateway para visualizar sus detalles. Añada los usuarios o grupo en el campo **Acceso otorgado a**.

Qué hacer a continuación

Si todavía no se han añadido las imágenes virtuales, añádalas y, a continuación, proporcione acceso a las mismas a los usuarios o al grupo.

Información relacionada:

IBM PureApplication System: Gestión de usuarios y grupos

Capítulo 4. Patrones, componentes y paquetes script

Un patrón proporciona una definición de topología para un despliegue repetible que puede compartirse. Los componentes de Patrón IBM SOA Policy Gateway son los componentes funcionales del patrón. Cada componente representa una única máquina virtual.

Los patrones describen la función que proporciona cada máquina virtual de un sistema virtual. Cada función se identifica como un componente del patrón. Los patrones asumen las características de sus componentes asociados. Por ejemplo, cuando un componente de WSRR se coloca en un patrón, que posteriormente se despliega, el resultado es una máquina virtual que tiene una instancia de WSRR en ejecución.

Patrones

Cuando las imágenes virtuales se cargan en IBM PureApplication System, y se asigna acceso a los usuarios, los usuarios pueden empezar a trabajar con los patrones.

Los patrones proporcionan una topología repetible que puede desplegarse en una nube. Los patrones desplegados son sistemas virtuales que se ejecutan en la nube. Los patrones, tanto si son predefinidos como si se han creado, contienen componentes. Algunos componentes son necesarios para que el patrón funcione cuando se despliega en la nube como un sistema virtual.

SOA Policy Gateway Basic Runtime Sample (x86)

SOA Policy Gateway Basic Runtime Sample suministra un patrón de tiempo de ejecución básico con una interfaz y aplicación de ejemplo que muestra las políticas actualmente soportadas en este release.

El patrón SOA Policy Gateway Basic Runtime Sample solo está disponible en sistemas x86 disponibles.

El patrón SOA Policy Gateway Basic Runtime Sample tiene los siguientes componentes:

- Servidor WSRR autónomo
- DB2 Enterprise
- DataPower

El patrón SOA Policy Gateway Basic Runtime Sample instala una aplicación de ejemplo en el entorno desplegado. El patrón instala un dominio de ejemplo en DataPower que implementa un servicio de ejemplo, instala WSDL de ejemplo y políticas asociadas en WSRR para el servicio, y proporciona una aplicación de prueba para mostrar las políticas aplicadas. Para obtener más información sobre la aplicación de ejemplo, consulte “La aplicación de ejemplo” en la página 58. Instala un dominio de ejemplo dentro de DataPower, instala el WSDL de ejemplo y las Políticas en WSRR y muestra varias políticas para un servicio.

El siguiente diagrama muestra el ejemplo de tiempo de ejecución básico.

Figura 5. Configuración PureApplication Server con DataPower VM (solo x86)

Las políticas implementadas son:

Tabla 1. Políticas incluidas en el patrón Tiempo de ejecución básico con ejemplo

Tipo de política	Descripción
Registro	Basado en un ID de contexto de solicitud, registra la solicitud en DataPower.
Direccionamiento	Basado en un ID de contexto de solicitud, registra la solicitud en un punto final especificado.
Validación	Valida la solicitud en base al WSDL de las implementaciones de servicio.
Rechazo	Controla las solicitudes para un servicio basándose en el recuento de mensajes con acciones: rechazar, poner en cola y otros.
Seguridad AAA	Controla el acceso al servicio utilizando la autorización de usuario basada en XACML. El XACML no se almacena en WSRR.
Redacción de la seguridad	Redacta los componentes del mensaje de respuesta basado en XACML. El XACML no se almacena en WSRR.

Scripts y opciones avanzadas

El patrón requiere los scripts siguientes.

En el componente Servidor autónomo de WSRR:
- SOA Policy Gateway 2.5.0.0 - Ejemplo

Consulte los parámetros de componentes y scripts:
- "Componente DB2 Enterprise" en la página 28
- "Componente Servidor WSRR autónomo" en la página 34
- "Componente DataPower" en la página 37
- "Script: SOA Policy Gateway 2.5.0.0 - Ejemplo" en la página 40

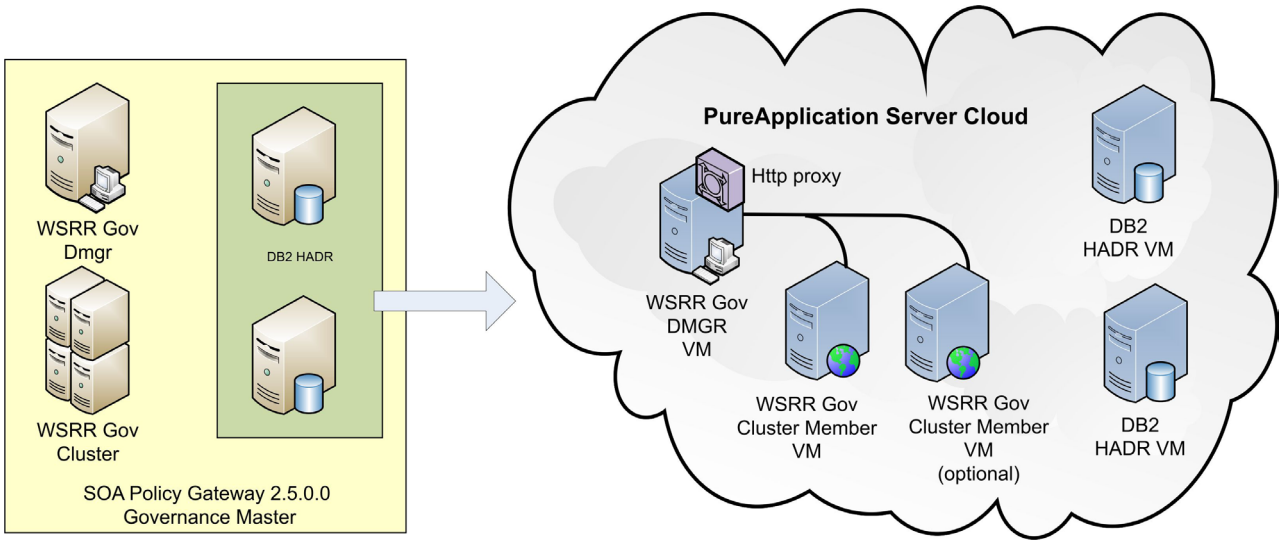
SOA Policy Gateway Governance Master

El patrón SOA Policy Gateway Governance Master proporciona un entorno de gobierno en clúster para crear y gestionar servicios y políticas. El entorno se suministra con el perfil de habilitación de gobierno predeterminado de WSRR configurado. El perfil de habilitación de gobierno predeterminado soporta dos destinos de promoción: Transición y Producción.

El patrón SOA Policy Gateway Governance Master requiere los siguientes componentes:
- DB2 HADR Primary
- DB2 HADR Standby
- Gestor de despliegue de WSRR
- Nodos personalizados de WSRR

Nota: El patrón Maestro de gobierno se debe desplegar antes de que se desplieguen los patrones de tiempo de ejecución. Los parámetros que se utilizan

para configurar el patrón Maestro de gobierno son utilizados por los patrones de tiempo de ejecución para configurarse en el Maestro de gobierno.



Parámetros de componente

Consulte los parámetros de componentes:

- "Componente DB2 Enterprise HADR Primary" en la página 30
- "Componente DB2 Enterprise HADR Standby" en la página 32
- "Componente Gestor de despliegue de WSRR" en la página 35
- "Componente Nodos personalizados de WSRR" en la página 36
- "Script: SOA Policy Gateway 2.5.0.0 - Seguridad" en la página 41
- "Script: SOA Policy Gateway 2.5.0.0 - Promoción" en la página 39

Utilizando el patrón de gobierno como un maestro de gobierno

El patrón SOA Policy Gateway Governance Master se despliega con el perfil de habilitación de gobierno de WSRR predeterminado, que incluye dos etapas de promoción: Transición y Producción. Para obtener más información sobre el perfil de habilitación de gobierno en WSRR, consulte Information Center de IBM WebSphere Service Registry and Repository, Versión 8.0 - Perfil de habilitación de gobierno. Los patrones Basic Runtime o Advanced Runtime pueden desplegarse en esta integración como destinos de promoción. Para obtener más información sobre cómo configurar destinos de promoción, consulte "Cómo añadir un entorno de ejecución adicional" en la página 55.

Información relacionada:

Information Center de IBM WebSphere Service Registry and Repository, Versión 8.0 - Perfil de habilitación de gobierno

SOA Policy Gateway Basic Runtime

El patrón SOA Policy Gateway Basic Runtime es la forma más sencilla para proporcionar un entorno de ejecución SOA Policy Gateway, incluye dos instancias DataPower (solo x86), una instancia WSRR autónoma, una instancia DB2 autónoma, y una instancia Base OS (para alojar los agentes de supervisión DataPower).

Nota: En este tema se describe el patrón disponible en x86. Para el patrón IBM Power, consulte "SOA Policy Gateway Basic Runtime External DataPower" en la página 23.

El patrón SOA Policy Gateway Basic Runtime requiere los siguientes componentes:

- Servidor WSRR autónomo
- DB2 Enterprise
- WebSphere DataPower X152 Virtual Edition
- Supervisión SOA para DataPower (en un componente Core OS)

El siguiente diagrama muestra la configuración de un patrón SOA Policy Gateway Basic Runtime.

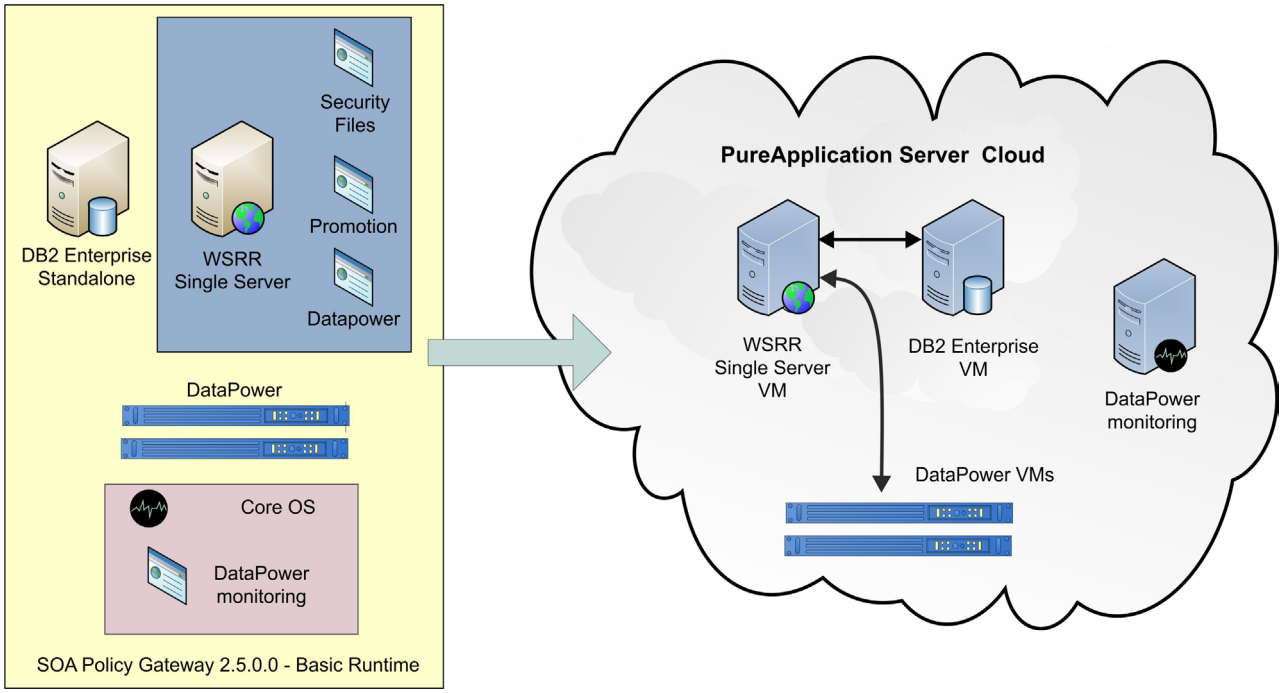


Figura 6. Configuración PureApplication Server con DataPower VM

Scripts y opciones avanzadas

El patrón requiere entrada de usuario a los siguientes scripts en tiempo de despliegue.

En el componente Servidor autónomo de WSRR:

- SOA Policy Gateway 2.5.0.0 - Seguridad
- SOA Policy Gateway 2.5.0.0 - Promoción
- SOA Policy Gateway 2.5.0.0 - Dominio DataPower

En el componente Core OS:

- SOA Policy Gateway 2.5.0.0 - Supervisión DataPower

Consulte los parámetros de componentes y scripts:

- "Componente Servidor WSRR autónomo" en la página 34
- "Componente DB2 Enterprise" en la página 28

- "Componente DataPower" en la página 37
- "Script: SOA Policy Gateway 2.5.0.0 - Seguridad" en la página 41
- "Script: SOA Policy Gateway 2.5.0.0 - Promoción" en la página 39
- "Script: SOA Policy Gateway 2.5.0.0 - Dominio DataPower" en la página 38
- "Script: SOA Policy Gateway 2.5.0.0 - Supervisión de DataPower (solo x86)" en la página 41

Configuración del tiempo de ejecución básico con un maestro de gobierno

Cuando se configura un patrón de tiempo de ejecución básico con un patrón de maestro de gobierno, se producen las siguientes acciones:

- Se configura la seguridad entre células
- El archivo `promotion.xml` en el maestro de gobierno se actualiza con los datos de despliegue para el despliegue de tiempo de ejecución básico.

Para configurar la promoción, deberá elegir una de las siguientes opciones de transición:

- producción
- transición

Estas opciones se alinean con los niveles proporcionados por el perfil de habilitación de gobierno en WSRR. Para obtener más información sobre el perfil de habilitación de gobierno en WSRR, consulte Information Center de IBM WebSphere Service Registry and Repository, Versión 8.0 - Perfil de habilitación de gobierno.

Nota: Puede utilizar este patrón para suministrar un sistema autónomo, sin maestro de administración. Para hacer esto, debe especificar los parámetros de gobierno maestro como "Sin definir" al desplegar el patrón. Estos valores provocan que el script de promoción genere un error durante el despliegue, y el despliegue se muestra como **fallido**, pero puede ignorar el error.

SOA Policy Gateway Basic Runtime External DataPower

El patrón SOA Policy Gateway Basic Runtime External DataPower es el mismo que el patrón Basic Runtime, pero requiere que se especifiquen dispositivos DataPower externos en el despliegue.

Nota: Esta descripción se aplica al patrón en sistemas IBM Power.

El patrón SOA Policy Gateway Basic Runtime External DataPower tiene los siguientes componentes:

- Servidor WSRR autónomo
- DB2 Enterprise
- Supervisión SOA para DataPower (en un componente Core OS)

El siguiente diagrama muestra la configuración de un patrón SOA Policy Gateway Basic Runtime External DataPower.

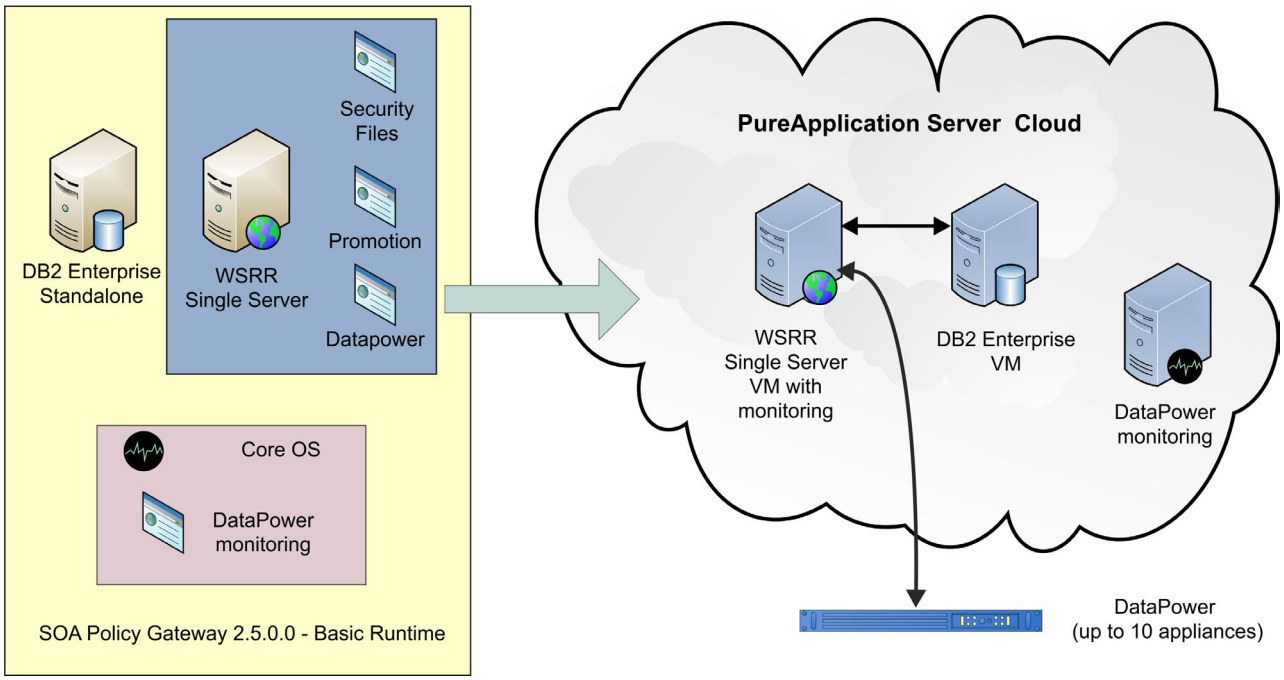


Figura 7. Configuración de PureApplication Server con el dispositivo DataPower

Scripts y opciones avanzadas

El patrón requiere entrada de usuario a los siguientes scripts en tiempo de despliegue.

En el componente Servidor autónomo de WSRR:

- SOA Policy Gateway 2.5.0.0 - Seguridad
- SOA Policy Gateway 2.5.0.0 - Promoción
- SOA Policy Gateway 2.5.0.0 - Dominio DataPower

En el componente Core OS:

- SOA Policy Gateway 2.5.0.0 - Supervisión DataPower

Consulte los parámetros de componentes y scripts:

- “Componente Servidor WSRR autónomo” en la página 34
- “Componente DB2 Enterprise” en la página 28
- “Script: SOA Policy Gateway 2.5.0.0 - Seguridad” en la página 41
- “Script: SOA Policy Gateway 2.5.0.0 - Promoción” en la página 39
- “Script: SOA Policy Gateway 2.5.0.0 - Dominio DataPower” en la página 38
- “Script: SOA Policy Gateway 2.5.0.0 - Supervisión de DataPower (solo x86)” en la página 41

Configuración del tiempo de ejecución básico con un maestro de gobierno

Cuando se configura un patrón de tiempo de ejecución básico con un patrón de maestro de gobierno, se producen las siguientes acciones:

- Se configura la seguridad entre células

- El archivo `promotion.xml` en el maestro de gobierno se actualiza con los datos de despliegue para el despliegue de tiempo de ejecución básico.

Para configurar la promoción, deberá elegir una de las siguientes opciones de transición:

- producción
- transición

Estas opciones se alinean con los niveles proporcionados por el perfil de habilitación de gobierno en WSRR. Si el perfil de gobierno difiere, se elige "otros" cuando se cambia el perfil de gobierno del maestro de gobierno. Para obtener más información sobre el perfil de habilitación de gobierno en WSRR, consulte Information Center de IBM WebSphere Service Registry and Repository, Versión 8.0 - Perfil de habilitación de gobierno.

Nota: Puede utilizar este patrón para suministrar un sistema autónomo, sin maestro de administración. Para hacer esto, debe especificar los parámetros de gobierno maestro como "Sin definir" al desplegar el patrón. Estos valores provocan que el script de promoción genere un error durante el despliegue, y el despliegue se muestra como **fallido**, pero puede ignorar el error.

SOA Policy Gateway Advanced Runtime

SOA Policy Gateway Advanced Runtime incluye dos instancias de servidor DB2 en una configuración HADR, y un clúster WSRR con un gestor de despliegue y dos nodos personalizados.

Nota: En este tema se describe el patrón disponible en x86. Para el patrón IBM Power, consulte "SOA Policy Gateway Advanced Runtime External DataPower" en la página 26.

El patrón requiere los siguientes componentes:

- Gestor de despliegue de WSRR
- Nodos personalizados de WSRR
- DB2 HADR Primary
- DB2 HADR Standby
- WebSphere DataPower X152 Virtual Edition
- Supervisión SOA para DataPower (en un componente Core OS)

El siguiente diagrama muestra la configuración de un sistema de tiempo de ejecución avanzado.

Figura 8. Configuración PureApplication Server con DataPower VM

Scripts y opciones avanzadas

El patrón requiere entrada de usuario a los siguientes scripts en tiempo de despliegue:

En el componente de gestor de despliegue de WSRR:

- SOA Policy Gateway 2.5.0.0 - Seguridad
- SOA Policy Gateway 2.5.0.0 - Promoción
- SOA Policy Gateway 2.5.0.0 - Dominio DataPower

En el componente Core OS:

- SOA Policy Gateway 2.5.0.0 - Supervisión DataPower

Consulte los parámetros de componentes y scripts:

- "Componente DB2 Enterprise HADR Primary" en la página 30
- "Componente DB2 Enterprise HADR Standby" en la página 32
- "Componente Gestor de despliegue de WSRR" en la página 35
- "Componente Nodos personalizados de WSRR" en la página 36
- "Script: SOA Policy Gateway 2.5.0.0 - Promoción" en la página 39
- "Script: SOA Policy Gateway 2.5.0.0 - Dominio DataPower" en la página 38
- "Script: SOA Policy Gateway 2.5.0.0 - Supervisión de DataPower (solo x86)" en la página 41

Configuración del tiempo de ejecución de avanzado con un maestro de gobierno

Cuando se configura un patrón de tiempo de ejecución avanzado con un patrón maestro de gobierno, se producen las siguientes acciones:

- Se configura la seguridad entre células
- El archivo `promotion.xml` en el maestro de gobierno se actualiza con los datos procedentes del despliegue de tiempo de ejecución avanzado.

Para configurar la promoción, deberá elegir una de las siguientes opciones de transición:

- producción
- transición

Estas opciones se alinean con los niveles proporcionados por el perfil de habilitación de gobierno en WSRR. Para obtener más información sobre el perfil de habilitación de gobierno en WSRR, consulte Information Center de IBM WebSphere Service Registry and Repository, Versión 8.0 - Perfil de habilitación de gobierno.

SOA Policy Gateway Advanced Runtime External DataPower

SOA Policy Gateway Advanced Runtime External DataPower es el mismo patrón que Advanced Runtime, pero requiere que se especifiquen dispositivos DataPower externos en el despliegue.

Nota: Esta descripción se aplica al patrón SOA Policy Gateway Advanced Runtime en sistemas IBM Power.

El patrón SOA Policy Gateway Advanced Runtime External DataPower necesita los componentes siguientes:

- Gestor de despliegue de WSRR
- Nodos personalizados de WSRR
- DB2 HADR Primary
- DB2 HADR Standby
- Supervisión SOA para DataPower (en un componente Core OS)

El siguiente diagrama muestra la configuración de un sistema de tiempo de ejecución avanzado.

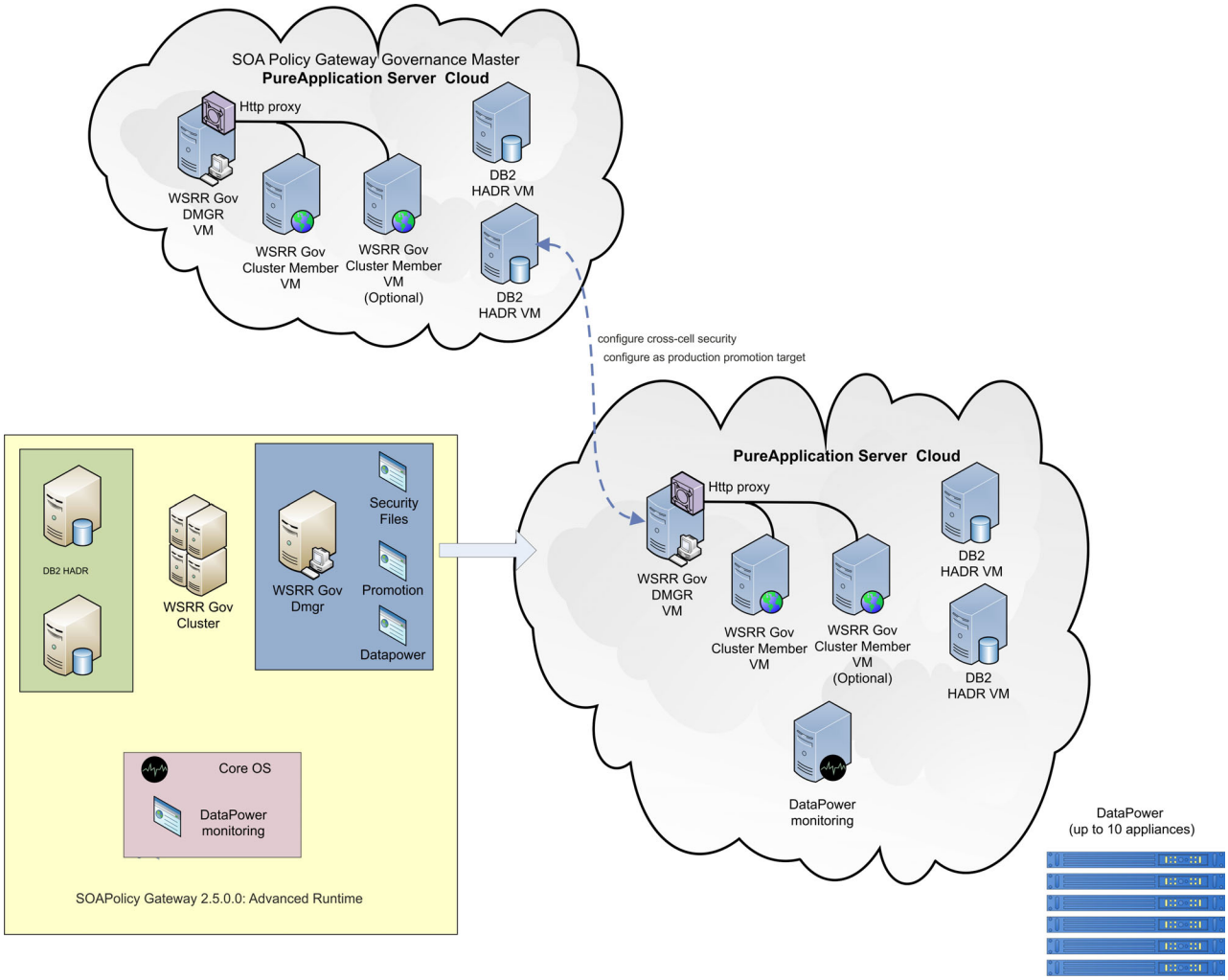


Figura 9. Configuración PureApplication Server con dispositivos DataPower

Scripts y opciones avanzadas

El patrón requiere entrada de usuario a los siguientes scripts en tiempo de despliegue.

En el componente de gestor de despliegue de WSRR:

- SOA Policy Gateway 2.5.0.0 - Seguridad
- SOA Policy Gateway 2.5.0.0 - Promoción
- SOA Policy Gateway 2.5.0.0 - Dominio DataPower

En el componente Core OS:

- SOA Policy Gateway 2.5.0.0 - Supervisión DataPower

Consulte los parámetros de componentes y scripts:

- "Componente DB2 Enterprise HADR Primary" en la página 30
- "Componente DB2 Enterprise HADR Standby" en la página 32
- "Componente Gestor de despliegue de WSRR" en la página 35
- "Componente Nodos personalizados de WSRR" en la página 36
- "Script: SOA Policy Gateway 2.5.0.0 - Promoción" en la página 39

- "Script: SOA Policy Gateway 2.5.0.0 - Dominio DataPower" en la página 38
- "Script: SOA Policy Gateway 2.5.0.0 - Supervisión de DataPower (solo x86)" en la página 41

Configuración del tiempo de ejecución de avanzado con un maestro de gobierno

Cuando se configura un patrón de tiempo de ejecución avanzado con un patrón maestro de gobierno, se produce lo siguiente:

- Se configura la seguridad entre células
- Se actualiza el archivo `promotion.xml` del maestro de gobierno con los datos de despliegue del Tiempo de ejecución avanzado.

Para configurar la promoción, deberá elegir una de las siguientes opciones de transición:

- producción
- transición

Estas opciones se alinean con los niveles proporcionados por el perfil de habilitación de gobierno en WSRR. Para obtener más información sobre el perfil de habilitación de gobierno en WSRR, consulte Information Center de IBM WebSphere Service Registry and Repository, Versión 8.0 - Perfil de habilitación de gobierno.

Servicio compartido

El patrón incluye un servicio compartido que utilizan los patrones desplegados para proporcionar supervisión.

Supervisión del sistema para SOA Policy Gateway

El servicio compartido de supervisión del sistema para SOA Policy Gateway proporciona los componentes de supervisión para SOA Policy Gateway.

La supervisión en los patrones de tiempo de ejecución básico y avanzado se proporciona mediante el servicio de supervisión DataPower que se ejecuta en un componente Core OS. El propio servicio de supervisión utiliza componentes ITCAM for SOA que se incluyen en la supervisión del sistema para el patrón SOA Policy Gateway. La supervisión de las instancias WSRR también requiere que se ejecute la supervisión del sistema para el servicio compartido de WebSphere Application Server.

Siga el enlace relacionado para obtener la documentación detallada de ITCAM for SOA.

Información relacionada:

Documentación de ITCAM for SOA 7.2.1 (desde Fix Central)

Componentes

El Patrón IBM SOA Policy Gateway consta de los componentes siguientes.

Componente DB2 Enterprise

El componente DB2 Enterprise proporciona algunas opciones de configuración.

Los parámetros configurables de la imagen del sistema virtual de DB2 Enterprise 10.1.0.2 se describen en la siguiente tabla:

Tabla 2. Parámetros configurables

Nombre del parámetro	Valor predeterminado	Descripción
CPU virtuales	1	El número de procesadores virtuales asignado a la máquina virtual que representa este componente.
Tamaño de la memoria (MB)	2048	La cantidad de memoria asignada a esta máquina virtual, en megabytes.
Grupo de propietarios de la instancia	db2iadm1	El grupo al que pertenece el propietario de la instancia de DB2.
Propietario de la instancia	db2inst1	El ID del propietario de instancia de DB2. Este ID de usuario se utiliza como propietario de instalación de la instancia de DB2 y como propietario de las bases de datos y esquemas.
Contraseña (Propietario de instancia)	contraseña	La contraseña para el ID de usuario db2inst1 del sistema operativo.
Verificar contraseña	contraseña	Verifica la contraseña de propietario de instancia.
Grupo de usuario delimitado	db2fadm1	El grupo al que pertenece el propietario delimitado de DB2.
Usuario delimitado	db2fenc1	El ID de usuario delimitado de DB2. El ID de usuario delimitado se utiliza para ejecutar las funciones definidas por el usuario (UDF) y procedimientos almacenados fuera del espacio de dirección que utiliza la base de datos DB2. El usuario delimitado es un usuario bajo el que se pueden ejecutar procedimientos almacenados "delimitados" con una autorización reducida en el sistema operativo.
Contraseña (db2fenc1)		La contraseña para el ID de usuario delimitado
Verificar contraseña		Verifica la contraseña de usuario delimitado.
Grupo de usuarios de DAS	dasadm1	El grupo al que pertenece el propietario de DB2 DAS.
Usuario de DAS	dasusr1	El ID de usuario del usuario de servidor de administración de DB2 que se utiliza para ejecutar el servidor de administración de DB2 del sistema. Este ID de usuario también lo utilizan las herramientas de la GUI de DB2 para llevar a cabo tareas de administración en las bases de datos y las instancias de la base de datos del servidor local.
Contraseña (usuario de DAS)	contraseña	La contraseña del usuario de DAS.
Verificar contraseña	contraseña	Verifica la contraseña dasusr1.

Tabla 2. Parámetros configurables (continuación)

Nombre del parámetro	Valor predeterminado	Descripción
Puerto de servicio de DB2	50000	El puerto está bloqueado y no puede modificarse.
Creación de la base de datos	Crear base de datos nueva	Este valor está bloqueado y no puede modificarse.
Nombre para la nueva base de datos	WSRR	Este valor está bloqueado y no puede modificarse.
Conjunto de códigos para la nueva base de datos	UTF-8	
Territorio para la nueva base de datos	US	
Ordenación para la nueva base de datos	SYSTEM	
Tamaño de página para la nueva base de datos	32768	Este valor está bloqueado y no puede modificarse.
Modalidad de compatibilidad de DB2	Predeterminado	Este valor está bloqueado y no puede modificarse.
Configure todos los discos RAW para su uso por DB2	NO	
Contraseña (root)		La contraseña para el ID de usuario root. Este es la contraseña para el sistema operativo de la máquina virtual que está representado por esta parte en el patrón.
Verificar contraseña		Verifica la contraseña root.
Contraseña (virtuser)		La contraseña para el ID de usuario virtuser del sistema operativo. Este ID de usuario se utiliza como un ID de usuario no root para la máquina virtual.
Verificar contraseña		Verifica la contraseña virtuser.
Habilitar VNC	True	Este valor está bloqueado y no puede modificarse.

Componente DB2 Enterprise HADR Primary

El componente DB2 Enterprise HADR Primary proporciona algunas opciones de configuración.

En la tabla siguiente se describen los parámetros configurables del componente DB2 Enterprise HADR Primary:

Tabla 3. Parámetros configurables

Nombre del parámetro	Valor predeterminado	Descripción
CPU virtuales	1	El número de procesadores virtuales asignado a la máquina virtual que representa este componente.
Tamaño de la memoria (MB)	2048	La cantidad de memoria asignada a esta máquina virtual, en megabytes.
Grupo de propietarios de la instancia	db2iadm1	El grupo al que pertenece el propietario de la instancia de DB2.

Tabla 3. Parámetros configurables (continuación)

Nombre del parámetro	Valor predeterminado	Descripción
Propietario de la instancia	db2inst1	El ID del propietario de instancia de DB2. Este ID de usuario se utiliza como propietario de instalación de la instancia de DB2 y como propietario de las bases de datos y esquemas.
Contraseña (Propietario de instancia)	contraseña	La contraseña para el ID de usuario db2inst1 del sistema operativo.
Verificar contraseña	contraseña	Verifica la contraseña de propietario de instancia.
Grupo de usuario delimitado	db2fadm1	El grupo al que pertenece el propietario delimitado de DB2.
Usuario delimitado	db2fenc1	El ID de usuario delimitado de DB2. El ID de usuario delimitado se utiliza para ejecutar las funciones definidas por el usuario (UDF) y procedimientos almacenados fuera del espacio de dirección que utiliza la base de datos DB2. El usuario delimitado es un usuario bajo el que se pueden ejecutar procedimientos almacenados "delimitados" con una autorización reducida en el sistema operativo.
Contraseña (db2fenc1)		La contraseña para el ID de usuario delimitado
Verificar contraseña		Verifica la contraseña de usuario delimitado.
Grupo de usuarios de DAS	dasadm1	El grupo al que pertenece el propietario de DB2 DAS.
Usuario de DAS	dasusr1	El ID de usuario del usuario de servidor de administración de DB2 que se utiliza para ejecutar el servidor de administración de DB2 del sistema. Este ID de usuario también lo utilizan las herramientas de la GUI de DB2 para llevar a cabo tareas de administración en las bases de datos y las instancias de la base de datos del servidor local.
Contraseña (usuario de DAS)	contraseña	La contraseña del usuario de DAS.
Verificar contraseña	contraseña	Verifica la contraseña dasusr1.
Puerto de servicio de DB2	50000	El puerto está bloqueado y no puede modificarse.
Creación de la base de datos	Crear base de datos nueva	Este valor está bloqueado y no puede modificarse.
Nombre para la nueva base de datos	WSRR	Este valor está bloqueado y no puede modificarse.
Conjunto de códigos para la nueva base de datos	UTF-8	
Territorio para la nueva base de datos	US	

Tabla 3. Parámetros configurables (continuación)

Nombre del parámetro	Valor predeterminado	Descripción
Ordenación para la nueva base de datos	SYSTEM	
Tamaño de página para la nueva base de datos	32768	Este valor está bloqueado y no puede modificarse.
Modalidad de compatibilidad de DB2	Predeterminado	Este valor está bloqueado y no puede modificarse.
Configure todos los discos RAW para su uso por DB2	NO	
Contraseña (root)		La contraseña para el ID de usuario root. Este es la contraseña para el sistema operativo de la máquina virtual que está representado por esta parte en el patrón.
Verificar contraseña		Verifica la contraseña root.
Contraseña (virtuser)		La contraseña para el ID de usuario virtuser del sistema operativo. Este ID de usuario se utiliza como un ID de usuario no root para la máquina virtual.
Verificar contraseña		Verifica la contraseña virtuser.
Habilitar VNC	True	Este valor está bloqueado y no puede modificarse.

Los demás parámetros se heredan del patrón del sistema virtual base y están bloqueados.

Componente DB2 Enterprise HADR Standby

El componente DB2 Enterprise HADR Standby proporciona algunas opciones de configuración.

Tabla 4. Parámetros configurables

Nombre del parámetro	Valor predeterminado	Descripción
CPU virtuales	1	El número de procesadores virtuales asignado a la máquina virtual que representa este componente.
Tamaño de la memoria (MB)	2048	La cantidad de memoria asignada a esta máquina virtual, en megabytes.
Grupo de propietarios de la instancia	db2iadm1	El grupo al que pertenece el propietario de la instancia de DB2.
Propietario de la instancia	db2inst1	El ID del propietario de instancia de DB2. Este ID de usuario se utiliza como propietario de instalación de la instancia de DB2 y como propietario de las bases de datos y esquemas.
Contraseña (Propietario de instancia)	contraseña	La contraseña para el ID de usuario db2inst1 del sistema operativo.
Verificar contraseña	contraseña	Verifica la contraseña de propietario de instancia.
Grupo de usuario delimitado	db2fadm1	El grupo al que pertenece el propietario delimitado de DB2.

Tabla 4. Parámetros configurables (continuación)

Nombre del parámetro	Valor predeterminado	Descripción
Usuario delimitado	db2fenc1	El ID de usuario delimitado de DB2. El ID de usuario delimitado se utiliza para ejecutar las funciones definidas por el usuario (UDF) y procedimientos almacenados fuera del espacio de dirección que utiliza la base de datos DB2. El usuario delimitado es un usuario bajo el que se pueden ejecutar procedimientos almacenados "delimitados" con una autorización reducida en el sistema operativo.
Contraseña (db2fenc1)		La contraseña para el ID de usuario delimitado
Verificar contraseña		Verifica la contraseña de usuario delimitado.
Grupo de usuarios de DAS	dasadm1	El grupo al que pertenece el propietario de DB2 DAS.
Usuario de DAS	dasusr1	El ID de usuario del usuario de servidor de administración de DB2 que se utiliza para ejecutar el servidor de administración de DB2 del sistema. Este ID de usuario también lo utilizan las herramientas de la GUI de DB2 para llevar a cabo tareas de administración en las bases de datos y las instancias de la base de datos del servidor local.
Contraseña (usuario de DAS)	contraseña	La contraseña del usuario de DAS.
Verificar contraseña	contraseña	Verifica la contraseña dasusr1.
Puerto de servicio de DB2	50000	El puerto está bloqueado y no puede modificarse.
Creación de la base de datos	Crear base de datos nueva	Este valor está bloqueado y no puede modificarse.
Nombre para la nueva base de datos	WSRR	Este valor está bloqueado y no puede modificarse.
Conjunto de códigos para la nueva base de datos	UTF-8	
Territorio para la nueva base de datos	US	
Ordenación para la nueva base de datos	SYSTEM	
Tamaño de página para la nueva base de datos	32768	Este valor está bloqueado y no puede modificarse.
Modalidad de compatibilidad de DB2	Predeterminado	Este valor está bloqueado y no puede modificarse.
Configure todos los discos RAW para su uso por DB2	NO	

Tabla 4. Parámetros configurables (continuación)

Nombre del parámetro	Valor predeterminado	Descripción
Contraseña (root)		La contraseña para el ID de usuario root. Este es la contraseña para el sistema operativo de la máquina virtual que está representado por esta parte en el patrón.
Verificar contraseña		Verifica la contraseña root.
Contraseña (virtuser)		La contraseña para el ID de usuario virtuser del sistema operativo. Este ID de usuario se utiliza como un ID de usuario no root para la máquina virtual.
Verificar contraseña		Verifica la contraseña virtuser.
Habilitar VNC	True	Este valor está bloqueado y no puede modificarse.

Los demás parámetros se heredan del patrón del sistema virtual base y están bloqueados.

Componente Servidor WSRR autónomo

El componente Servidor WSRR autónomo proporciona algunas opciones de configuración.

Los parámetros configurables del componente Servidor WSRR autónomo se describen en la tabla siguiente:

Tabla 5. Parámetros configurados

Nombre del parámetro	Valor predeterminado	Descripción
CPU virtuales	1	El número de procesadores virtuales asignado a la máquina virtual que representa este componente.
Tamaño de la memoria (MB)	4096	La cantidad de memoria asignada a esta máquina virtual, en megabytes.
Nombre de célula	Establezca uno de los siguientes valores: • SOAPolicySampleCell (patrón Basic Runtime Sample) • SOAPolicyBasicCell (patrón Basic Runtime) • SOAPolicyBasicCell (patrón Basic Runtime External DataPower)	
Nombre de nodo	Establezca uno de los siguientes valores: • SOAPolicySampleNode (patrón Basic Runtime Sample) • SOAPolicyBasicNode (patrón Basic Runtime) • SOAPolicyBasicNode (patrón Basic Runtime External DataPower)	

Tabla 5. Parámetros configurados (continuación)

Nombre del parámetro	Valor predeterminado	Descripción
Contraseña (root)		La contraseña para el ID de usuario root. Este es la contraseña para el sistema operativo de la máquina virtual que está representado por esta parte en el patrón.
Verificar contraseña		Verifica la entrada de usuario para la Contraseña (root).
Nombre de usuario administrativo de WebSphere	virtuser	El nombre de usuario administrativo de WebSphere Application Server. No debe cambiar este valor.
Contraseña administrativa de WebSphere		La contraseña del usuario administrativo de WebSphere Application Server.
Verificar contraseña		Verifica la entrada de usuario de la contraseña administrativa de WebSphere Application Server.
Habilitar VNC	True	Este valor está bloqueado y no puede modificarse.

Componente Gestor de despliegue de WSRR

Componente Gestor de despliegue de WSRR proporciona algunas opciones de configuración.

Los parámetros configurables del componente Gestor de despliegue de WSRR se describen en la tabla siguiente:

Tabla 6. Parámetros configurables

Nombre del parámetro	Valor predeterminado	Descripción
CPU virtuales	1	El número de procesadores virtuales asignado a la máquina virtual que representa este componente.
Tamaño de la memoria (MB)	2048	La cantidad de memoria asignada a esta máquina virtual, en megabytes.
Nombre de célula	SOAPolicyAdvancedCell	El nombre de célula del patrón Advanced Runtime.
Nombre de nodo	SOAPolicyAdvancedNode	El nombre de nodo del nodo que reside en la máquina virtual del gestor de despliegue en el patrón Advanced Runtime.
Contraseña (root)		La contraseña para el ID de usuario root. Este es la contraseña para el sistema operativo de la máquina virtual que está representado por esta parte en el patrón.
Verificar contraseña		Verifica la entrada de usuario para la Contraseña (root).
Nombre de usuario administrativo de WebSphere	virtuser	El nombre del usuario administrador de WebSphere Application Server. No debe cambiar este valor.

Tabla 6. Parámetros configurables (continuación)

Nombre del parámetro	Valor predeterminado	Descripción
Contraseña administrativa de WebSphere		La contraseña del usuario administrativo de WebSphere Application Server.
Verificar contraseña		Verifica la entrada de usuario de la contraseña administrativa de WebSphere Application Server.
Habilitar VNC	True	Este valor está bloqueado y no puede modificarse.

Componente Nodos personalizados de WSRR

El componente Nodos personalizados de WSRR proporciona algunas opciones de configuración.

Los parámetros configurables del componente Nodos personalizados de WSRR se describen en la tabla siguiente:

Tabla 7. Parámetros configurables

Nombre del parámetro		Descripción
CPU virtuales	2	El número de procesadores virtuales asignado a la máquina virtual que representa este componente.
Tamaño de la memoria (MB)	4096	La cantidad de memoria asignada a esta máquina virtual, en megabytes.
Nombre de célula	CloudBurstCell	Se omite el valor de nombre de célula de la configuración del componente Nodos personalizados.
Nombre de nodo	SOAPolicyAdvancedNode	El nombre de nodo del nodo que reside en la máquina virtual del nodo personalizado del patrón Tiempo de ejecución avanzado.
Contraseña (root)		La contraseña para el ID de usuario root. Este es la contraseña para el sistema operativo de la máquina virtual que está representado por esta parte en el patrón.
Verificar contraseña		Verifica la entrada de usuario para la Contraseña (root).
Nombre de usuario administrativo de WebSphere	virtuser	El nombre del usuario administrador del entorno WebSphere Application Server. No debe cambiar este valor.
Contraseña administrativa de WebSphere		La contraseña del usuario administrativo del entorno WebSphere Application Server.
Verificar contraseña		Verifica la entrada de usuario de la contraseña administrativa de WebSphere Application Server.
Habilitar VNC	True	Este valor está bloqueado y no puede modificarse.

Componente DataPower

El componente DataPower tiene algunas opciones de configuración.

Los parámetros configurables de la imagen del sistema virtual de DataPower se describen en la tabla siguiente:

Tabla 8. Parámetros configurados

Nombre del parámetro	Valor predeterminado	Descripción
CPU virtuales	4	El número de procesadores virtuales asignado a la máquina virtual que representa este componente.
Tamaño de la memoria (MB)	4096	La cantidad de memoria asignada a esta máquina virtual, en megabytes.
contraseña de administrador		La contraseña para el administrador de DataPower.
Verificar contraseña		Verifica la entrada de usuario de la contraseña de administrador.
Habilitar SSH	True	Habilita SSH (para utilizar la interfaz de línea de mandatos de DataPower).
Puerto SSH	22	El puerto para SSH.
Habilitar la interfaz de gestión XML	True	Habilita la interfaz de gestión de XML. Cuando está habilitada, esta interfaz permite a los administradores enviar solicitudes de estado y configuración al dispositivo DataPower a través de una interfaz SOAP estándar.
Puerto de interfaz de gestión XML	5550	El puerto para la interfaz de gestión XML.
Habilitar servicio de gestión web	True	Habilita la interfaz gráfica de usuario web para interactuar con el dispositivo de DataPower.
Puerto de servicio de gestión web	9090	El puerto para la interfaz gráfica de usuario web.
Directorio RAID	raid0	El directorio en el que puede acceder a los archivos en el almacenamiento de datos auxiliar de DataPower.

Paquetes script

Existen siete paquetes script que se proporcionan con el Patrón IBM SOA Policy Gateway.

Los siguientes paquetes script se incluyen con este patrón:

- SOA Policy Gateway 2.5.0.0 - Dominio DataPower
- SOA Policy Gateway 2.5.0.0 - Promoción
- SOA Policy Gateway 2.5.0.0 - Ejemplos
- SOA Policy Gateway 2.5.0.0 - Seguridad
- SOA Policy Gateway 2.5.0.0 - Dominio DataPower
- SOA Policy Gateway 2.5.0.0 - Añadir consultas con nombre
- SOA Policy Gateway 2.5.0.0 - Anular

Los scripts Añadir consultas con nombre y Anular no contienen parámetros configurables por el usuario.

Script: SOA Policy Gateway 2.5.0.0 - Dominio DataPower

El script del dominio DataPower suministra el dominio DataPower durante el despliegue. El script configura la conexión entre el tiempo de ejecución de WSRR y hasta 10 dispositivos DataPower (virtuales).

Parámetros

Tabla 9. Parámetros configurables

Nombre del parámetro	Valor predeterminado	Descripción
DataPower_hostname	*Este valor está bloqueado y no puede modificarse.*	El nombre de host para la instancia o dispositivo DataPower que se va a supervisar.
DataPower_admin_id	*Este valor está bloqueado y no puede modificarse.*	El ID de usuario administrador para esa instancia o dispositivo.
DataPower_XML_mgmt_port	*Este valor está bloqueado y no puede modificarse.*	El puerto para comunicarse con la interfaz de gestión XML en la instancia o aplicación DataPower.
DataPower_admin_password	*Este valor está bloqueado y no puede modificarse.*	Contraseña para el ID del usuario administrador.
Verificar contraseña	*Este valor está bloqueado y no puede modificarse.*	Repita la contraseña para el ID del usuario administrador.
DataPower2_hostname	*Este valor está bloqueado y no puede modificarse.*	
DataPower2_admin_id	*Este valor está bloqueado y no puede modificarse.*	
DataPower2_XML_mgmt_port	*Este valor está bloqueado y no puede modificarse.*	
DataPower2_admin_password	*Este valor está bloqueado y no puede modificarse.*	
Verificar contraseña	*Este valor está bloqueado y no puede modificarse.*	
...		...
DataPower10_hostname	*Este valor está bloqueado y no puede modificarse.*	
DataPower10_admin_id	*Este valor está bloqueado y no puede modificarse.*	
DataPower10_XML_mgmt_port	*Este valor está bloqueado y no puede modificarse.*	
DataPower10_admin_password	*Este valor está bloqueado y no puede modificarse.*	
Verificar contraseña	*Este valor está bloqueado y no puede modificarse.*	

Tabla 9. Parámetros configurables (continuación)

Nombre del parámetro	Valor predeterminado	Descripción
New_DataPower_domain	El valor predeterminado depende del tipo de patrón: • SOAPolicyAdvancedRuntime • SOAPolicyBasicRuntime	El nuevo nombre de dominio que se debe crear en cada dispositivo o instancia DataPower. No debe coincidir con ningún dominio existente, de lo contrario, el paquete script falla o concluye su ejecución. El valor no puede contener espacios.
Remove_security_files	True	Para da soporte a la utilización, puede ignorar este valor.

Script: SOA Policy Gateway 2.5.0.0 - Promoción

El script Promoción permite integrar el patrón Basic Runtime o Advanced Runtime con un patrón SOA Policy Gateway Governance Master desplegado previamente. Establece la seguridad entre células entre el patrón Tiempo de ejecución y Gobierno, mientras que opcionalmente configura la promoción de WSRR en el maestro de gobierno.

Parámetros

Tabla 10. Parámetros configurables

Nombre del parámetro	Valor predeterminado	Descripción
WSRR_GOV_DMGR_hostname		El nombre de host del gestor de despliegue para el clúster WSRR.
WSRR_GOV_DMGR_cellname	SOAPolicyGMCell	El nombre de célula para el clúster WSRR.
WSRR_GOV_admin_user	virtuser	El ID de administración para la célula de Gobierno de WSRR.
WSRR_GOV_admin_password		La contraseña para el ID de administración de la célula de gobierno de WSRR.
Verificar contraseña		Verifica los datos de entrada del usuario para WSRR_admin_password.
Promotion_environment		El valor debe ser Transición, Producción o Sin definir. Estos valores distinguen entre mayúsculas y minúsculas, y deben coincidir exactamente.
LTPA_key_password		En el paquete script, se exporta y utiliza una clave LTPA. La clave procede del Maestro de Gobierno y se utiliza en todas las células del entorno de promoción. Esta es la contraseña que se utiliza cuando se exporta la clave LTPA.
Verificar contraseña		Verifica los datos de entrada del usuario para LTPA_key_password.

Script: SOA Policy Gateway 2.5.0.0 - Ejemplo

El script Ejemplo configura los parámetros de la aplicación de ejemplo que se utilizarán con el patrón SOA Policy Gateway Basic Runtime Sample.

Parámetros

El usuario no puede definir ninguno de estos parámetros.

Tabla 11. Parámetros configurables

Nombre del parámetro		Descripción
SCP_host	*Este valor está bloqueado y no puede modificarse.*	
SCP_user	*Este valor está bloqueado y no puede modificarse.*	
SCP_password	*Este valor está bloqueado y no puede modificarse.*	
Verificar contraseña	*Este valor está bloqueado y no puede modificarse.*	
SCP_zip_location	*Este valor está bloqueado y no puede modificarse.*	
CLIENT_PUBLIC_KEY_file	*Este valor está bloqueado y no puede modificarse.*	
CLIENT_PUBLIC _KEY_password	*Este valor está bloqueado y no puede modificarse.*	
Verificar contraseña		
CLIENT_PRIVATE_KEY_file	*Este valor está bloqueado y no puede modificarse.*	
CLIENT_PRIVATE_KEY_password	*Este valor está bloqueado y no puede modificarse.*	
Verificar contraseña		
CLI_FILE_file	*Este valor está bloqueado y no puede modificarse.*	
Verificar contraseña	*Este valor está bloqueado y no puede modificarse.*	
DataPower_hostname	*Este valor está bloqueado y no puede modificarse.*	El nombre de host de la instancia DataPower.
DataPower_XML_mgmt_port	*Este valor está bloqueado y no puede modificarse.*	El puerto que se utiliza para la interfaz de gestión XML de DataPower.
DataPower_admin_id	*Este valor está bloqueado y no puede modificarse.*	El ID del usuario administrativo con los permisos adecuados para utilizar la interfaz de gestión XML.
DataPower_admin_password	*Este valor está bloqueado y no puede modificarse.*	La contraseña de DataPower_admin_id.
Verificar contraseña	*Este valor está bloqueado y no puede modificarse.*	Verifica la entrada de usuario de DataPower_admin_password.
SOAPolicySample_DataPower_domain	*Este valor está bloqueado y no puede modificarse.*	El nombre de dominio de ejemplo. No debe coincidir con ningún dominio existente en la instancia de DataPower.

Tabla 11. Parámetros configurables (continuación)

Nombre del parámetro		Descripción
SamplePolicySample_starting_port	*Este valor está bloqueado y no puede modificarse.*	La aplicación necesita 5 puertos libres, que se utilizan de forma secuencial a partir de este valor. Por ejemplo, si el valor es 62000, se utilizan los puertos 62000-62004. El script no comprueba si los puertos están libres.
LDAP_hostname	*Este valor está bloqueado y no puede modificarse.*	El nombre de host del componente autónomo WSRR, donde también se aloja un servidor LDAP.
LDAP_port	*Este valor está bloqueado y no puede modificarse.*	El puerto del servidor LDAP.
LDAP_password	*Este valor está bloqueado y no puede modificarse.*	La contraseña que se utiliza al enlazar con el LDAP_DN.
Verificar contraseña	*Este valor está bloqueado y no puede modificarse.*	Verifica la entrada de usuario de LDAP_password.
LDAP_DN	*Este valor está bloqueado y no puede modificarse.*	El nombre distinguido que se utiliza para enlazar con LDAP.

Script: SOA Policy Gateway 2.5.0.0 - Seguridad

El script Seguridad copia información de seguridad (certificados, etc.) entre sistemas DataPower y WSRR en el patrón.

Los parámetros de configuración para los archivos de script de seguridad son para utilizar como soporte. Debe dejarlos con sus valores predeterminados.

Script: SOA Policy Gateway 2.5.0.0 - Supervisión de DataPower (solo x86)

El script de supervisión de DataPower especifica los parámetros de conexión para el servicio compartido de supervisión de DataPower. El agente y los recopiladores de datos ITCAM DataPower se ejecutan en el componente Core OS.

Parámetros

El servicio de supervisión puede supervisar un máximo de 10 dispositivos virtuales DataPower.

Tabla 12. Parámetros configurables

Nombre del parámetro	Valor predeterminado	Descripción
DataPower1_hostname		El nombre de host para el dispositivo virtual DataPower que se supervisará.
DataPower1_admin_id	admin	El ID de usuario administrador para ese dispositivo virtual.
DataPower1_XML_mgmt_port	5550	El puerto para comunicarse con la interfaz de gestión XML en el dispositivo virtual DataPower.
DataPower1_admin_password		Contraseña para el ID del usuario administrador.

Tabla 12. Parámetros configurables (continuación)

Nombre del parámetro	Valor predeterminado	Descripción
Verificar contraseña		Repita la contraseña para el ID del usuario administrador.
DataPower2_hostname		
DataPower2_admin_id	admin	
DataPower2_XML_mgmt_port	5550	
DataPower2_admin_password		
Verificar contraseña		
...		...
DataPower10_hostname		
DataPower10_admin_id	admin	
DataPower10_XML_mgmt_port	5550	
DataPower10_admin_password		
Verificar contraseña		

Script: SOA Policy Gateway 2.5.0.0 - Supervisión de DataPower externa

El script de supervisión de DataPower especifica los parámetros de conexión para el servicio compartido de supervisión de DataPower. El agente y los recopiladores de datos ITCAM DataPower se ejecutan en el componente Core OS.

Parámetros

El servicio de supervisión puede supervisar un máximo de 10 dispositivos DataPower.

Tabla 13. Parámetros configurables

Nombre del parámetro	Valor predeterminado	Descripción
DataPower1_hostname		El nombre de host para el dispositivo DataPower que se supervisará.
DataPower1_admin_id	admin	El ID de usuario administrador para ese dispositivo.
DataPower1_XML_mgmt_port	5550	El puerto para comunicarse con la interfaz de gestión XML en el dispositivo DataPower.
DataPower1_admin_password		Contraseña para el ID del usuario administrador.
Verificar contraseña		Repita la contraseña para el ID del usuario administrador.
DataPower2_hostname		
DataPower2_admin_id	admin	
DataPower2_XML_mgmt_port	5550	
DataPower2_admin_password		
Verificar contraseña		
...		...

Tabla 13. Parámetros configurables (continuación)

Nombre del parámetro	Valor predeterminado	Descripción
DataPower10_hostname		
DataPower10_admin_id	admin	
DataPower10_XML_mgmt_port	5550	
DataPower10_admin_password		
Verificar contraseña		

Capítulo 5. Trabajar con el Patrón IBM SOA Policy Gateway

El Patrón IBM SOA Policy Gateway proporciona definiciones de patrones para despliegues repetibles. En estos temas se describe cómo desplegar los patrones.

Como parte del proceso de despliegue, configure los parámetros de los componentes. Para obtener más información, consulte “Despliegue de patrones” en la página 47. Los patrones se describen en Capítulo 4, “Patrones, componentes y paquetes script”, en la página 19.

Tareas relacionadas:

Capítulo 3, “Iniciación al Patrón IBM SOA Policy Gateway”, en la página 13
Este patrón utiliza WebSphere DataPower para controlar los mensajes utilizando políticas gobernadas y definiciones de servicio en WSRR. Revise los temas de esta sección para saber cómo descargar e instalar el patrón, cómo verificarlo tras la instalación, aceptar licencias y los roles de usuario implicados.

Planificación de la configuración del patrón y los requisitos previos del patrón

El Patrón IBM SOA Policy Gateway proporciona un medio para proporcionar, de forma rápida y fiable, un entorno para gobernar definiciones de servicio y políticas, y aplicar esas políticas. El despliegue del patrón comienza con el maestro de gobierno, seguido por el patrón de tiempo de ejecución.

Preparación y despliegue del Patrón IBM SOA Policy Gateway

- Si está utilizando un dispositivo DataPower externo, preparare el dispositivo para la administración remota. Para obtener más información, consulte “Configuración de un dispositivo de DataPowerpara el Patrón IBM SOA Policy Gateway” en la página 46.

Despliegue el patrón de maestro de gobierno:

1. Despliegue de un patrón de SOA Policy Gateway Governance Master. Espere a que finalice el despliegue antes de desplegar patrones de ejecución. Para obtener más información, consulte “Despliegue del patrón de maestro de gobierno” en la página 50.

Despliegue los patrones de ejecución:

1. Decida si se necesita un patrón de tiempo de ejecución básico con un entorno autónomo, o un patrón de tiempo de ejecución avanzado con un entorno en clúster.
2. Determine cuántos dispositivos e instancias DataPower requieren sus patrones de tiempo de ejecución.

   Los patrones que incluye DataPower tienen dos instancias DataPower de forma predeterminada. Puede configurar hasta 10 instancias DataPower. Para obtener más información, consulte “Adición de instancias DataPower a un patrón” en la página 56.

   Los patrones con DataPower externo se pueden configurar para que funcionen con hasta 10 dispositivos DataPower. Consulte el apartado “Despliegue de patrones DataPower externos avanzados y básicos” en la página 57.

Nota: No se pueden añadir instancias y dispositivos DataPower adicionales después de completar la configuración.

3. Configure el patrón de ejecución con la información del patrón de maestro de gobierno. Para obtener más información, consulte “Información sobre el despliegue del SOA Policy Gateway Governance Master” en la página 51. Puede omitir información de patrones de maestro de gobierno para desplegar un sistema autónomo, si es necesario (aunque esto mostrará un error en el despliegue, el error se puede ignorar).
4. Especifique si el sistema de tiempo de ejecución es de transición o producción.
5. Despliegue el patrón. Para obtener más información, consulte “Despliegue de un patrón de tiempo de ejecución avanzado” en la página 53 o “Despliegue de un patrón de tiempo de ejecución básico” en la página 52.
6. Espere a que finalice totalmente el despliegue antes de desplegar otro tiempo de ejecución.

Cuando finalice el despliegue de los patrones de tiempo de ejecución:

1. WSRR y la seguridad de WebSphere se pueden actualizar a una configuración de seguridad diferente de la configuración predeterminada. Para obtener más información, consulte “Seguridad para los patrones Patrón IBM SOA Policy Gateway”.
2. El dominio DataPower está listo para la configuración de la pasarela. Si utiliza un dispositivo DataPower virtual, primero debe aplicar el fixpack más reciente, consulte “Actualización de DataPower en la instancia desplegada” en la página 54.

Configuración de un dispositivo de DataPowerpara el Patrón IBM SOA Policy Gateway

Complete los pasos siguientes de configuración de DataPower antes de ejecutar los scripts SOAPolicy.

Procedimiento

1. Inicie sesión en la interfaz gráfica de usuario web del dispositivo de DataPower como administrador.
2. Busque `Interfaz de gestión XML`.
3. Asegúrese de que su estado está habilitado.
4. Asegúrese de que lo siguiente esté activo y asegurado correctamente:
   - URI de gestión SOAP
   - Gestión de la configuración SOAP
   - Gestión de la configuración SOAP (v2004)
   - Punto final AMP
   - Punto final SLM
   - Punto final WS-Management
   - Punto final WSDM
   - Suscripción UDDI
   - Suscripción WSRR

Seguridad para los patrones Patrón IBM SOA Policy Gateway

La autenticación mutua se produce entre las aplicaciones DataPower y los scripts de los patrones Básico y Avanzado. Los scripts realizan el intercambio de

certificados necesario. Tenga en cuenta que los certificados SSL predeterminados que se proporcionan con el patrón se atribuyen al host que se ha utilizado para crear el patrón.

Aumento de la seguridad

Las imágenes de WSRR y las imágenes de WebSphere Application Server utilizadas en los patrones sólo tienen en vigor la seguridad predeterminada. Para generar un entorno más seguro, puede utilizar técnicas de seguridad de WebSphere Application Server estándar.

Consulte el Information Center de WebSphere Network Deployment Versión 8.0 en los enlaces siguientes:

- WebSphere Application Server, Network Deployment (Plataformas distribuidas y Windows), Versión 8.0: Information Center de IBM WebSphere Application Server, Network Deployment (Plataformas distribuidas y Windows), Versión 8.0
- Seguridad de aplicación: Information Center de IBM WebSphere Application Server, Network Deployment (Plataformas distribuidas y Windows), Versión 8.0 - Protección de aplicaciones y su entorno
- Vías globales de seguridad: Information Center de IBM WebSphere Application Server, Network Deployment (Plataformas distribuidas y Windows), Versión 8.0 - Protección de aplicaciones y su entorno

Despliegue de patrones

El despliegue de patrones con IBM PureApplication System en la nube proporciona un entorno de pasarela de políticas SOA en ejecución. Puede desplegar los patrones predefinidos disponibles con las imágenes Patrón IBM SOA Policy Gateway o bien desplegar los patrones que ha creado.

Antes de empezar

Para desplegar un patrón, primero debe tener un patrón predefinido o un patrón nuevo que esté completo, con todos los componentes necesarios configurados. Necesita detalles del entorno, grupo de nubes y grupo de IP para desplegar, procedentes del administrador del sistema PureAS.

Acerca de esta tarea

Despliegue el patrón utilizando la consola de carga de trabajo.

Procedimiento

Para desplegar los Patrón IBM SOA Policy Gateway, de modo que se ejecuten en la nube privada, siga estos pasos:

1. En la lista de patrones de la ventana Patrones del sistema virtual, seleccione el patrón que se ha de desplegar.
2. Pulse el icono **Desplegar**.
3. Complete los campos necesarios para desplegar el patrón. En la ventana, proporcione un nombre para el sistema virtual y proporcione cualquier otra información necesaria. Una marca de selección junto a cada elemento indica que no requiere configuración adicional. Puede cambiar los parámetros para componentes configurados, antes de desplegar el patrón, pulsando el nombre

de componente para abrir el editor del componente. Las máquinas virtuales se crean, en el orden adecuado, y luego se inician.

Resultados

El proceso de despliegue crea e inicia las máquinas virtuales para los componentes definidos y proporciona enlaces a las consolas necesarias. La duración del despliegue depende de la complejidad del patrón desplegado. Un patrón desplegado es un sistema virtual, o el entorno de tiempo de ejecución del Patrón IBM SOA Policy Gateway recién suministrado.

Qué hacer a continuación

Puede ver el estado de la instancia, para comprobar si el despliegue se ha completado y empezar a administrarlo, desde la ventana Instancias del sistema virtual.

Información relacionada:

IBM PureApplication System: Gestión de patrones del sistema virtual

Despliegue del servicio compartido de supervisión de sistemas

El despliegue del servicio compartido de supervisión del sistema para SOA Policy Gateway proporciona componentes de supervisión para el sistema virtual.

Antes de empezar

El administrador del sistema de PureAS debe iniciar el servicio compartido de supervisión del sistema e informarle del entorno y grupo de nubes en el que lo han iniciado. Debe utilizar el mismo entorno y grupo de nubes para desplegar el servicio compartido de supervisión del sistema para SOA Policy Gateway y los patrones de gobierno y tiempo de ejecución.

La supervisión de instancias WSRR también requiere que se inicie el servicio compartido de supervisión del sistema para WebSphere, de manera que debe asegurarse de que esté en su sistema PureAS.

Procedimiento

Complete los pasos siguientes en la consola de carga de trabajo:

1. Pulse **Instancias** > **Servicios compartidos**.
2. Verifique que el servicio de supervisión del sistema esté ejecutándose en el grupo de nubes en el que se desplegarán los patrones. Si no se está ejecutando, póngase en contacto con el administrador de PureAS para iniciarlo.
3. Para habilitar el servicio compartido de supervisión de DataPower:
   a. Pulse **Nube** > **Tipos de patrón**.
   b. Seleccione la entrada **System Monitoring for SOA Policy Gateway Pattern 2.5.0.0** en el panel Tipos de patrón.
   c. Pulse **Habilitar** en el campo **Estado** campo, y espere hasta que el campo de estado cambie a **Inhabilitar**.
4. Para iniciar el servicio compartido de supervisión de WebSphere Application Server:
   a. Pulse **Instancias** > **Servicios compartidos**.

b. Pulse el símbolo más en el panel Instancias de servicios compartidos para abrir la ventana Desplegar servicio compartido.
c. Seleccione **Supervisión del sistema para WebSphere Application Server** y pulse **Aceptar**.
d. En la ventana Configurar y desplegar un servicio compartido, especifique si desea que el servicio se inicie en patrones previamente desplegados seleccionando los dos recuadros de selección de la parte inferior. Pulse **Aceptar**.
e. En la ventana Desplegar aplicación virtual, especifique **Grupo de nubes de destino**, **Grupo de IP** y **Perfil** según la información proporcionada por el administrador del sistema PureAS. Deben ser los mismos que aquellos en los que se despliegan los sistemas virtuales.

5. Para iniciar el servicio compartido de supervisión de WebSphere DataPower:
   a. Pulse **Instancias** > **Servicios compartidos** en la barra de menús.
   b. Pulse el símbolo más en el panel Instancias de servicios compartidos para abrir la ventana Desplegar servicio compartido.
   c. Seleccione **Supervisión del sistema para WebSphere DataPower** de la lista y pulse **Aceptar**.
   d. En la ventana Configurar y desplegar un servicio compartido, especifique si desea que la supervisión se inicie en patrones previamente desplegados seleccionando los dos recuadros de selección de la parte inferior. Pulse **Aceptar**.
   e. En la ventana Desplegar aplicación virtual, especifique **Grupo de nubes de destino**, **Grupo de IP** y **Perfil** según la información proporcionada por el administrador del sistema PureAS. Deben ser los mismos que aquellos en los que se despliegan los sistemas virtuales.
   f. Genere y guarde una clave SSH si necesita acceso de depuración al servicio compartido de supervisión.
   g. Pulse **Aceptar**.

Resultados

El servicio compartido de supervisión del sistema para WebSphere DataPower se muestra como en ejecución. El servicio compartido de supervisión del sistema para WebSphere Application Server se muestra como en ejecución.

Qué hacer a continuación

Para verificar el despliegue, consulte “Verificación del despliegue” en la página 55.

Despliegue del patrón de ejemplo de tiempo de ejecución básico

Cuando se despliega el patrón SOA Policy Gateway Basic Runtime Sample se crea una instancia de sistema virtual en ejecución del patrón. Este patrón sólo está disponible en sistemas x86.

Acerca de esta tarea

El despliegue de un patrón crea una instancia de sistema virtual en ejecución en la nube.

Procedimiento

Para desplegar el patrón SOA Policy Gateway Basic Runtime Sample, complete los pasos siguientes:

1. En la consola de carga de trabajo, pulse **Patrones** > **Sistemas virtuales**.
2. En la lista Patrones de sistema virtual, seleccione **SOA Policy Gateway 2.5.0.0 - Basic Runtime Sample**.
3. Pulse el icono **Desplegar**.
4. Complete los campos necesarios para desplegar el patrón. Una marca de selección junto a cada elemento indica que no requiere configuración adicional.
   a. En el recuadro **Nombre de sistema virtual**, escriba un nombre exclusivo para la instancia.
   b. Expanda la sección **Seleccionar entorno**, y especifique el **Perfil** que le ha proporcionado el administrador del sistema PureAS.
   c. Configure los patrones virtuales. Pulse **Configurar componentes virtuales** y, a continuación, pulse el nombre del componente para abrir el editor para componentes y scripts. Especifique el **Grupo de nubes** y **Grupo de IP**, según la información proporcionada por el administrador del sistema PureAS. Consulte los siguientes temas para obtener detalles sobre los parámetros de configuración específicos del script y del patrón.

      Nota: Todas las contraseñas para este patrón toman el valor predeterminado `password`.
      - "Componente DataPower" en la página 37
      - "Componente DB2 Enterprise" en la página 28.
      - "Componente Servidor WSRR autónomo" en la página 34
      - "Script: SOA Policy Gateway 2.5.0.0 - Ejemplo" en la página 40
5. Pulse **Aceptar** para desplegar el patrón.

Qué hacer a continuación

Para verificar el despliegue, consulte "Verificación del despliegue" en la página 55.

Despliegue del patrón de maestro de gobierno

Cuando se despliega el patrón SOA Policy Gateway Governance Master se crea una instancia de sistema virtual en ejecución del patrón.

Procedimiento

Para desplegar el patrón SOA Policy Gateway Governance Master, realice los pasos siguientes :

1. En la consola de carga de trabajo, pulse **Patrones** > **Sistemas virtuales**.
2. En la lista Patrones de sistema virtual, seleccione **SOA Policy Gateway 2.5.0.0 - Governance Master**.
3. Pulse el icono **Desplegar**.
4. Complete los campos para desplegar el patrón. Una marca de selección junto a cada elemento indica que no requiere configuración adicional.
   a. En el recuadro **Nombre de sistema virtual**, escriba un nombre exclusivo para la instancia.
   b. Expanda la sección **Seleccionar entorno**, y especifique el **Perfil**, según la información proporcionada por el administrador del sistema PureAS.

c. Configure los patrones virtuales. Pulse **Configurar componentes virtuales** y, a continuación, pulse el nombre del componente para abrir el editor para componentes y scripts. Especifique el **Grupo de nubes** y **Grupo de IP**, según la información proporcionada por el administrador del sistema PureAS. Consulte los siguientes temas para obtener detalles sobre los parámetros de configuración específicos del script y del patrón.
   - "Componente DB2 Enterprise HADR Primary" en la página 30
   - "Componente Gestor de despliegue de WSRR" en la página 35
   - "Componente Nodos personalizados de WSRR" en la página 36
   - "Componente DB2 Enterprise HADR Standby" en la página 32

5. Pulse **Aceptar** para desplegar el patrón.

Qué hacer a continuación

Para verificar el despliegue, consulte "Verificación del despliegue" en la página 55.

Información sobre el despliegue del SOA Policy Gateway Governance Master

El Maestro de gobierno se debe desplegar antes de que se despliegen los patrones de tiempo de ejecución.

Acerca de esta tarea

La información de despliegue de la instancia del Maestro de gobierno se debe especificar como entrada para los valores de despliegue de los patrones de tiempo de ejecución.

Procedimiento

Para encontrar los valores necesarios de la instancia del Maestro de gobierno:

1. Navegue hasta **Instancias** > **Sistemas virtuales**.
2. Seleccione la instancia del Maestro de gobierno de despliegue.
3. Expanda **Máquinas virtuales**.
4. Expanda la máquina virtual denominada ***WSRRDMGR***.
5. Observe los puntos siguientes:
   - En la sección **Hardware y red**, anote la dirección de host y dirección IP. El nombre de host es el valor de **Interfaz de red 0**.
   - En la sección **Configuración de WebSphere**, anote el Nombre de célula.

   El nombre de host o dirección IP, el nombre de célula y el nombre de usuario administrativo y contraseña de WebSphere utilizados durante el despliegue de la instancia del Maestro de gobierno se deben especificar como entrada para los parámetros siguientes en los patrones de tiempo de ejecución:
   - WSRR_GOV_DMGR_hostname
   - WSRR_GOV_DMGR_cellname
   - WSRR_GOV_admin_user
   - WSRR_GOV_admin_password

   Si desea desplegar un patrón de tiempo de ejecución como un sistema autónomo, puede establecer estos parámetros en "Sin definir". Este valor hace que el despliegue aparezca como **fallido** en el **Sistema virtual** > **Instancias** porque el paquete script de promoción falla. Sin embargo, el despliegue todavía no se puede utilizar.

Despliegue de un patrón de tiempo de ejecución básico

Cuando se despliega el patrón de tiempo de ejecución básico, se crea una instancia de sistema virtual en ejecución del patrón.

Antes de empezar

Complete las siguientes tareas antes de desplegar un patrón de tiempo de ejecución básico:

- Si despliega un patrón de tiempo de ejecución básico con DataPower externo, configure los dispositivos DataPower para el Patrón IBM SOA Policy Gateway; consulte "Configuración de un dispositivo de DataPowerpara el Patrón IBM SOA Policy Gateway" en la página 46. En sistemas Power, solo se admite DataPower externo.
- Obtenga la información de despliegue del Maestro de gobierno; consulte "Información sobre el despliegue del SOA Policy Gateway Governance Master" en la página 51.

Acerca de esta tarea

El despliegue de un patrón crea una instancia de sistema virtual en ejecución en la nube.

Nota: Si está utilizando el perfil de habilitación de gobierno (GEP), no puede desplegar un entorno de transición y un entorno de producción de forma simultánea en los patrones de tiempo de ejecución. Esta limitación se debe a que puede causar conflictos durante el proceso de configuración de las propiedades de promoción. Despliegue primero el entorno de transición y luego el entorno de producción.

Procedimiento

Para desplegar un patrón de tiempo de ejecución básico, complete los pasos siguientes:

1. Pulse **Patrones** > **Sistemas virtuales**.
2. En la lista Patrones de sistema virtual, seleccione **SOA Policy Gateway 2.5.0.0 - Basic Runtime External DataPower** o **SOA Policy Gateway 2.5.0.0 - Basic Runtime**.
3. Pulse el icono **Desplegar**.
4. Complete los campos necesarios para desplegar el patrón. Una marca de selección junto a cada elemento indica que no requiere configuración adicional.
   a. En el recuadro **Nombre de sistema virtual**, escriba un nombre exclusivo para la instancia.
   b. Expanda la sección **Seleccionar entorno**, y especifique el **Perfil** que le ha proporcionado el administrador del sistema PureAS.
   c. Configure los patrones virtuales. Pulse **Configurar componentes virtuales** y, a continuación, pulse el nombre del componente para abrir el editor para componentes y scripts. Especifique el **Grupo de nubes** y **Grupo de IP**, según la información proporcionada por el administrador del sistema PureAS. Consulte los siguientes temas para obtener detalles sobre los parámetros de configuración específicos del script y del patrón.

      Nota: Si desea desplegar el patrón sin un maestro de gobierno, especifique 'Sin definir' como el parámetro de nombre de host de maestro de gobierno.

Tenga en cuenta que esto provoca que el script de promoción se notifique como error en el despliegue, pero no tiene otras consecuencias.

- "Componente DataPower" en la página 37
- "Componente DB2 Enterprise" en la página 28
- "Componente Servidor WSRR autónomo" en la página 34
- "Script: SOA Policy Gateway 2.5.0.0 - Seguridad" en la página 41
- "Script: SOA Policy Gateway 2.5.0.0 - Promoción" en la página 39
- "Script: SOA Policy Gateway 2.5.0.0 - Dominio DataPower" en la página 38
- "Script: SOA Policy Gateway 2.5.0.0 - Supervisión de DataPower (solo x86)" en la página 41

5. Pulse **Aceptar** para desplegar el patrón.

Qué hacer a continuación

Para verificar el despliegue, consulte "Verificación del despliegue" en la página 55.

Despliegue de un patrón de tiempo de ejecución avanzado

Cuando se despliega el patrón de tiempo de ejecución avanzado, se crea una instancia de sistema virtual en ejecución del patrón.

Antes de empezar

Complete las siguientes tareas antes de desplegar un patrón de tiempo de ejecución avanzado:

- Si despliega un patrón de tiempo de ejecución avanzado con DataPower externo, configure los dispositivos DataPower para conectarse al patrón. Consulte el apartado "Configuración de un dispositivo de DataPowerpara el Patrón IBM SOA Policy Gateway" en la página 46. En sistemas Power, solo se admite DataPower externo.
- Obtenga la información de despliegue del Maestro de gobierno; consulte "Información sobre el despliegue del SOA Policy Gateway Governance Master" en la página 51.

Acerca de esta tarea

El despliegue de un patrón crea una instancia de sistema virtual en ejecución en la nube.

Nota: Si está utilizando el perfil de habilitación de gobierno (GEP), no puede desplegar un entorno de transición y un entorno de producción de forma simultánea en los patrones de tiempo de ejecución. Esta limitación se debe a que puede causar conflictos durante el proceso de configuración de las propiedades de promoción. Despliegue primero el entorno de transición y luego el entorno de producción.

Procedimiento

Para desplegar un patrón de tiempo de ejecución avanzado, complete los pasos siguientes:

1. Pulse **Patrones** > **Sistemas virtuales**.

2. En la lista Patrones de sistema virtual, seleccione **SOA Policy Gateway 2.5.0.0 - Advanced Runtime External DataPower** o **SOA Policy Gateway 2.5.0.0 - Advanced Runtime**.
3. Pulse el icono **Desplegar**.
4. Complete los campos necesarios para desplegar el patrón. Una marca de selección junto a cada elemento indica que no requiere configuración adicional.
   a. En el recuadro **Nombre de sistema virtual**, escriba un nombre exclusivo para la instancia.
   b. Expanda la sección **Seleccionar entorno**, y especifique el **Perfil** que le ha proporcionado el administrador del sistema PureAS.
   c. Configure los patrones virtuales. Pulse **Configurar componentes virtuales** y, a continuación, pulse el nombre del componente para abrir el editor para componentes y scripts. Especifique el **Grupo de nubes** y **Grupo de IP**, según la información proporcionada por el administrador del sistema PureAS. Consulte los siguientes temas para obtener detalles sobre los parámetros de configuración específicos del script y del patrón.

      Nota: Si desea desplegar el patrón sin un maestro de gobierno, especifique 'Sin definir' como el parámetro de nombre de host de maestro de gobierno. Tenga en cuenta que esto provoca que el script de promoción se notifique como error en el despliegue, pero no tiene otras consecuencias.
      - "Componente DataPower" en la página 37
      - "Componente DB2 Enterprise HADR Primary" en la página 30
      - "Componente Gestor de despliegue de WSRR" en la página 35
      - "Script: SOA Policy Gateway 2.5.0.0 - Promoción" en la página 39
      - "Script: SOA Policy Gateway 2.5.0.0 - Dominio DataPower" en la página 38
      - "Componente Nodos personalizados de WSRR" en la página 36
      - "Componente DB2 Enterprise HADR Standby" en la página 32
      - "Script: SOA Policy Gateway 2.5.0.0 - Supervisión de DataPower (solo x86)" en la página 41
5. Pulse **Aceptar** para realizar el despliegue.

Qué hacer a continuación

Para verificar el despliegue, consulte "Verificación del despliegue" en la página 55.

Actualización de DataPower en la instancia desplegada

Después de desplegar un patrón que incluye un componente de WebSphere DataPower, debe actualizar DataPower al fixpack más reciente.

Acerca de esta tarea

Actualice DataPower descargando el fixpack desde Fix Central y aplicándolo en la interfaz gráfica de usuario web de DataPower.

Procedimiento

1. Descargue el paquete de actualización desde Fix Central:
   a. En Fix Central, busque dispositivos WebSphere DataPower SOA.
   b. Seleccione y descargue el paquete XI52-virtual-6.0.0.1-Firmware.

2. Conéctese a la interfaz gráfica de usuario web para la máquina virtual de DataPower en el patrón desplegado, consulte “Conexión a la consola de un DataPower virtual” en la página 86.
3. En el panel de control, seleccione **Control del sistema**.
4. Localice la sección **Imagen de arranque**.
5. Suba al dispositivo DataPower el archivo `xi6001.scrypt4` desde el fixpack descargado. Utilice el gestor de archivos en la interfaz gráfica de usuario web de DataPower.
6. Seleccione el script subido desde la lista de **Archivo de firmware**.
7. Acepte las condiciones de licencia y pulse **Imagen de arranque**.
8. Siga las solicitudes para instalar el fixpack.

Verificación del despliegue

Después de desplegar el patrón, verifique que el despliegue se ha realizado correctamente.

Procedimiento

1. Compruebe en los registros del historial de despliegue del sistema virtual si se ha producido cualquier anomalía. Para obtener más información, consulte “Resolución de problemas con el despliegue” en la página 103.
2. Opcional: Si ha desplegado el SOA Policy Gateway Basic Runtime Sample, pruebe la instancia desplegada siguiendo la guía de aprendizaje para enviar algunos mensajes de ejemplo utilizando las aplicaciones de ejemplo proporcionadas. Consulte el apartado “Ejecución de los casos de prueba de ejemplo” en la página 61.

Cómo añadir un entorno de ejecución adicional

El perfil de habilitación de gobierno se proporciona con un sistema de clasificación de entornos predefinido que contiene cuatro entornos diferentes: desarrollo, prueba, transición y producción.

Acerca de esta tarea

Los entornos de Transición y Producción también están codificados en el ciclo de vida SOA que define el ciclo de las versiones de capacidad, tales como las versiones de servicio. Existen estados y transacciones que son específicos de los entornos de transición y producción, lo que permite realizar una promoción controlada hacia estos entornos de ejecución definiendo sistemas de destino en el archivo de configuración de la promoción. Este procedimiento es apropiado si su organización define los entornos del mismo modo, es decir, la transición es un entorno de pre-producción que permite realizar pruebas antes de poder utilizar la versión de capacidad de forma generalizada. Sin embargo, muchas organizaciones necesitan más entornos, por lo que es necesario realizar modificaciones en el perfil para tener en cuenta estas diferencias. Esta sección describe una manera de añadir un nuevo entorno de ejecución al perfil de habilitación de gobierno de WSRR.

Para obtener más información sobre la planificación de un entorno de despliegue, consulte “Planificación de la configuración del patrón y los requisitos previos del patrón” en la página 45.

Procedimiento

1. Despliegue el SOA Policy Gateway Governance Master predefinido. Para obtener más información, consulte “Despliegue del patrón de maestro de gobierno” en la página 50.
2. Opcional: Modifique el perfil de habilitación de gobierno de WSRR. Para obtener más información, consulte Information Center de IBM WebSphere Service Registry and Repository, Versión 8.0 - Guía de aprendizaje: Personalización de entornos de ejecución.
3. Configure los patrones de tiempo de ejecución básico o avanzado con los detalles del Maestro de gobierno. Para obtener más información, consulte “Información sobre el despliegue del SOA Policy Gateway Governance Master” en la página 51.

   Nota: El valor de entorno de promoción debe estar establecido en “Sin definir”.
4. Despliegue los patrones de tiempo de ejecución avanzado o tiempo de ejecución básico predefinidos. Para obtener más información, consulte “Despliegue de un patrón de tiempo de ejecución básico” en la página 52 y “Despliegue de un patrón de tiempo de ejecución avanzado” en la página 53.

Adición de instancias DataPower a un patrón

Los patrones básicos y avanzados con instancias DataPower internas tienen dos instancias de forma predeterminada. Cada patrón puede tener hasta 10 instancias DataPower en total.

Acerca de esta tarea

Los propios patrones no pueden editarse. Puede añadir instancias DataPower a los patrones de tiempo de ejecución básico o avanzado haciendo una copia del patrón y editándolo.

Procedimiento

1. Abra el patrón en la consola de carga de trabajo.
2. Pulse **Clonar**, y especifique un nombre para la copia del patrón.
3. Pulse **Editar**.
4. Arrastre más componentes de DataPower de la lista de componentes para añadirlos al patrón.
5. Pulse **Edición finalizada**.

Como suprimir instancias DataPower de un patrón

Puede suprimir las instancias DataPower de un patrón en caso necesario.

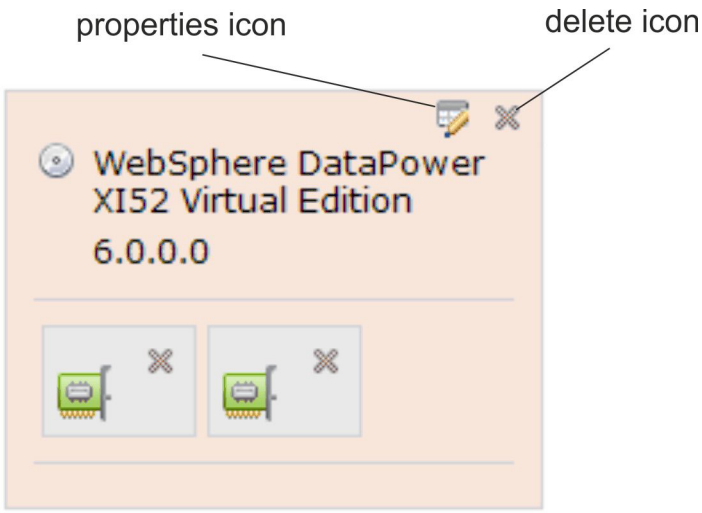
Acerca de esta tarea

Los propios patrones no pueden editarse. Puede suprimir instancias DataPower de los patrones de tiempo de ejecución básico o avanzado haciendo una copia del patrón y editándolo.

Procedimiento

1. Abra el patrón en la consola de carga de trabajo.
2. Pulse **Clonar**, y especifique un nombre para la copia del patrón.
3. Pulse **Editar**.

4. Suprima una instancia DataPower mediante el icono de supresión.



Nota: Las instancias DataPower deben suprimirse en orden número inverso. Cada instancia DataPower del lienzo tiene un número en su campo de nombre, que es visible pulsando el icono de propiedades. El nombre tiene el formato: 'DataPower_XI52*x*' donde *x* es el número (la primera instancia DataPower no tiene ningún número, su nombre es: 'DataPower_XI52'). Las instancias DataPower con los números más alto normalmente se encuentran en la esquina superior izquierda del lienzo.

5. Pulse **Edición finalizada**.

Despliegue de patrones DataPower externos avanzados y básicos

Los patrones de SOA Policy Gateway Basic Runtime External DataPower y SOA Policy Gateway Advanced Runtime External DataPower pueden desplegarse con hasta 10 dispositivos DataPower.

Acerca de esta tarea

Para obtener más información sobre el despliegue de los patrones, consulte “Despliegue de un patrón de tiempo de ejecución básico” en la página 52 o “Despliegue de un patrón de tiempo de ejecución avanzado” en la página 53.Para obtener más información sobre los parámetros de configuración de los cuales debe establecer los valores, consulte “Componente Servidor WSRR autónomo” en la página 34, “Componente Gestor de despliegue de WSRR” en la página 35 y “Script: SOA Policy Gateway 2.5.0.0 - Supervisión de DataPower (solo x86)” en la página 41.

Procedimiento

1. Despliegue el patrón y pulse **Configurar componentes virtuales**.
2. Para el componente de gestor de despliegue de WSRR o WSRR autónomo, especifique la siguiente información para cada dispositivo:
   - DataPower_hostname
   - DataPower_XML_mgmt_port
   - DataPower_admin_id
   - DataPower_admin_password

- Verificar contraseña
- New_DataPower_domain

La aplicación de ejemplo

La aplicación de ejemplo consta de un servicio Web y una API RESTful, ambos descritos y gobernados en WSRR. Un dominio DataPower está configurado con WSRR para ser una pasarela y se proporciona un cliente Web de ejemplo para ejecutar los servicios.

El escenario básico de la aplicación de ejemplo es una aplicación de inventario para una tienda (almacén), y un servicio RESTful que duplica una de las operaciones para móvil. El servicio web Store tiene tres operaciones:

- purchase
- findInventory
- returnProduct

La última operación, findInventory, también está disponible como servicio RESTful.

El servicio web de ejemplo

La definición de nivel de servicio (SLD) básica tiene dos políticas de mediación asociadas:

- Validación por comparación con Store.wsdl. El ejemplo supone que la validación de DataPower está desactivada.
- Rechazar si existen más de 5 mensajes en 90 segundos. Este umbral es bajo para facilitar la demostración.

El consumidor del servicio Store es la aplicación StoreConsumer, que tiene el ID de consumidor de “CEO”. Este consumidor tiene dos acuerdos de nivel de servicio (SLA), Gold y Silver. Si se incluye una solicitud en DataPower con el ID de consumidor de “CEO”, y un ID de contexto de “Silver”, se permite que la solicitud pase, porque el SLA Silver está en vigor. Si el ID de consumidor es “CEO”, y el ID de contexto es “Gold”, el SLA Gold coincide. Este SLA tiene una política de redireccionamiento asociada a él, de manera que la solicitud se redirige al punto final alternativo indicado en la política.

Si llega una solicitud con un ID de consumidor que no sea “CEO”, no habrá ninguna versión Application con este ID de consumidor. Por lo tanto, tampoco hay ningún SLA que pueda coincidir, así que se trata de una solicitud de un consumidor anónimo. Como tal, se aplica cualquier política asociada a un SLA anónimo. En este caso, esto provoca que aparezca una notificación en los registros. Observe que el ejemplo no incluye una forma de enviar una solicitud con un ID de consumidor que no sea “CEO”.

El escenario también realiza la autorización para la operación findInventory, que se basa en la pertenencia a un grupo de usuarios. Se proporciona un servidor LDAP con el ejemplo para correlacionar credenciales de usuario con el grupo correcto.

El diagrama de flujo de aplicaciones de ejemplo muestra el flujo de la aplicación, donde cada cuadro representa una pasarela DataPower diferente.

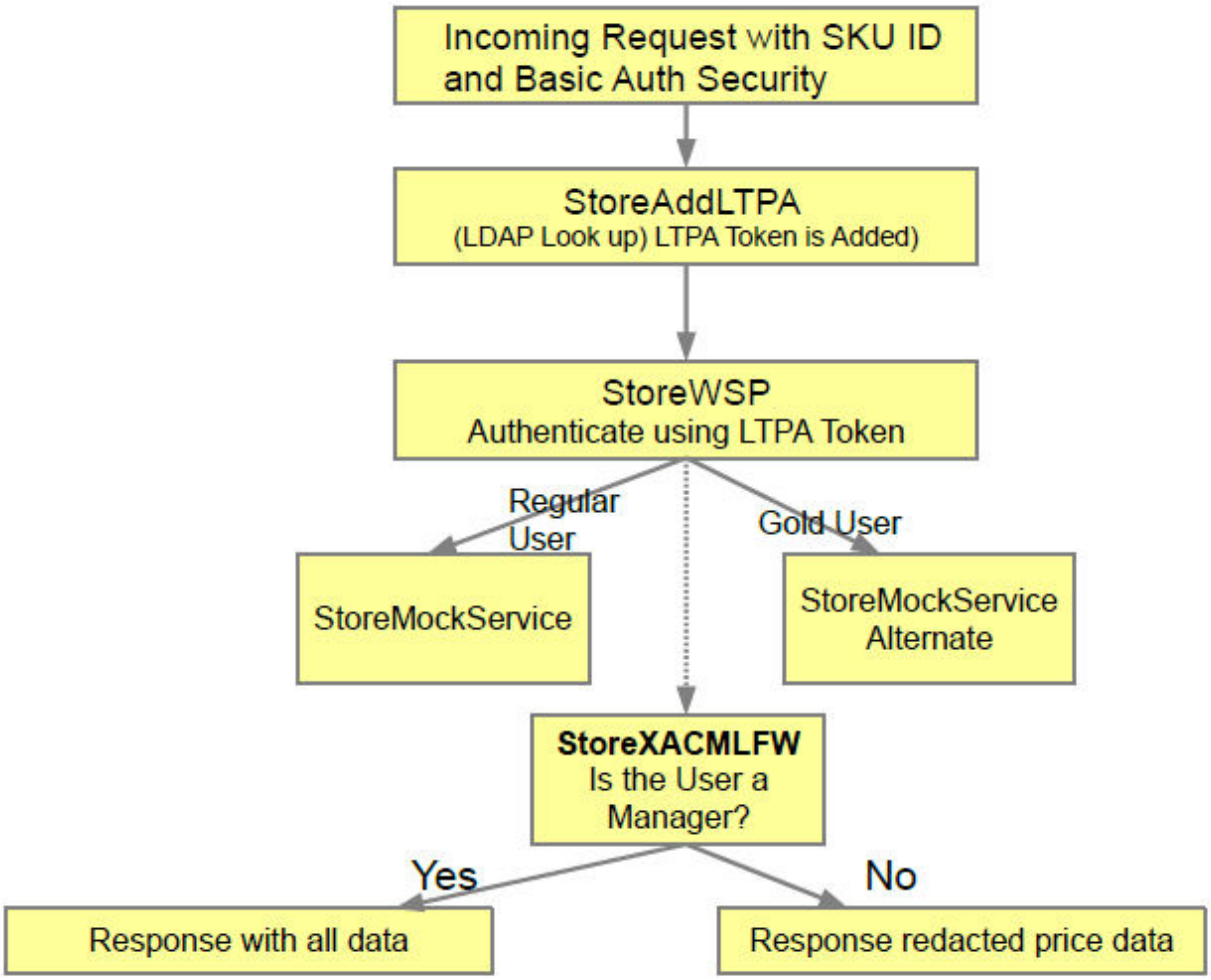


Figura 10. Diagrama de flujo de la aplicación de ejemplo

El servicio RESTful de ejemplo

El servicio RESTful está gobernado de forma similar al servicio web, excepto en cómo se utilizan las políticas. Con el servicio web hay dos SLA: una para clientes Silver y una para clientes Gold. Sin embargo, para el servicio REST, no existen políticas asociadas al nivel SLD (aplicado a todas las solicitudes). En su lugar, hay una política asociada a cada SLA. El SLA Gold tiene una política que rechaza mensajes después de realizar 5 solicitudes en 9 segundos, y Silver permite 2 solicitudes en 90 segundos antes de rechazar.

Visión general de los artefactos de WSRR del ejemplo

Los artefactos de WSRR que describen el servicio Store se describen aquí. Los artefactos para el servicio REST siguen un patrón similar.

Bob's Warehouse es la organización propietaria del servicio Store proveedor y de la aplicación StoreConsumer consumidora.

Warehouse Business Service es el objeto bajo el que residen todas las versiones del servicio Store. La versión del servicio Store representa una versión específica del

servicio Store. Esta versión es el servicio que se proporcionan para reutilizar. La definición de nivel de servicio Store (SLD) tiene dos políticas asociadas; la primera política rechaza los mensajes después de recibir 5 mensajes en el plazo de 90 segundos y la segunda política realiza una validación por comparación con el esquema Store.wsdl. Estas políticas significan que las solicitudes para el servicio Store se han validado, y se permiten un máximo de 5 solicitudes para el servicio en cualquier periodo de 90 segundos, independientemente de quién proceda la solicitud. El SLD también tiene un acuerdo de nivel de servicio (SLA) anónimo. Cualquier política asociada a este a este se SLA se aplica cuando las solicitudes que entran no tienen ningún SLA coincidente. Un SLA coincide si se cumplen las siguientes condiciones:

- Hay una versión Application consumidora que coincide con el ID de consumidor de la solicitud.
- Hay un SLA en vigor entre esta versión de aplicación consumidora y el SDL para el servicio que se consume, que coincide con el ID de contexto de la solicitud.

La aplicación empresarial StoreConsumer representa la aplicación StoreConsumer, mientras que la versión StoreConsumer Application es una versión específica de esta aplicación. Esta aplicación es el consumidor: está reutilizando el servicio Store. Tiene el ID de consumidor de “CEO”. Hay dos SLA vigentes para esta aplicación, que constituyen un acuerdo para permitir que esta aplicación consuma el servicio Store. Uno tiene el ID de contexto “Gold”, lo que significa que coincide con las solicitudes de la aplicación StoreConsumer, que tiene el ID de contexto de “Gold” en la solicitud, y una coincide con Silver. El SLA Gold tiene una política asociada para redirigir solicitudes, por lo que cualquier solicitud de la aplicación StoreConsumer que tenga un ID de contexto establecido en Gold se redirigirá al punto final especificado en la política. El SLA Silver no tiene políticas asociadas, por lo que su existencia significa que las solicitudes de la aplicación StoreConsumer que tengan un ID de contexto de Silver tienen permiso para pasar, aunque haya ninguna política aplicada.

En este ejemplo, hay una política de notificaciones asociada al SLA anónimo.

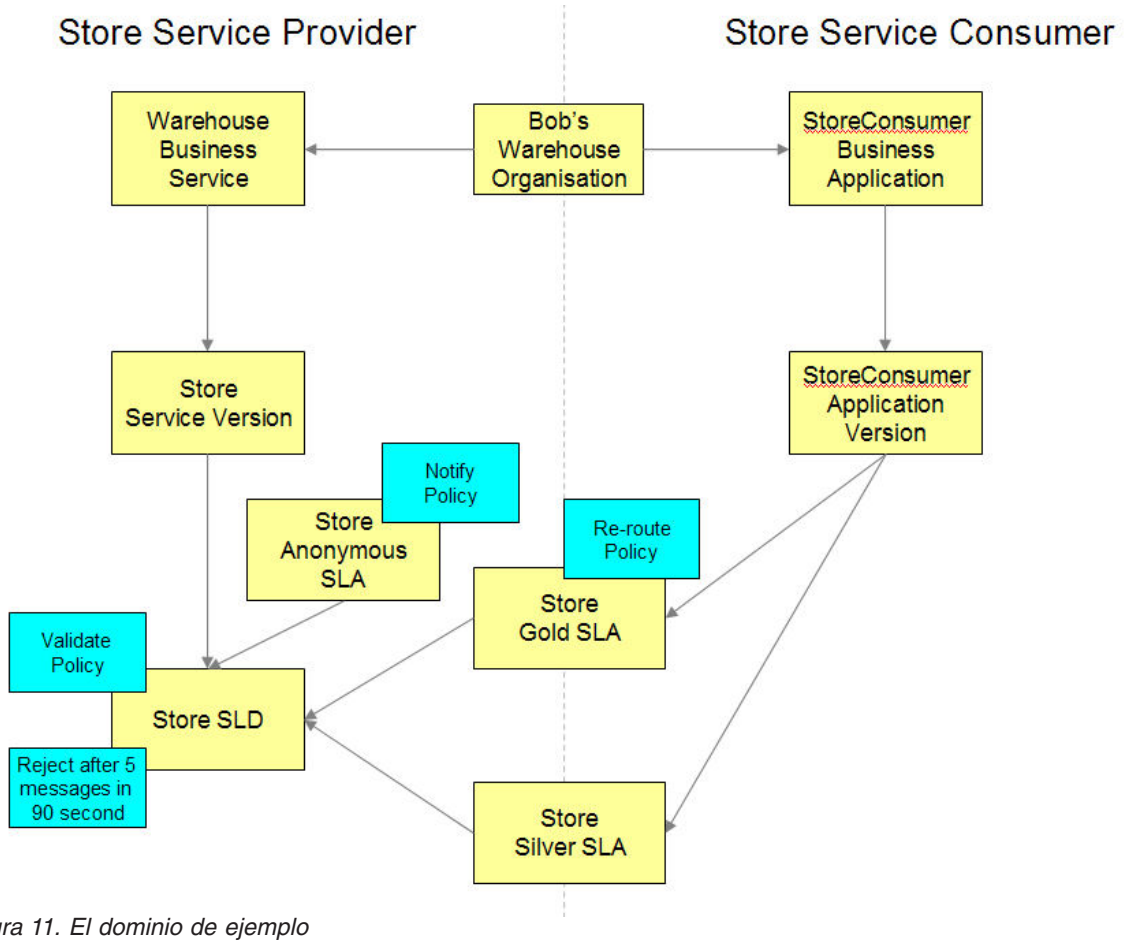


Figura 11. El dominio de ejemplo

Ejecución de los casos de prueba de ejemplo

Puede utilizar la aplicación web de ejemplo o la línea de mandatos para probar la aplicación de ejemplo en el SOA Policy Gateway Basic Runtime Sample desplegado. Seis variaciones de prueba de línea de mandatos se pueden ejecutar en la aplicación de ejemplo.

Para desplegar el tiempo de ejecución de ejemplo básico, consulte "Despliegue del patrón de ejemplo de tiempo de ejecución básico" en la página 49.

Ejecución del caso de prueba de la aplicación web de ejemplo

Para ejecutar el caso de prueba de la aplicación web:

1. Encuentre el nombre de host del entorno WSRR desplegado abriendo la instancia de sistema virtual desplegada. Para encontrar el nombre de host, expanda la sección **Máquinas virtuales** y seleccione la máquina virtual del servidor autónomo WSRR para ver los detalles de la máquina virtual. En la sección **Hardware y de red**, el nombre de host es el valor de **Interfaz de red 0**.
2. Abra el URL en un navegador Web: `http://<nombre_host_wssr>:9080/SoaPolicyTester`
3. Están disponibles las opciones siguientes:

- **Solicitud estándar**: envía una solicitud findInventory al servicio de almacén. El ID de contexto es Silver. El ID de consumidor es CEO. Un resultado exitoso muestra el texto “Part: SKU10 Price: 401.73”.
- **Prueba de política de direccionamiento**: igual que Solicitud estándar pero con ID de contexto Gold. La solicitud se dirige a un punto final que ejecuta el servicio. Un resultado exitoso devuelve “Part: GOLDSKU10 Price: 401.73”.
- **Prueba de política de validación**: envía una solicitud con una carga útil no válida. La política de validación solicita que DataPower valide la solicitud y rechace aquellos mensajes que no sean válidos. Un resultado exitoso es un mensaje de respuesta de DataPower `"Internal Error (from client)"`.
- **REST Gold**: envíe la solicitud al servicio SKU RESTful con CEO de ID de cliente e ID de contexto Gold. Las solicitudes Gold están sujetas a una política que permite solo 5 mensajes en 90 segundos. Una solicitud exitosa muestra el resultado “Part: SKU33 Price: 136.43”.
- **REST Silver**: Igual que Rest GOLD, pero con el ID de contexto Silver. Las solicitudes Silver permiten 3 solicitudes separadas en 90. Una solicitud exitosa muestra el resultado “Part: SKU33 Price: 136.43”.
- **ID de usuario**: la opción ID de usuario tiene dos posibles valores; Contenido completo o Contenido redactado. Cada opción crea solicitudes provenientes de distintos usuarios. El ejemplo utiliza una política XACML, que permite ver el precio solo a los Gestores. El valor de Precio en el mensaje de respuesta se redacta a menos que se seleccione Contenido completo. Un resultado exitoso para solicitudes cuando se selecciona Contenido relacionado contiene “Price: 0.0”. El servicio RESTful no da soporte a la redacción. El usuario seleccionado no tiene ningún efecto.

4. Abra la consola de WSRR y explore el servicio y las políticas. Para obtener más información, consulte “Conexión a WSRR - Business Space” en la página 82.

El ejemplo se puede poner en práctica utilizando la línea de mandatos. Esta es la única manera de enviar tráfico que utiliza el acuerdo de nivel de servicio anónimo

Demostración de Permitir/Denegar de XACML en el escenario Redacción utilizando la línea de mandatos

La siguiente solicitud XML se puede enviar al servicio StoreAddLTPA de DataPower:

```
<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>
```

Presuponiendo que el XML de la solicitud de ejemplo está contenido en un archivo denominado `silver.xml`, especifique el siguiente mandato curl:

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

En este ejemplo, ConsumerX es Manager, por lo tanto, se visualizará la información de precio completo en la respuesta:

```
<?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>
```

Ejecución del escenario Redacción utilizando la línea de mandatos

ConsumerA no es Manager, por lo tanto, se visualizará una respuesta diferente. Especifique el mandato curl:

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

Tenga en cuenta que la respuesta tiene el precio redactado. El precio se visualiza como 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>
```

Prueba de la política de direccionamiento utilizando la línea de mandatos

Para la política de direccionamiento conectada al SLA de Gold que se aplicará, el ID de contexto y el ID de consumidor deben coincidir. En este caso, el SLA para los Clientes Gold tiene el ID de consumidor de CEO. El siguiente es el contenido de la solicitud de ejemplo (puede ver que es necesario que el ID de contexto y el ID de consumidor coincidan):

```
<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>
```

Presuponiendo que el XML de la solicitud de ejemplo está contenido en un archivo denominado `gold.xml`, especifique el siguiente mandato curl:

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

La respuesta es la siguiente:

```
<?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>
```

Tenga en cuenta la respuesta de retorno tiene `GOLDSKU` como valor de SKU, lo que indica que se ha utilizado el punto final Gold.

Prueba de la validación del esquema utilizando la línea de mandatos

La política de validación comprueba el esquema de la solicitud en el Store.wsdl y su Company.xsd asociado.

El XML siguiente, `badvalid.xml`, muestra una solicitud que no es válida debido a que el cuerpo contiene un elemento denominado `<skubad>`, cuando éste debería ser `<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 especifica la siguiente solicitud curl:

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

Se visualiza el siguiente error:

```
<?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>
```

Prueba del rechazo en la política de mediación utilizando la línea de mandatos

Una de las políticas de mediación incluida en el rechazo de las pruebas de ejemplo después de que el recuento de mensajes se ejecute 5 veces en 90 segundos. Ejecute el mandato siguiente 6 veces:

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

La solicitud de ejemplo es la siguiente:

```
<?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>
```

En este caso, ConsumerX es Manager, por lo tanto, se mostrará la información completa de precios para las cinco primeras ejecuciones:

```
<?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>
```

En la sexta ejecución, se produce el siguiente error:

```
<?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>
```

Nota: Es posible que detecte este error antes si ejecuta otras pruebas dentro del intervalo de 90 segundos.

Prueba de la notificación en la política de mediación utilizando la línea de mandatos

La política de notificaciones se adjunta al SLA anónimo. Este se aplica cuando una solicitud viene de un consumidor que no tiene un SLA vigente. En este ejemplo, el único consumidor que tiene SLA vigentes es CEO, por lo que una solicitud que contiene el ID de consumidor establecido en otra cosa provocará que se aplique de la política en el SLA anónimo. En este caso ConsumerX es Manager, por lo tanto, se visualizará la información de precio completo:

Para probar esta funcionalidad utilizando la línea de mandatos, cree un archivo denominado `anon.xml` que contenga el siguiente xml:

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

A continuación, especifique el mandato siguiente:

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

Se registra el mensaje siguiente en el archivo de registro predeterminado del dominio:

```
Notify action triggered ('operation_38_2_sla1-1-filter_1-notify') from source policy (
   'LogEveryTime_287d0790-83d9-11e1-a255-9187e20cddb0_05aec6ec-3674-4165-85de-a0f7be48a938'
```

Nota: El registro debe establecerse en “aviso” para ver este mensaje. Si no lo está, pulse el icono **Resolución de problemas** en la consola web de DataPower. En la sección Registro, cambie el valor de Nivel de registro a “aviso” y pulse **Establecer nivel de registro**. Para encontrar el registro, vuelva al panel de control y pulse el icono **Ver registros**.

Prueba del servicio RESTful mediante la línea de mandatos

También puede acceder a la interfaz RESTful desde la línea de mandatos mediante curl. Como con el cliente web, un ID de contexto Gold permite 5 mensajes en 90 segundos y Silver solo 2 mensajes.

Para probar esta funcionalidad utilizando la línea de mandatos, cree un archivo denominado restRequest.xml, que contenga el siguiente xml:

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

A continuación, especifique el mandato siguiente para probar con el ID de contexto Gold:

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

Para probar con el ID de contexto Silver, utilice el mismo mandato pero sustituya Gold por Silver.

Un respuesta correcta es:

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

Si traspasa el umbral, recibirá el siguiente mensaje:

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

Para aplicar el SLA anónimo al servicio RESTful, que simplemente tiene una política de notificación adjunta, utilice cualquier ID de contexto o ID de consumidor distinto al registrado. La notificación aparece en el registro de DataPower, como se describe anteriormente en el ejemplo de Servicios web.

Tareas relacionadas:

"Despliegue del patrón de ejemplo de tiempo de ejecución básico" en la página 49
Cuando se despliega el patrón SOA Policy Gateway Basic Runtime Sample se crea una instancia de sistema virtual en ejecución del patrón. Este patrón sólo está disponible en sistemas x86.

Ampliación de la aplicación de ejemplo

La aplicación de ejemplo se puede modificar modificando la hoja de estilo de enlaces y las hojas de estilo XSL.

Modificaciones de la hoja de estilo Enlaces

La variable xacml-subjects se ha añadido a la hoja de estilo `apil-xacml-binding-new.xsl`. Esta abarca la creación de la sección de asuntos de la solicitud. Posteriormente, se accede a esta variable en `sendToPDP.xsl`.

```
<xsl:variable name="xacml-subjects">
  <xacml-context:Subject
  SubjectCategory="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject">
<!--
*************************************************
Starting here, use the MC result as subject.
*************************************************
```

sendToPDP.xsl

Esta hoja de estilo llama a StoreXACMLFW utilizando url-open. La llamada se dirige a otro cortafuegos XML, por lo que no se utiliza ningún perfil proxy SSL. Para mover el punto de decisión de política (PDP) a otro buzón DataPower, se podría crear un perfil proxy SSL y utilizarlo con la llamada 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>
-->
- <!--
building the XACML request for masking
-->
<xsl:variable name="customized-request">
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
<soapenv:Header />
<soapenv:Body>
<xacml-context:Request xmlns:wsa="http://www.w3.org/2005/08/addressing"
  xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xacml-context="urn:oasis:names:tc:xacml:2.0:context:schema:os"
xmlns:ws="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
wss-wssecurity-secext-1.0.xsd">
- <!--
copy in the subjects saved from AAA request processing
-->
<xsl:copy-of select="dp:variable('var://context/snip/xacml/xacmlSubjects')/*" />
<xacml-context:Resource>
<xacml-context:ResourceContent>
<xsl:copy-of select="./soap:Envelope/soap:Body" />
</xacml-context:ResourceContent>
<xacml-context:Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#string">
<xacml-context:AttributeValue>PriceInfo</xacml-context:AttributeValue>
</xacml-context:Attribute>
</xacml-context:Resource>
<xacml-context:Action>
<xacml-context:Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
DataType="http://www.w3.org/2001/XMLSchema#string">
<xacml-context:AttributeValue>View</xacml-context:AttributeValue>
</xacml-context:Attribute>
</xacml-context:Action>
<xacml-context:Environment>
<xacml-context:Attribute AttributeId="ContextId" DataType="http://www.w3.org/2001/XMLSchema#string"
Issuer="http://security.tivoli.ibm.com/policy/distribution">
<xacml-context:AttributeValue>StorePriceData</xacml-context:AttributeValue>
</xacml-context:Attribute>
```

```
</xacml-context:Environment>
</xacml-context:Request>
</soapenv:Body>
</soapenv:Envelope>
</xsl:variable>
- <!--
Use set-variable so that it is visible in Probe, which is convenient
-->
<dp:set-variable name="'var://context/snip/xacml/BacksideXacmlRequest'" value="$customized-request" />
- <!--
Report the XACML-REQUEST to the debug log
-->
<xsl:message dp:priority="debug">
<XACML-REQUEST>
<xsl:copy-of select="$customized-request" />
</XACML-REQUEST>
</xsl:message>
<xsl:variable name="headers">
<header name="SOAPAction">xacml:authorization</header>
</xsl:variable>
- <!--
Call the XACML PDP for decision
-->
<xsl:variable name="rtss-response">
<xsl:variable name="StoreGWURL">
<xsl:value-of select="concat('http://','127.0.0.1',':',$StoreGWPort,'/rtss/authz/services/AuthzService')" />
</xsl:variable>
<dp:url-open target="{$StoreGWURL}" http-headers="$headers" response="responsecode">
<xsl:copy-of select="$customized-request" />
</dp:url-open>
</xsl:variable>
- <!--
Use set-variable so that it is visible in Probe, which is convenient
-->
<dp:set-variable name="'var://context/snip/xacml/BacksideXacmlResponse'" value="$rtss-response" />
- <!--
Report the XACML-RESPONSE to the debug log
-->
<xsl:message dp:priority="debug">
<XACML-RESPONSE>
<xsl:value-of select="$rtss-response" />
</XACML-RESPONSE>
</xsl:message>
</xsl:template>
</xsl:stylesheet>
```

Observe los puntos siguientes sobre el archivo `sendToPDP.xsl`:

1. La hoja de estilo obtiene el puerto para XACMLFW de `soavars.xsl`.
2. Se espera que la variable rtssResponse tenga exactamente el formato utilizado por Runtime Security Services y, a su vez, el formato que el PDP de DataPower puede procesar.
3. La hoja de estilo construye una solicitud SOAP. La información del asunto se crea mediante la hoja de estilo `apil-binding.xsl` anterior, la cual se obtiene mediante la copia de la solicitud de selección siguiente:

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

4. La acción es simplemente para ver la acción: `<xacml-context:AttributeValue>View</xacml-context:AttributeValue>`
5. El entorno es StorePriceData, conocido como objeto de aplicación en la terminología de IBM Tivoli Security Policy Manager o Runtime Security Services.

StorePrivateDataXACML.xml

El siguiente código muestra la hoja de estilo de política para redacción.

```
<PolicySet PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:deny-overrides"
PolicySetId="RPS:StorePrivateData:policy:dc703409-d408-49b3-acc1-16c89c844fce:rolec4a9f664-a0af-451b-b80b-
1cafdb9fd9f0:role:2884ab77-58d1-4b1d-8728-7d528169d608" Version="1.0">
<Target>
<Subjects>
<Subject>
<SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
<xacml:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"
xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os">MANAGER</xacml:AttributeValue>
<SubjectAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role"
DataType="http://www.w3.org/2001/XMLSchema#string"
SubjectCategory="urn:oasis:names:tc:xacml:1.0:subject-category:accesssubject"
/>
</SubjectMatch>
</Subject>
</Subjects>
</Target>
<Policy PolicyId="PPS:StorePrivateData:dc703409-d408-49b3-acc1-16c89c844fce:c4a9f664-a0af-451b-
b80b-1cafdb9fd9f0:c4a9f664-a0af-451b-b80b-1cafdb9fd9f0:pps"
RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-applicable"
Version="1.0">
<Target>
<Resources>
<Resource>
<ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
<xacml:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"
xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os">PriceInfo</xacml:AttributeValue>
<ResourceAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#string" />
</ResourceMatch>
</Resource>
</Resources>
<Actions>
<Action>
<ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
<xacml:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"
xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os">View</xacml:AttributeValue>
<ActionAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
DataType="http://www.w3.org/2001/XMLSchema#string" />
</ActionMatch>
</Action>
</Actions>
</Target>
<Rule Effect="Permit" RuleId="PPS:StorePrivateData:dc703409-d408-49b3-acc1-16c89c844fce:c4a9f664-a0af-451b-
b80b-1cafdb9fd9f0:c4a9f664-a0af-451b-b80b-1cafdb9fd9f0:pps:rules:0">
<Target />
</Rule>
</Policy>
</PolicySet>
</PolicySet>
```

Observe los puntos siguientes:

- El rol debe ser Manager:

```
<xacml:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"
xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os">MANAGER</xacml:AttributeValue>
```

- El recurso debe ser 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>
```

- La acción debe ser 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>
```

Modificación de las hojas de estilo XSL de ejemplo

Puede modificar la hoja de estilo de redacción, `noPriceInfo.xsl`

Procedimiento

Modifique la hoja de estilo de redacción.
La hoja de estilo `noPriceInfo.xsl` contiene el código siguiente, que sustituirá cualquier valor de precio por ceros. Puede añadir otros campos a la lógica de redacción o añadir transformaciones más complicadas que impliquen cálculos para determinar los valores de los campos.

```
<!-- private access only fields -->
<xsl:template match="price">
<price>0.0</price>
</xsl:template>
<xsl:template match="Price">
<Price>0.0</Price>
</xsl:template>
```

Posteriormente, la hoja de estilo realiza una transformación de identidad en todos los demás elementos.

Exploración adicional del ejemplo

Para conocer más sobre el ejemplo, puede configurar el punto de decisión de política (PDP) de XACML en DataPower y editar documentos de política.

Alteración del PDP XACML en DataPower

Puede alterar el XACML utilizado para el PDP (punto de decisión de política) de seguridad en DataPower para obtener más información sobre el control de accesos con XACML.

Procedimiento

Para cambiar o añadir un PDP:

1. En el Panel de control de DataPower, busque `PDP XACML`.
2. Pulse en un PDP existente o pulse **Añadir**.
3. Escriba un URL, por ejemplo, `local:///storePrivateDataXACML.xml`.
4. Añada cualquier archivo dependiente o de directorio necesario para dar soporte a la política.

   Nota: Si edita un archivo de política XACML directamente en el sistema de archivos, debe volver a la definición del PDP y volver a entrar el URL, o cualquier cosa que haya modificado, o debe reiniciar el dominio para que los cambios entren en vigor.

Cómo añadir nuevos documentos de política o editar los existentes

Utilice la interfaz de usuario de Business Space para añadir nuevos documentos de política o editar los existentes.

Antes de empezar

Configure el espacio de gobierno SOA. Para obtener más información, consulte "Configuración de Business Space para utilizarlo por primera vez" en la página 83.

Procedimiento

1. Cree una política de mediación con las condiciones y las acciones que necesite; por ejemplo, una condición de Número de mensajes > 5 mensajes en 5 minutos y una acción de rechazo. Para obtener más información sobre cómo crear una política de mediación, consulte "Creación de nuevas políticas de mediación" en la página 98.
2. Gobierne la política de mediación. Para obtener más información sobre el gobierno de una política de mediación, consulte "Gestión del ciclo de vida de la política" en la página 100.
   a. Pulse el documento de política en el navegador del registro de servicio o búsquelo en el widget de búsqueda. Las acciones se mostrarán en el editor de documentos de política.
   b. Pulse **Proponer especificación**.
   c. Pulse **Aprobar especificación**.

   Se aprobará la política. Puede volver a definir, reemplazar o dejar de utilizar la política para gestionar el ciclo de vida o editar una definición existente.
3. Adjunte la política. En Business Space, busque el SLD o SLA al que desea adjuntar la política. En el ejemplo hay cuatro sitios donde podría hacerlo.
   - Store SLD: adjunte la política aquí si desea que se aplique a cualquier uso del servicio Store.
   - Gold SLA - adjunte la política aquí si desea que se aplique solo a solicitudes Gold desde el consumidor CEO.
   - Silver SLA - adjunte la política aquí si desea que se aplique solo a solicitudes Silver desde el consumidor CEO.
   - SLA anónimo - adjunte la política aquí si desea que se aplique a cualquier solicitud procedente de consumidores que no sean CEO.

Tareas relacionadas:

"Creación de nuevas políticas de mediación" en la página 98
Puede crear nuevas políticas de mediación utilizando la interfaz de usuario de Business Space. Cuando cree las políticas de mediación, especifique las condiciones y las acciones para la política.

"Gestión del ciclo de vida de la política" en la página 100
Las políticas se pueden cambiar de un estado de gobierno a otro utilizando la interfaz de usuario de Business Space. Las políticas deben estar en el estado Aprobado para que DataPower las aplique.

Información relacionada:

Information Center de IBM WebSphere Service Registry and Repository, Versión 8.0 - Utilización de la interfaz de usuario de Business Space

El dominio DataPower de ejemplo

El patrón proporciona un dominio DataPower de ejemplo, que le permite comenzar a utilizar el patrón. Como desarrollador de DataPower, puede utilizar las pasarelas existentes como plantilla para sus propias aplicaciones. El entorno de ejemplo contiene cinco pasarelas. Hay una pasarela principal para el servicio Store, y cuatro pasarelas de soporte que proporcionan aplicaciones de fondo a las que

puede llamar la pasarela Store, soporte XCAML para un escenario de redacción y un extremo frontal que proporciona funciones de seguridad adicionales.

Proxy de servicio web de tienda

El Proxy de servicio web (WSP) de tienda es la pasarela principal del dominio de aplicación. El proxy recibe una solicitud con una señal LTPA asociada.

Cuando se solicita, la regla de proceso de la solicitud realiza las acciones siguientes:

1. Valida la solicitud, de acuerdo con lo solicitado por la política de validación. Para obtener más información, consulte "Visión general de los artefactos de WSRR del ejemplo" en la página 59.
2. Encamina la solicitud hacia el punto final alternativo si el acuerdo de nivel de servicio (SLA) es "Gold".
3. Realiza la autenticación, autorización y contabilidad (AAA) para la solicitud. La autenticación incluye las siguientes acciones:
   a. Autentica al usuario con una señal LTPA.
   b. Compara las credenciales con el servidor LDAP que proporciona información sobre los grupos a los que pertenece el cliente. Estos grupos son Manager, Clerk y Customer.
   c. Transforma los datos de entrada proporcionados en un objeto de solicitud que el punto de decisión de política (PDP) XACML puede comprender.
   d. Realiza la autorización mediante un PDP XACML en el dispositivo DataPower, con un documento de política XACML que se puede crear en el Gestor de políticas de seguridad de IBM Tivoli. El criterio de la política es que el usuario debe ser un Manager, Customer o Clerk. Para la operación findInventory, las devoluciones deben ser realizadas por usuario que sea Manager o Clerk, y las compras pueden ser realizadas por los usuarios Customer.
4. Define el valor ConsumerID utilizando un script XSL.
5. Elimina la cabecera de seguridad HTTP completa de la solicitud.
6. Invoca el programa de fondo del servicio Store.

Cuando se procesa la solicitud, la regla de proceso de respuesta realiza las acciones siguientes:

1. Llama a la pasarela StoreXACMLFW, la cual actúa como el PDP en la situación.
2. De acuerdo con la respuesta, se escribe el campo de información de precio (poner a cero) dependiendo de si el usuario tiene el rol de Manager.

Cortafuegos XML definidos en el ejemplo

Los cortafuegos XML siguientes están definidos en el ejemplo.

Cortafuegos XML StoreAddLTPA

La función del cortafuegos XML StoreAddLTPA es proporcionar un componente frontal con un puerto al que los usuarios pueden llamar utilizando sólo la autenticación básica (por ejemplo, sin LTPA). La regla de proceso de la solicitud:

1. Identifica con la autenticación básica.
2. Autentica con una búsqueda LDAP sencilla.
3. Añade una señal LTPA como parte del proceso posterior.
4. Envía la solicitud a la política de seguridad StoreWSP con la información LTPA ahora asociada.

Cortafuegos XML StoreMockService

StoreMockService es un servicio de ejemplo que utiliza un cortafuegos XML como implementación. Las operaciones findInventory, compra y devolución están todas ellas soportadas. Los valores de respuesta son estáticos. Este servicio de ejemplo se crea cuando no es posible incluir un WebSphere Application Server en el patrón. Las tres reglas de solicitud de la política utilizan una acción de comparación para determinar la operación de solicitud y, basándose en una coincidencia, responden con una respuesta SOAP estática. Las respuestas SOAP estáticas se proporcionan de acuerdo con la operación de solicitud, en lugar de una implementación de servicio completo.

Cortafuegos XML StoreMockServiceAlternate

StoreMockServiceAlternate es un servicio de ejemplo que utiliza un cortafuegos XML como implementación. Las operaciones findInventory, compra y devolución están todas ellas soportadas. Este servicio se utiliza para demostrar que se aplica la política de direccionamiento.

Cortafuegos StoreXACMLFW

Este escenario realiza la redacción de acuerdo con el resultado de un mecanismo de permitir/denegar basado en XACML. En DataPower, no es posible invocar una acción AAA individual en el flujo de respuesta. Se crea una pasarela separada para contener el punto de decisión de política (PDP) de XACML. Este PDP se ha encapsulado en una acción AAA en la regla de solicitud de StoreXACMLFW.

StoreXACMLFW es una pasarela de cortafuegos XML en DataPower. Se utiliza esta implementación porque es una manera sencilla de proporcionar la funcionalidad. El cortafuegos StoreXML utiliza la misma interfaz WSDL que el servidor Tivoli Runtime Security Services. La pasarela StoreWSP crea el objeto de solicitud y lo envía, protegido mediante SSL, a la pasarela StoreXMLFW.

La regla de solicitud del cortafuegos StoreXML efectúa las siguientes tareas:

1. Realiza la acción AAA utilizando la información SSL para autenticación.
2. Realiza la autorización utilizando un PDP de XACML incluido. La política que utiliza el PDP se crea originalmente en IBM Tivoli Security Policy Manager, pero se puede volver a crear utilizando un editor estándar, y el esquema se define en la especificación XACML.
3. No es necesario realizar ninguna transformación de la solicitud en este proceso de autorización.
4. Si la solicitud XACML es válida, la regla de proceso de solicitud captura una respuesta Permitir y la devuelve al cliente. En otro caso, se produce una excepción que se maneja mediante la regla de proceso de excepciones y se devuelve una respuesta Denegar al cliente.

Nota: Permitir/Denegar/Indeterminada es únicamente una respuesta a nivel de ejemplo. Se puede incluir información de error adicional en un flujo específico del cliente.

Política de seguridad XACML

En este tema se describe cómo se crean los documentos XACML.

Los documentos XACML utilizados en el ejemplo se han creado mediante el editor de políticas IBM Tivoli Security Policy Manager, pero puede utilizar cualquier

editor de texto o XML para crear los documentos. Para crear o modificar las políticas XACML existentes, consulte las especificaciones de OASIS: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml.

La política de seguridad de XACML utilizada en el ejemplo está contenida en `storeSWPXACML.xml` y `storePrivateDataXACML.xml`. Estas políticas se utilizan para evaluar la solicitud que llega al punto de decisión de política (PDP). La solicitud consta de cuatro elementos clave :

1. La sección Subjects: contiene el nombre distinguido del emisor de la solicitud, así como los grupos a los que pertenece.
2. La sección de recursos: contiene los documentos a los que el emisor desea tener acceso. En el ejemplo se utilizan dos tipos de recursos. El primer tipo es la operación en el servicio web y el segundo tipo es la autorización para los datos de la respuesta, que, en este caso, es priceInfo.
3. La sección Environment: contiene información sobre el entorno de la solicitud.
4. La acción: lo que el usuario desea realizar con el material autorizado. En el escenario de redacción, la acción es simplemente ver los datos de priceInfo.

Política de seguridad StoreWSP

La política de seguridad del archivo `storeSWPXACML.xml` correlaciona grupos con operaciones de servicio web.

Una política de seguridad de ejemplo tiene el aspecto siguiente:

```
<PolicySet PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:denyoverrides"
PolicySetId="RPS:Store:policy:aed2df4e-4159-4df0-ada2-f148d9b56cef:roled200c213-27f9-
4d17-8305-b0d3ca8fcf54:role:09b60522-76b8-4280-9c1a-31d026441164" Version="1.0">
<Target>
<Subjects>
<Subject>
<SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:x500Name-equal">
<xacml:AttributeValue DataType="urn:oasis:names:tc:xacml:1.0:data-type:x500Name"
xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os">CN=MANAGER, CN=groups,
DC=ibm.com</xacml:AttributeValue>
<SubjectAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:subject:group-id"
DataType="urn:oasis:names:tc:xacml:1.0:data-type:x500Name"
SubjectCategory="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject" />
</SubjectMatch>
</Subject>
<Subject>
<SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
<xacml:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"
xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os">MANAGER</xacml:AttributeValue>
<SubjectAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role"
DataType="http://www.w3.org/2001/XMLSchema#string"
SubjectCategory="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject" />
</SubjectMatch>
</Subject>
</Subjects>
</Target>
<Policy PolicyId="PPS:StoreSOAP:findInventory:aed2df4e-4159-4df0-ada2-f148d9b56cef:d200c213-27f9-
4d17-8305-b0d3ca8fcf54:d200c213-27f9-4d17-8305-b0d3ca8fcf54:pps"
RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-applicable"
Version="1.0">
<Target>
<Resources>
<Resource>
<ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
<xacml:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"
xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os">{http://company.ibm.com/store}findInventory</xa
cml:AttributeValue>
<ResourceAttributeDesignator AttributeId="urn:ibm:xacml:profiles:web-services:1.0:wsdl:1.1:operation"
```

```
DataType="http://www.w3.org/2001/XMLSchema#string" />
</ResourceMatch>
<ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
<xacml:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"
xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os">{http://company.ibm.com/store}StoreSOAP</xac
ml:AttributeValue>
<ResourceAttributeDesignator AttributeId="urn:ibm:xacml:profiles:web-services:1.0:wsdl:1.1:port"
DataType="http://www.w3.org/2001/XMLSchema#string" />
</ResourceMatch>
<ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
<xacml:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"
xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os">{http://company.ibm.com/store}Store</xacml:Attr
ibuteValue>
<ResourceAttributeDesignator AttributeId="urn:ibm:xacml:profiles:web-services:1.0:wsdl:1.1:service"
DataType="http://www.w3.org/2001/XMLSchema#string" />
</ResourceMatch>
</Resource>
</Resources>
</Target>
```

Nota: En la sección Subjects, existe una coincidencia para el nombre x500 o el rol Manager. Si examina el archivo de política `.xml` completo, podrá ver que existen correlaciones similares para Customer y Clerk. Podrá ver que la operación findInventory puede utilizar los tres grupos de usuarios, mientras que las operaciones returnProduce y purchase están limitadas sólo a determinados grupos.

La pasarela Redaction

Detalles sobre la hoja de estilo storeCallPDP.xsl.

Examine la hoja de estilo storeCallPDP.xsl, y observe los puntos siguientes:

1. La inclusión de la hoja de estilo storeSendToPDP.xsl. Esta hoja de estilo contiene la lógica para llamar a storeXAMLFW.
2. La inclusión de la llamada a la plantilla call_PDP dentro de storeSendToPDP.
3. La extracción de la decisión a partir de la respuesta de la llamada, por ejemplo, “Permit”.
4. El valor de `var:/context/response/displayfilter` para las hojas de estilo allData.xsl o noPriceInfo.xsl.
5. La estructura de XACML para la Reacción, storePrivateDataXACML.xml, es casi idéntica a la estructura utilizada en el escenario StoreWSP. La diferencia es que sólo el rol Gestor tiene acceso.

storeCallPDP.xsl

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

```
      <xsl:when test="$decision = 'Permit'">
        <xsl:message dp:priority="debug">****** SETTING THE PRIVATE FILTER ********</xsl:message>
        <dp:set-variable name="'var://context/response/displayFilter'" value="'local:///allData.xsl'" />
      </xsl:when>
      <xsl:otherwise>
        I<dp:set-variable name="'var://context/response/displayFilter'" value="'local:///noPriceInfo.xsl'" />
      </xsl:otherwise>
    </xsl:choose>
  </xsl:template>
</xsl:stylesheet>
```

Artefactos de WSRR creados en el SOA Policy Gateway Basic Runtime Sample

Artefactos de WSRR creados en el patrón SOA Policy Gateway Basic Runtime Sample, cómo el ejemplo los utiliza.

Tabla 14. Artefactos de WSRR creados para el patrón SOA Policy Gateway Basic Runtime Sample

Objeto	Descripción
Organización	Bob's Warehouse. Esta es el área del negocio que pertenece al servicio Store.
Función empresarial	Warehouse. Esto representa todas las versiones del servicio Store, y pertenece a la organización Bob's Warehouse.
Versión de servicio	Store. Esto representa la versión 1.0 del servicio Store.
WSDL	Store.wsdl
XSD	Company.xsd
Política	• Validate.xml • RouteForGold.xml • LogEveryTime.xml • RejectAfter5MsgIn90Seconds.xml
SLD	Store SLD. Cualquier política asociada aquí se aplica a cualquier solicitud para este servicio.
Gold SLA	Gold SLA. La existencia de este SLA significa que las solicitudes gold del consumidor CEO no se cuentan como anónimas. Cualquier política aquí asociada se aplica en solicitudes gold del consumidor CEO.
Silver SLA	Silver SLA. La existencia de este SLA significa que las solicitudes silver del consumidor CEO no se cuentan como anónimas. Sin políticas asociadas, se permite que la solicitud pase.
Acuerdo de nivel de servicio Anonymous	Usuarios anónimos. Las políticas aquí asociadas se aplican a cualquier solicitud que no tenga un SLA coincidente en vigor. En este ejemplo, cualquier solicitud de un consumidor que no sea CEO, o cualquier solicitud de un CEO que no sea Gold o Silver, tiene las políticas de SLA anónimas aplicadas.

Artefactos de DataPower creados en el SOA Policy Gateway Basic Runtime Sample

Artefactos de DataPower creados en el patrón SOA Policy Gateway Basic Runtime Sample.

Tabla 15. Artefactos de DataPower creados para el patrón SOA Policy Gateway Basic Runtime Sample

Tipo	Nombre	Finalidad
Proxy de servicio web	StoreWSP	El servicio principal.
Cortafuegos XML	StoreAddLTPA StoreMockService StoreAlternateMockService StoreXACMLFW	Autentica y añade la señal LTPA. El proveedor de servicios para usuarios que no son Gold. El proveedor de servicios para usuarios Gold. Controla el acceso a PriceInfo.
Servidor WSRR	WSRRSVR	La conexión a WSRR.
Suscripción WSRR	StoreSub	Proporciona información de búsqueda para el espacio de nombres de WSRR, el objeto, etc.
Política AAA	StoreAddLTPA	Identificación y autenticación básica para LDAP. Busca la autenticación. Añade la señal LTPA a la solicitud.
Política AAA	StoreWSDLAAA	Identificación y autenticación LTPA. Correlación de grupos para la autorización. Autorización XACML.
Política AAA	StoreXACMLFWAZ	Autorización XACML para PriceInfo.
Perfil de proxy SSL	WSRRPP	Perfil proxy SSL para el servidor WSRR.
Perfil criptográfico	WSRRCP	Perfil criptográfico para el servidor WSRR.
Credenciales de validación	WSRRVC	Las credenciales de validación contienen el certificado criptográfico WSRRCERT. Todos los demás valores son valores predeterminados.
Certificado criptográfico	WSRRCERT	WSRRCERT utiliza el certificado de firmante. Este certificado se ha extraído de NodeDefaultKeyStore, que es el certificado predeterminado para un servidor individual, o desde el certificado predeterminado CMSKeyStore en el caso de un entorno ND en el que existía un IBM HTTP Server.

Reglas de proceso del proxy de servicio web StoreWSP

La pasarela central del ejemplo es StoreWSP. La política de la pasarela contiene una regla de solicitud y respuesta.

Regla de solicitud

La acción de política principal de StoreWSP_default_request-rule se denomina AAA. En la acción AAA, se valida la señal LTPA, se recuperan los grupos de

usuarios y se realiza una autorización para ver si el usuario está en el grupo Manager, Clerk o Customer de LDAP. Esta validación se lleva a cabo cuando el paso AZ de AAA llama al PDP (Policy Decision Point) StoreWSDLPDP en el dispositivo DataPower. Este PDP utiliza la política XACML storeWSPXACML.xml.

Regla de respuesta

En la regla de respuesta, StoreWSP_default_response-rule, la transformación llama al servicio cortafuegos XML StoreXACMLFW.

Esta transformación determina si el usuario tiene autorización para acceder a la información de precios basándose en si el usuario es miembro del grupo Manager. Si es así, la variable *var:///context/response/displayFilter* se establece en `local:///allData.xsl`. Si el usuario no es miembro del grupo Manager de LDAP, la variable *var:///context/response/displayFilter* se establece en `local:///noPriceInfo.xsl`.

A continuación, la transformación realiza las acciones de la hoja de estilo en la respuesta.

Reglas de proceso de StoreXAMLFW

La hoja de estilo personalizada storeSendToPDP.xsl realiza una llamada al FW XML local StoreXACMLFW. En este cortafuegos se utilizan dos reglas de proceso. StoreXACMLFW_request contiene una sola acción de política AAA que utiliza la transformación allData.xsl. Esta acción AAA, StoreXACMLFWAZ, a su vez llama a la acción XACML PDP StorePDP. Mediante la política XACML storePrivateDataXACML.xml, se determina si el usuario está autorizado para ver la información de precios.

Las hojas de estilo XSL de ejemplo

La aplicación de ejemplo contiene las hojas de estilo siguientes que terminan en `.xsl`, que se encuentran en el directorio local del dominio instalado.

Tabla 16. Hojas de estilo de la aplicación de ejemplo

Hoja de estilo	Finalidad
`allData.xsl`	Una hoja de estilo de identidad que copia todos los datos del origen en el destino. Se utiliza para la función de redacción para llamar a la pasarela XML XACML.
`apil-xacml-binding-new.xsl`	Utiliza la información de correlación de credenciales para crear una solicitud SOAP que puede ser procesada por el punto de decisión de política (PDP) del dispositivo DataPower. Esta hoja de estilo es una modificación de la hoja de estilo tspm-xacml-binding-sample.xsl que se proporciona en el directorio de almacenamiento del dispositivo DataPower. La funcionalidad clave que proporciona este script adaptado es añadir una variable accesible externamente que permite que la información de asunto de la solicitud XACML esté disponible en la hoja de estilo de redacción.
`noPriceInfo.xsl`	Esta hoja de estilo establece el elemento de precio en el valor 0.0.

Tabla 16. Hojas de estilo de la aplicación de ejemplo (continuación)

Hoja de estilo	Finalidad
rgxacml.xsl	Esta hoja de estilo es una personalización de la hoja de estilo tspm-retrieve-groups.xsl contenida en el directorio de almacenamiento del dispositivo DataPower. La finalidad principal de esta hoja de estilo es proporcionar el nombre de dominio LDAP, el nombre de host, la contraseña, el puerto, etc., de modo que se pueda buscar al usuario entrante y se pueda recuperar su información de grupo.
soavars.xsl	Esta hoja de estilo de ejemplo define la información LDAP de las variables utilizadas por la hoja de estilo rgxacml.xsl. En el ejemplo, la contraseña no está cifrada, lo cual no es una práctica utilizada en producción.
storeCallPDP.xsl	Esta hoja de estilo contiene el código para llamar a la pasarela XACML, gestiona la decisión permitir/denegar y establece la variable de filtro para ejecutar allData.xsl o noPriceInfo.xsl.
storeSendToPDP.xsl	Esta hoja de estilo crea una solicitud SOAP que se envía a la pasarela XACML. Incluye la información de asunto obtenida en la hoja de estilo apil-xacml-binding-new.xsl, la información de recursos, la información de acciones y la información de entorno.

Objetos DataPower que utilizan las hojas de estilo XSL

Los objetos DataPower utilizan algunas de las hojas de estilo XSL que se proporcionan con la aplicación de ejemplo.

Tabla 17. Objetos DataPower que utilizan las hojas de estilo XSL

Hoja de estilo	Finalidad
allData.xsl	Se utiliza internamente en la hoja de estilo storeCallPDP.xsl. La hoja de estilo se utiliza como transformación personalizada en la política AAA StoreXACMLFWAZ.
apil-xacml-binding-new.xsl	Se utiliza como hoja de estilo personalizada en el paso AZ de la política AAA StoreWSDLAAA.
noPriceInfo.xsl	Se utiliza internamente en la hoja de estilo storeCallPDP.xsl.
soavars.xsl	Se utiliza internamente en la hoja de estilo rgxacml.xsl.
storeCallPDP.xsl	Se invoca como una transformación en la regla Store_default-response.
storeSendToPDP.xsl	Se utiliza internamente en la hoja de estilo storeCallPDP.xsl.

Capítulo 6. Cómo trabajar con la instancia desplegada

Después de desplegar un Patrón IBM SOA Policy Gateway, puede visualizar la instancia desplegada pulsando **Instancias** > **Sistemas virtuales** en la consola de carga de trabajo.

Visualización de los detalles de la instancia

Puede ver los detalles de una instancia desplegada seleccionándola de la lista de instancias en la ventana Instancias de sistemas virtuales. Se muestran los detalles de la instancia de sistema virtual. Los detalles incluyen una lista de máquinas virtuales suministradas en la infraestructura de nube para este despliegue, la dirección IP y el estado de máquina virtual.

Para ver el estado de suministro y despliegue de la instancia, consulte el valor **Estado actual** en la vista de detalles.

Para ver el estado de las máquinas virtuales y scripts durante el suministro, expanda la sección **Historial** en la vista de detalles.

Para ver los detalles de las máquinas virtuales y los registros de scripts durante el suministro, expanda la sección **Historial** en la vista de detalles. El host y la dirección IP del sistema es el valor de la **Interfaz de red 0** en la sección **Hardware y red**. Se puede acceder a los registros de scripts en la sección **Paquetes de script**. Puede conectarse a cualquier consola disponible utilizando los enlaces de la sección **Consolas**.

Acceso a instancias desplegadas

Después de desplegar un patrón de sistema virtual, puede ver la instancia de sistema virtual que se ha creado para ver su entorno del Patrón IBM SOA Policy Gateway, y acceder a sus componentes.

Antes de empezar

Para ver una instancia de sistema virtual, primero debe desplegar un patrón de sistema virtual.

Acerca de esta tarea

Cuando se despliega un patrón se crea una instancia de sistema virtual o un entorno de tiempo de ejecución del Patrón IBM SOA Policy Gateway recién suministrado. Cuando el despliegue se completa, se ejecuta la instancia de sistema virtual.

Procedimiento

Para administrar las instancias de sistema virtual del Patrón IBM SOA Policy Gateway, realice los siguientes pasos:

1. Pulse **Instancias** > **Sistemas virtuales** para acceder a la ventana Instancias de sistema virtual.

2. En la lista de instancias de la ventana Instancias de sistema virtual, seleccione la instancia que se ha desplegado.
3. Si la instancia se está ejecutando, puede iniciar la sesión en los componentes del sistema virtual desde los enlaces de la consola en la vista del sistema virtual. Los componentes que están disponibles dependen del patrón que haya creado. Pueden incluir:
   - Consola administrativa de WebSphere Application Server
   - Interfaz de usuario web de WSRR
   - WSRR Business Space
   - Interfaz gráfica de usuario web de DataPower

Conexión a WSRR - Business Space

Utilice la interfaz de usuario de Business Space para trabajar con WSRR.

Acerca de esta tarea

Business Space es una de las dos interfaces gráficas que puede utilizar para trabajar con WSRR. Encontrará una descripción completa sobre el uso de Business Space con WSRR en el Information Center de WSRR (vea el enlace relacionado).

Puede conectarse a una instancia WSRR de Business Space en el patrón desplegado pulsando un enlace en la consola de carga de trabajo, o bien especificando el URL en el navegador web.

Procedimiento

1. Para conectarse desde la consola de carga de trabajo:
   a. Pulse **Instancias** > **Sistemas virtuales** para acceder a la ventana Instancias de sistema virtual.
   b. En la lista de instancias de la ventana Instancias del sistema virtual, seleccione el patrón desplegado.
   c. Pulse **Máquinas virtuales** en la vista detalles del sistema desplegado para expandir la lista.
   d. Localice WSRR en la lista de máquinas virtuales y pulse el signo más para ver los detalles.
   e. En la sección **Consolas**, pulse **WSRR_Business_Space**.
   f. Especifique el ID y contraseña de usuario administrativo de WSRR.
2. Para conectarse desde un navegador web:
   a. Abra un navegador web.
   b. Busque el nombre de host y los números de puertos para WSRR. Consulte los detalles del despliegue como se describe en el paso 1. Expanda la sección **Máquinas virtuales** y seleccione la máquina virtual para el servidor WSRR para ver los detalles de la máquina virtual. En la sección **Hardware y red**, el nombre de host es el valor **Interfaz de red 0**.
   c. Especifique el URL de la interfaz de usuario web de WSRR: http://*hostname*:9443/BusinessSpace, donde *hostname* es el nombre de host del servidor WSRR.
   d. Especifique el ID y contraseña de usuario administrativo de WSRR.

Resultados

Se abrirá Business Space, que se puede utilizar para añadir, editar o eliminar políticas de mediación, y otros artefactos WSRR.

Qué hacer a continuación

Si está utilizando Business Space en el sistema WSRR por primera vez, consulte "Configuración de Business Space para utilizarlo por primera vez" y siga los pasos para crear el espacio de gobierno de SOA.

Información relacionada:

Information Center de IBM WebSphere Service Registry and Repository, Versión 8.0

Configuración de Business Space para utilizarlo por primera vez

Antes de que se pueda utilizar la interfaz de usuario de Business Space para crear políticas, se debe crear el espacio de gobierno de SOA.

Antes de empezar

Para obtener más información acerca de cómo acceder a Business Space, consulte "Conexión a WSRR - Business Space" en la página 82.

Acerca de esta tarea

Para utilizar los widgets de Business Space, debe crear un espacio. Los espacios se definen para roles específicos. La creación de políticas es más adecuada para trabajar en el espacio de gobierno SOA. Si todavía no existe un espacio de gobierno de SOA, debe crearlo. Para crear un espacio basado en la plantilla Registro de servicio para gobierno SOA, realice los pasos siguientes:

Procedimiento

1. Pulse **Gestionar espacios** en la parte superior de la página. Aparecerá el diálogo de Space Manager.
2. Pulse **Crear espacio**. Aparecerá el diálogo Crear espacio.
3. Escriba un nombre en el campo **Nombre de espacio**; por ejemplo, `Gobierno SOA`. Opcionalmente, escriba una descripción.
4. Seleccione **Registro de servicio para gobierno SOA** en la lista **Crear un nuevo espacio utilizando una plantilla** y pulse **Guardar**.
5. Aparece el nuevo espacio en la lista de **Space manager**. Pulse el nuevo espacio para abrirlo.

Resultados

Se ha creado el espacio de gobierno de SOA. Para abrir el espacio de gobierno de SOA:

1. Pulse **Ir a espacios** en la parte superior de la página. Aparece el diálogo Ir a espacios.
2. Pulse el espacio correspondiente a los usuarios del gobierno SOA. El nombre específico depende de lo que se haya especificado al crear el espacio.

Qué hacer a continuación

Puede añadir más acciones al widget Acciones del registro de servicio:

1. En Business Space, pulse **Editar página**.
2. En el widget Acciones del registro de servicio, pulse **Editar valores**.
3. Seleccione las acciones siguientes para visualizar:
   - Crear una definición de nivel de servicio
   - Crear una versión de servicio
   - Crear un acuerdo de nivel de servicio
   - Crear una capacidad de negocio
4. En el widget Acciones del registro de servicio, pulse **Guardar y cerrar**.
5. Pulse **Finalizar edición**.

Conexión a WSRR - Interfaz de usuario web WSRR

Utilice la interfaz de usuario web de WSRR para trabajar con WSRR.

Acerca de esta tarea

La interfaz de usuario web de WSRR es una de las dos interfaces gráficas que puede utilizar para trabajar con WSRR. Encontrará una descripción completa sobre el uso de la interfaz de usuario web de WSRR en el Information Center de WSRR (vea el enlace relacionado). En la mayoría de los casos es posible que prefiera utilizar la interfaz de Business Space, pero hay algunas tareas (como por ejemplo la creación de las políticas de supervisión) que deben completarse en la interfaz de usuario web de WSRR.

Puede conectarse a la interfaz de usuario web de WSRR de una instancia WSRR en el patrón desplegado pulsando un enlace en la consola de carga de trabajo, o bien especificando el URL en el navegador web.

Procedimiento

1. Para conectarse desde la consola de carga de trabajo:
   a. Pulse **Instancias** > **Sistemas virtuales** para acceder a la ventana Instancias de sistema virtual.
   b. En la lista de instancias de la ventana Instancias del sistema virtual, seleccione el patrón desplegado.
   c. Pulse **Máquinas virtuales** en la vista detalles del sistema desplegado para expandir la lista.
   d. Localice WSRR en la lista de máquinas virtuales y pulse el signo más para ver los detalles.
   e. En la sección **Consolas**, pulse **WSRR_Web_UI**.
   f. Especifique el ID y contraseña de usuario administrativo de WSRR.
2. Para conectarse desde un navegador web:
   a. Abra un navegador web.
   b. Busque el nombre de host y los números de puertos para WSRR. Consulte los detalles del despliegue como se describe en el paso 1. Expanda la sección **Máquinas virtuales** y seleccione la máquina virtual para el servidor WSRR para ver los detalles de la máquina virtual. En la sección **Hardware y red**, el nombre de host es el valor **Interfaz de red 0**.

c. Especifique el URL de la interfaz de usuario web de WSRR: http://*hostname*:9443/ServiceRegistry, donde *hostname* es el nombre de host del servidor WSRR.

d. Especifique el ID y contraseña de usuario administrativo de WSRR.

Información relacionada:

Information Center de IBM WebSphere Service Registry and Repository, Versión 8.0

Conexión de la consola administrativa de WebSphere Application Server

Utilice la consola administrativa de WebSphere Application Server para ajustar los valores de seguridad y completar otras tareas administrativas.

Acerca de esta tarea

Los detalles completos sobre cómo trabajar con la consola administrativa de WebSphere Application Server se encuentran en el Information Center. Siga el enlace relacionado.

Puede conectarse a la consola administrativa de WebSphere Application Server en el patrón desplegado pulsando un enlace en la consola de carga de trabajo, o bien especificando el URL en el navegador web.

Procedimiento

1. Para conectarse desde la consola de carga de trabajo:
   a. Pulse **Instancias** > **Sistemas virtuales** para acceder a la ventana Instancias de sistema virtual.
   b. En la lista de instancias de la ventana Instancias del sistema virtual, seleccione el patrón desplegado.
   c. Pulse **Máquinas virtuales** en la vista detalles del sistema desplegado para expandir la lista.
   d. Localice WSRR en la lista de máquinas virtuales y pulse el signo más para ver los detalles.
   e. En la sección **Consolas**, pulse **WebSphere**.
   f. Especifique el ID y contraseña de usuario administrativo de WSRR.
2. Para conectarse desde un navegador web:
   a. Abra un navegador web.
   b. Busque el nombre de host y los números de puertos para WSRR. Consulte los detalles del despliegue como se describe en el paso 1. Expanda la sección **Máquinas virtuales** y seleccione la máquina virtual para el servidor WSRR para ver los detalles de la máquina virtual. En la sección **Hardware y red**, el nombre de host es el valor **Interfaz de red 0**.
   c. Especifique el URL de la interfaz de usuario web de WSRR: http://*hostname*:9043/ibm/console, donde *hostname* es el nombre de host del servidor WSRR.
   d. Especifique el ID y contraseña de usuario administrativo de WSRR.

Información relacionada:

Information Center de WebSphere Application Server V8.0

Conexión a la consola de un DataPower virtual

Utilice la consola DataPower para configurar el punto de aplicación de políticas.

Acerca de esta tarea

Los detalles completos de la configuración de la pasarela se encuentran en el Information Center de WebSphere DataPower. Siga el enlace relacionado.

Para conectarse a la consola utilizando un navegador web. Puede recuperar los detalles de conexión visualizando los detalles de su patrón desplegado en la consola de carga de trabajo.

Procedimiento

1. Recupere los detalles que necesite mediante la consola de carga de trabajo:
   a. Pulse **Instancias** > **Sistemas virtuales** para acceder a la ventana Instancias de sistema virtual.
   b. En la lista de instancias de la ventana Instancias del sistema virtual, seleccione el patrón desplegado.
   c. En la vista de detalles, expanda la sección **Máquinas virtuales** y seleccione la máquina virtual para el dispositivo DataPower para ver los detalles de la máquina virtual. En la sección **Hardware y red**, el nombre de host es el valor **Interfaz de red 0**.
2. Abra un navegador web y especifique el URL `https://`*`hostname`*`:9090/dp`, donde *hostname* es el nombre de host de su dispositivo virtual.

Información relacionada:

Information Center de WebSphere DataPower V6.0

Conexión a la consola de supervisión

Utilice la consola de supervisión para ver información de supervisión.

Acerca de esta tarea

Acceda a la consola de supervisión desde la ventana Instancias de sistema virtual.

ITCAM for SOA proporciona la funcionalidad de supervisión. Descargue la documentación del enlace relacionado para obtener más información, y busque información sobre las instalaciones DataPower.

Procedimiento

1. Pulse **Instancias** > **Sistemas virtuales** para acceder a la ventana Instancias de sistema virtual.
2. En la lista de instancias de la ventana Instancias de sistema virtual, seleccione la instancia que se ha desplegado. Se muestran los detalles de la instancia.
3. Expanda la sección **Máquinas virtuales** y seleccione la máquina virtual que desea supervisar.
4. En **Información general**, localice **Supervisión** y pulse el enlace **Pulsar para abrir**.

Información relacionada:

Documentación de ITCAM for SOA 7.2.1 (desde Fix Central)

Como detener e iniciar la instancia desplegada

Puede detener e iniciar la instancia desplegada desde una consola de carga de trabajo. También puede detener e iniciar las máquinas virtuales individuales en el patrón.

Para detener la ejecución de un instancia desplegada:

1. Seleccione **Instancias** > **Sistemas virtuales** y seleccione la instancia de la lista **Instancias de sistemas virtuales**.
2. Pulse el icono **Detener** en la barra de título de la instancia.

Para iniciar una instancia desplegada detenida:

1. Seleccione **Instancias** > **Sistemas virtuales** y seleccione la instancia de la lista **Instancias de sistemas virtuales**.
2. Pulse el icono **Iniciar** en la barra de título de la instancia.

Nota: Un defecto conocido en DB2 10.1.0.2 provoca que los procesos DB2 no siempre se reinicien cuando la instancia se detiene y reinicia. En este caso, debe iniciar el proceso DB2 manualmente, iniciando sesión en el nodo DB2 como db2inst1 y ejecutando **db2start**. Asimismo, es posible que tenga que reiniciar los procesos WSRR en los nodos WSRR.

Para detener las máquinas virtuales individuales.

1. Expanda la sección **Máquinas virtuales** de la vista de instancia.
2. Seleccione el enlace **Gestionar** para la máquina que desea detener.
3. Pule el icono Detener en la barra de gestión.

Para iniciar las máquinas virtuales individuales.

1. Expanda la sección **Máquinas virtuales** de la vista de instancia.
2. Seleccione el enlace **Gestionar** para la máquina que desea detener.
3. Pule el icono Iniciar en la barra de gestión.

También puede detener e iniciar WSRR y DB2 de la línea de mandatos. Pulse el enlace **Iniciar sesión** para conectar utilizando la consola SSH.

Detenga e inicie WSRR deteniendo e iniciando el perfil de WebSphere Application Server. Consulte Gestión de perfiles mediante mandatos en el Information Center de WebSphere Application Server.

En el patrón avanzado, después de que se reinicien los nodos personalizados y DMGR, es necesario iniciar el clúster WSRR. Para ello, abra la consola administrativa de WebSphere Application Server y seleccione **Servidores** > **Clústeres** > **Clústeres de WebSphere Application Server**. Seleccione **WSRRCluster_1** y, a continuación, pulse **Iniciar**.

Puede detener e iniciar DB2 mediante los mandatos del sistema. Consulte Mandatos del sistema en el Information Center de DB2.

Configuración de patrones después del despliegue

Después de desplegar los patrones, debe configurar la seguridad y otros valores.

Configuración del punto de aplicación de políticas

El dispositivo o instancia de DataPower es el punto de aplicación de políticas del Patrón IBM SOA Policy Gateway. Una vez desplegado el dominio de aplicación, se puede crear el contenido de dicho dominio.

Procedimiento

Al definir las configuraciones, asegúrese de que se utilizan distintos nombres de dominio en cada dispositivo DataPower, de lo contrario los espacios de trabajo de topología ITCAM for SOA no muestran los datos correctos.
Cree un proxy de servicio web (WSP):

1. En el panel de control de DataPower, pulse **Proxy de servicio web**.
2. Pulse **Añadir** y escriba un nombre para el proxy.
3. Abra el separador **Suscripción WSRR**. En la lista Servidor WSRR, pulse **WSRRSVR**.
4. Proporcione la información restante necesaria, tal como el manejador del extremo frontal, el espacio de nombres, el nombre de objeto, etc., para crear la configuración del proxy de servicio web.

Cree las políticas para el WSP:

5. Abra el separador **Política** para el editor de WSP.
6. Pulse **Reglas de proceso** en el nivel adecuado. Puede crear una nueva regla o editar la regla predeterminada que se proporciona. La acción de política clave que se ha de añadir es la **Acción AAA**. Esta maneja la identificación, la autenticación y autorización que son claves para el patrón.

   Los elementos clave que debe especificar para la acción AAA incluyen la entrada y salida, así como la política AAA. Puede crear la política mientras crea una acción de política AAA, o bien puede crearla antes utilizando el editor de AAA.

   - La identificación es el paso en el que se identifica al usuario. En el ejemplo, se utilizan dos formas de identificación. En el cortafuegos StoreAddLTPA XML, la identificación ha se ha realizado con la autenticación básica. En el cortafuegos StoreWSP, la identificación la proporciona la señal LTPA.
   - La autenticación es el paso en que se demuestra que el sistema conoce al usuario. Existen muchas opciones para elegir. En este ejemplo, se han mostrado dos ejemplos. En el primero se ha buscado al usuario con LDAP y en el segundo se ha aceptado una señal LTPA válida.
   - La autorización es el paso en que el usuario tiene autorización para el recurso, que en este caso son las operaciones de servicio web. Se deben especificar los siguientes elementos clave para utilizar la autorización del PDP de XACML incluido:
     - El método: **Utilizar la autorización XACML**.
     - La versión de XACML, por ejemplo, 2.0.
     - El tipo de PDP, por ejemplo, denegación basada en PDP.
     - El PDP incluido: **Activado**
     - El nombre del PDP, que tiene el XACML especificado.
     - Configure el PDP. Para obtener más información, consulte “Alteración del PDP XACML en DataPower” en la página 71.
     - La hoja de estilo XSL personalizada para enlazar AAA y XACML: utilice `apil-xacml-bindingnew.xsl` como un punto de partida.

Para configurar la pasarela de modo que utilice la redacción:

7. Modifique el archivo `.xml` de XACML de modo que coincida con las políticas de seguridad concretas que desea aplicar a la redacción.
8. Cree un cortafuegos XML con una acción AAA que siga el ejemplo de redacción.
9. Modifique el PDP que utiliza la acción AAA anterior para que indique la hoja de estilo que está utilizando para aplicar la redacción.
10. Copie y modifique la hoja de estilo `storeCallPDP.xsl`, que crea la carga útil de SOAP para el servicio de XACML. En especial, asegúrese de que la acción y los recursos coincidan con los requisitos para el documento de políticas XACML que ha creado.
11. Asegúrese de que la hoja de estilo modificada llama al puerto correcto para su nuevo cortafuegos XML de XACML.

Objetos DataPower creados en los patrones tiempo de ejecución básico y tiempo de ejecución avanzado.

Una visión general de los objetos DataPower que se han creado en los patrones de tiempo de ejecución básico y tiempo de ejecución avanzado y su función.

Tabla 18. Objetos del patrón DataPower

Objeto	Descripción
Dominio	Un dominio que puede utilizarse para la aplicación de los usuarios.
Servidor WSRR	WSRRSVR con nombre. El URL de SOAP, el nombre de usuario y la contraseña están configurados, así como un perfil de proxy SSL con credenciales de validación.
Perfil de proxy SSL	El WSRRPP con nombre es un perfil de envío (cliente). Utiliza el WSRRCP del perfil de cifrado. Se utilizan todos los demás valores predeterminados.
Perfil criptográfico	El WSRRCP contiene un WSRRVC de objeto de credenciales de validación, que contiene el certificado de firmante que se ha cargado como parte de los scripts del patrón.
Credenciales de validación	Las credenciales de validación WSRR contienen el WSRRCERT del certificado criptográfico. Todos los demás valores son valores predeterminados.
Certificado criptográfico	WSRRCERT utiliza el certificado de firmante. Este certificado se ha extraído de NodeDefaultKeyStore, o es el certificado de un único servidor o es el certificado predeterminado de CMSKeyStore en el caso de un entorno ND en el que existía un IBM HTTP Server.

Ejemplo de uso de la definición de servidor WSRR en un Proxy de servicio web:

1. En el panel de control de DataPower, pulse **Proxy de servicio web**.
2. Pulse **Añadir** y proporcione un **Nombre** para el proxy.
3. A continuación, seleccione el separador **Subscripción WSRR**.
4. Seleccione el servidor WSRR en el menú. El objeto WSRRSVR está disponible.
5. Proporcione la información restante necesaria, tal como el manejador del extremo frontal, el espacio de nombres, el nombre de objeto, etc., para crear la configuración del proxy de servicio web.

Valores de DN de certificado para certificados de DataPower

Cuando SSL se utiliza con el Patrón IBM SOA Policy Gateway proporcionado, la verificación de host de DN es más estricta que la seguridad predeterminada de WebSphere Application Server. (Este tema se aplica a dispositivos DataPower externos).

La verificación de host de DN no está habilitada en WebSphere Application Server de forma predeterminada. Pero en los paquetes script que utiliza el Patrón IBM SOA Policy Gateway, la verificación de host de DN está habilitada y no se puede inhabilitar. Un certificado específico que funciona entre el WebSphere Application Server predeterminado y DataPower podría no funcionar para el paquete script "SOA Policy Gateway 2.5.0.0 - Seguridad" o el paquete script "SOA Policy Gateway 2.5.0.0 - Ejemplo" que se utiliza con el Patrón IBM SOA Policy Gateway. Por ejemplo, un nombre distinguido de `myserver.yourcompany.com` podría ser aceptado por los valores predeterminados de WebSphere Application Server, pero no por los paquetes script. Para añadir o eliminar los certificados de DataPower que se utilizan con el despliegue, consulte "Añadir o eliminar certificados DataPower para el almacén de WSRR".

Añadir o eliminar certificados DataPower para el almacén de WSRR

Esta tarea describe cómo añadir o eliminar certificados de DataPower. Este tema se aplica a patrones desplegados con dispositivos DataPower externos.

Acerca de esta tarea

Los certificados DataPower se suben al almacén de confianza WSRR para simplificar la actualización de sincronización entre WSRR y DataPower para actualizaciones de políticas. Si esta capacidad no es necesaria, puede eliminar los certificados DataPower. También puede añadir nuevos certificados DataPower, si se deben cambiar los certificados.

Procedimiento

1. Para eliminar certificados:
   a. Inicie sesión en la consola administrativa de WebSphere Application Server en `https://`*`hostname`*`:9043/ibm/console`, donde *hostname* es el nombre de host del sistema WSRR. Escriba el nombre y contraseña del usuario administrativo.
   b. Vaya a **Seguridad, certificados SSL y gestión de claves**.
   c. Pulse **Almacenes de claves y certificados**.
   d. Pulse **NodeDefaultTrustStore** si el despliegue se basa en un patrón de tiempo de ejecución básico, o **CellDefaultTruststore** si ha desplegado un patrón de tiempo de ejecución avanzado.
   e. Pulse **Certificados de firmante**.
   f. Seleccione los recuadros de selección de cualquier certificado que desee eliminar.
   g. Pulse **Suprimir**.
   h. Pulse **Guardar**.
2. Para añadir nuevos certificados de DataPower, pulse **Añadir** para añadir el nuevo certificado.

a. Inicie sesión en la consola administrativa de WebSphere Application Server en `https://hostname:9043/ibm/console`, donde *hostname* es el nombre de host del sistema WSRR. Escriba el nombre y contraseña del usuario administrativo.
b. Vaya a **Seguridad, certificados SSL y gestión de claves**.
c. Pulse **Almacenes de claves y certificados**.
d. Pulse **NodeDefaultTrustStore** si el despliegue se basa en un patrón de tiempo de ejecución básico, o **CellDefaultTruststore** si ha desplegado un patrón de tiempo de ejecución avanzado.
e. Pulse **Certificados de firmante**.
f. Pulse **Añadir** y especifique los nuevos certificados.
g. Pulse **Guardar**.

Modificación de las claves LTPA

Este procedimiento describe cómo cambiar la clave LTPA. La clave LTPA se comparte entre todas las celdas en los patrones. No se utiliza en el patrón SOA Policy Gateway Basic Runtime Sample. La clave LTPA se exporta desde el maestro de gobierno y se importa a entornos de ejecución, tales como los de transición o producción.

Acerca de esta tarea

Puede completar estas acciones en la consola administrativa de WebSphere Application Server. Para obtener más información, siga el enlace relacionado.

Procedimiento

1. Exporte la nueva clave LTPA desde el gestor de despliegue WSRR del maestro de gobierno.
2. Importe la clave LTPA en las instancias de WSRR de WSRR, que son Dmgr (gestor de despliegue) o Autónoma.
3. Si la instancia de ejecución se basa en un patrón de tiempo de ejecución avanzado, complete los pasos siguientes en orden:
   a. Sincronice todos los nodos.
   b. Detenga el clúster WSRR.
   c. Detenga los agentes de nodo.
   d. Detenga el Dmgr.
4. Si el sistema WSRR se basa en un patrón de tiempo de ejecución avanzado, debe reiniciarse en orden inverso:
   a. Inicie el gestor de despliegue.
   b. Inicie los agentes de nodo.
   c. Inicie el clúster WSRR.
5. Si el WSRR es un servidor autónomo (basado en un patrón de tiempo de ejecución básico), se debe detener y reiniciar para que el cambio de la clave LTPA entre en vigor.

Información relacionada:

Information Center de WebSphere Application Server V8.0

Creación y gobierno de servicios

Utilice la interfaz de usuario Business Space de WSRR para crear y gobernar servicios de negocio y sus objetos asociados.

Se debe crear el espacio de gobierno SOA en Business Space para poder crear políticas. Si no existe el espacio de gobierno SOA, consulte “Configuración de Business Space para utilizarlo por primera vez” en la página 83 y siga los pasos para crear el espacio.

Para obtener más información sobre la creación de un nuevo servicio gobernado, consulte Information Center de IBM WebSphere Service Registry and Repository, Versión 8.0 - Guía de aprendizaje: Gobierno de un nuevo servicio.

Para obtener más información sobre el gobierno de un servicio existente, consulte Information Center de IBM WebSphere Service Registry and Repository, Versión 8.0 - Guía de aprendizaje: Gobierno de un servicio existente.

Tareas relacionadas:

“Conexión a WSRR - Business Space” en la página 82
Utilice la interfaz de usuario de Business Space para trabajar con WSRR.

Políticas

Detalles de implementación para utilizar WSRR como el punto de creación de políticas y WebSphere DataPower como punto de aplicación de políticas al crear políticas de mediación.

Políticas en WSRR

Puede utilizar WSRR para crear todas las políticas SOA, incluidas las políticas SLA (Acuerdo de nivel de servicio), las políticas de mediación, las políticas de supervisión y las políticas personalizadas. Mediante la interfaz de usuario de Business Space, puede crear, actualizar o suprimir un documento de políticas en WSRR. El documento de políticas puede contener una expresión de política que especifique un número de políticas para un dominio de política determinado. De forma alternativa, puede crear un documento de políticas que ensambla políticas existentes de otros documentos. Se hace referencia a las políticas individuales mediante los identificadores de política, los cuales se especifican cuando se añaden políticas al documento. Una expresión de política representa la declaración de una política y es equivalente a un elemento `<wsp:Policy>` de un documento WS-Policy.

Para crear una política de mediación en Business Space, consulte “Creación de nuevas políticas de mediación” en la página 98.

Aserciones de políticas de mediación

Los Acuerdos de nivel de servicio (SLA) se originan a partir de un requisito empresarial de que la calidad de servicio que proporciona un servicio cumpla un estándar determinado. A medida que se diseña un servicio, se crean requisitos funcionales que guían la lógica de lo que lleva a cabo el servicio. De forma paralela se especifican requisitos no funcionales como parte del análisis y diseño del servicio para identificar la calidad que se espera del servicio. Por ejemplo, la empresa puede tener un servicio que proporciona información en respuesta a una consulta del cliente realizada en Internet. El objetivo es devolver la respuesta en el plazo de 3 segundos. Como parte del diseño de la transacción entre puntos finales,

se determina que el servicio debe devolver la información en el plazo de 2 segundos para cumplir los requisitos no funcionales de la empresa.

Puede escribir una política que implemente comprobaciones de tiempo de ejecución en el rendimiento del servicio y actúe cuando se cumplan los requisitos para garantizar que el servicio cumple su SLA. Por ejemplo, puede tener un punto final de servicio primario que normalmente (un 95% del tiempo) puede proporcionar una respuesta de servicio en 2 segundos. El arquitecto SOA crea un punto final secundario en otro servidor que puede utilizarse como repuesto cuando se interrumpe el punto final principal, pero que también puede ser utilizado para el tráfico excesivo cuando el punto final principal no puede hacer frente a la carga de transacciones. Puede escribir una política que controla el tiempo de respuesta del servicio y redirecciona el tráfico cuando sea necesario para cumplir el acuerdo de nivel de servicio.

Otro ejemplo en el que se mantiene el acuerdo de nivel de servicio mediante una política de tiempo de ejecución es cuando un servicio responde a transacciones donde intervienen diversos consumidores, cada uno con un nivel de prioridad diferente. Un ejemplo sencillo es la situación donde existen clientes "Gold" y "Bronze" y sólo se asegura una calidad de servicio determinada para los clientes "Gold". En este ejemplo, puede comprobar si el consumidor es "Gold" y redireccionarlo hacia el punto final secundario, mientras que el cliente "Bronze" recibe un tiempo de respuesta más lento. La empresa lo ha decidido porque los clientes “Bronze” no proporcionan un aumento de beneficios suficiente para justificar los gastos de implementar un tiempo de respuesta que cumpla el acuerdo de nivel de servicio de los clientes “Gold”.

En un tercer ejemplo, puede tener una situación en la que un servicio hace todo cuanto sea posible, pero cuando determine que está sometido a una carga de trabajo, pone en cola o incluso rechaza los mensajes procedentes de servicios de consumidor de prioridad baja. Un ejemplo es cuando una rutina de proceso por lotes inunda el sistema con solicitudes de consumidores en un momento inesperado. Para proteger la calidad de servicio, puede crear una política de tiempo de ejecución que entre en vigor sólo durante el horario de trabajo y rechace todas las solicitudes de proceso por lotes durante este período.

De forma más genérica, la política de mediación permite la validación y transformación del mensaje entrante del cliente (consumidor) antes de presentarlo al servidor (proveedor).

Las políticas dan soporte a este tipo de validación y transformación del mensaje. Se pueden especificar políticas para un servicio de proveedor, para un par consumidor-proveedor específico o para los consumidores anónimos de un servicio de proveedor. Las políticas para consumidores anónimos proporcionan una manera de definir una política predeterminada que sólo se aplica a los consumidores para los que no se aplican otras políticas. Esto permite especificar una política para los consumidores no autorizados que no se identifican. Para esos servicios de consumidor se pueden luego rechazar sus transacciones. Esto puede ser útil para impedir ataques de denegación de servicio de piratas informáticos que intentan inundar el sistema con transacciones para colapsar un servicio de proveedor.

Condiciones de las políticas de mediación

Se pueden realizar aserciones de mediación que permiten que la política de ejecución controle el Acuerdo de nivel de servicio, transforme los mensajes del consumidor al proveedor o valide el esquema del mensaje del consumidor.

Las condiciones de la política de SLA son un tipo especial de política de mediación que permiten utilizar una estructura if-then-else con una condición y luego efectuar un conjunto de acciones dependiendo del resultado de evaluar la condición. Especificar una condición es opcional. Si no se especifica ninguna condición, equivale a que la condición lógica se evalúe en True, y cualquier acción especificada se ejecutará de acuerdo con esto.

Si se especifica la condición, debe ser una expresión booleana o una especificación de planificación, o incluir ambas cosas.

Planificación

Si se especifica una planificación, ésta identifica cuándo entra en vigor la política. El punto de aplicación de políticas local evalúa la fecha y hora y la zona horaria utilizada es la del punto de aplicación de políticas. Si no se especifica ninguna planificación, la política se inicia en cuanto se descarga desde el punto de creación de políticas al punto de aplicación de políticas, y prosigue de forma indefinida.

La planificación define una fecha de inicio opcional y una fecha de detención opcional, un intervalo de tiempo diario opcional y una lista de días de la semana opcionales. Por ejemplo, se puede definir una planificación para que sea efectiva desde el 1 de octubre de 2012 al 30 de octubre de 2012, desde las 8 am hasta las 5 pm en los miércoles y domingos.

Los parámetros de la planificación se pueden especificar de este manera:

- **StartDate**: este atributo opcional especifica la fecha en la que la planificación es efectiva, con el formato xs:date. StarDate es inclusivo y si este atributo no está presente, la planificación será efectiva de forma inmediata en el día actual. (Pulse el hiperenlace xs:time para conocer este estándar del sector).
- **StopDate** - este atributo opcional especifica la fecha en la que la planificación deja de ser efectiva, con el formato xs:date. StopDate es exclusivo y la fecha especificada debe ser posterior a la fecha de inicio. Cuando la fecha de detención es anterior o igual a la fecha de inicio, la planificación nunca se hace efectiva. Si este atributo no está presente, la planificación es efectiva de forma indefinida.
- **Daily**: este elemento opcional especifica el intervalo de tiempo diario durante el cual la planificación es efectiva. Si este elemento no está presente, la planificación es efectiva todo el día.
  - **StartTime**: si se especifica Daily, entonces este atributo es necesario. Especifica la hora en que la planificación comienza cada día con el formato xs:time. (Pulse el hiperenlace xs:time para conocer este estándar del sector).
  - **StopTime**: si se especifica Daily, entonces este atributo es necesario. Especifica la hora en que la planificación se detiene cada día con el formato xs:time. StopTime es exclusiva y si la hora especificada es anterior o la misma que la hora de inicio diaria de la planificación se detiene en la hora de detención especificada del día siguiente.
- **Weekdays**: este elemento opcional especifica los días de la semana incluidos en la planificación. Si este elemento no está presente, se incluyen todos los días de la semana en la planificación. Este elemento solo afecta al inicio del intervalo de tiempo diario, ya que las planificaciones pueden ejecutarse pasada la medianoche. Por ejemplo, si una planificación está definida para iniciarse a las 11 pm y se ejecuta durante 2 horas los miércoles, la planificación finaliza el jueves a la 1 am.
  - **Days**: si se especifica Weekdays, entonces este atributo es necesario. Lista los días de la semana incluidos en la planificación, separados por el signo más

('+'), tal como
“Monday+Tuesday+Wednesday+Thursday+Friday+Saturday+Sunday”.

Expresión de la condición de la política de mediación

La expresión de la condición, si se especifica, es un elemento no repetitivo que especifica una expresión booleana.

La expresión consta de tres parámetros: Atributo, Operador y Valor, además de los parámetros opcionales Intervalo y Límite. Cuando se aplica el Operador sobre el Atributo y el Valor, más el Intervalo y el Límite cuando sean pertinentes, si el resultado de la evaluación es True, entonces el resultado de evaluar la expresión es True. El elemento Límite sólo se utiliza con los operadores HighLow y TokenBucket. Si no se especifica el Límite, su valor es 0. Si no se especifica el Intervalo, el valor predeterminado es 60 segundos.

Los parámetros de la Expresión se pueden especificar de este modo:

- **Atributo**: la tabla siguiente resume los atributos definidos y su tipo.

Tabla 19. Atributos definidos

Atributo	**Descripción y tipo**
ErrorCount	Número de errores observados durante el intervalo de supervisión.
MessageCount	Número de mensajes reales interceptados durante el intervalo de supervisión.
InternalLatency	Latencia interna (tiempo de proceso) en segundos.
BackendLatency	Latencia de dispositivo-a-servidor en segundos.
TotalLatency	Suma de la latencia de dispositivo a servidor y la latencia interna en segundos.

- **Operador**: la tabla siguiente resume los operadores disponibles y su significado.

Tabla 20. Operadores

Operador	**Significado**
GreaterThan	Algoritmo numérico simple que se evalúa como true cuando el atributo es mayor que el valor definido.
LessThan	Algoritmo numérico simple que se evalúa como true cuando el atributo es menor que el valor definido.

Tabla 20. Operadores (continuación)

Operador	Significado
TokenBucket	Algoritmo basado en el ritmo de transmisión que permite la transmisión por ráfagas. El algoritmo consta de un grupo con una capacidad máxima de señales de límite. El grupo se vuelve a llenar a una velocidad constante de señales de valor por intervalo, mientras que para cada unidad de atributo se elimina una señal. Este algoritmo se evalúa como True cuando no hay señales en el grupo y se evalúa como False cuando las hay. A continuación se muestra un ejemplo que ayuda a describir el algoritmo: presuponga que Limit=100, Value=5, Interval=1 segundo y Attribute=MessageCount. 1. Inicialmente el grupo está lleno con una capacidad máxima de 100 señales 2. Cuando llega un mensaje, el algoritmo comprueba si el grupo contiene las señales: a. Si es así, el algoritmo se evalúa como False y se elimina una señal del grupo b. Si no es así, el algoritmo se evalúa como True. 3. Mientras tanto, cada segundo, el algoritmo vuelve a añadir 5 señales al grupo, si el espacio lo permite.
HighLow	Algoritmo que se evalúa como True cuando el atributo alcanza el umbral alto especificado como valor, y continúa evaluándose como True hasta que el atributo alcanza el umbral bajo especificado como el límite.

- **Valor**: este es un elemento entero positivo. "0" es válido.
- **Intervalo**: este elemento opcional define el intervalo de tiempo, utilizado como intervalo móvil, para medir wsme:Attribute cuando se evalúa la expresión, con el formato xs:duration. Si no se especifica, el intervalo utilizado es 60 segundos. Si se especifica, se debe especificar un valor razonable, teniendo en cuenta las funciones configuradas del punto de aplicación de políticas. Esto es, cuanto mayor sea este valor, más memoria necesitará el punto de aplicación de políticas para hacer un seguimiento del atributo. (Pulse el hiperenlace xs:duration para conocer este estándar del sector).
- **Límite**: este elemento entero opcional define el argumento adicional Límite que es necesario cuando wsme:Operator es TokenBucket o HighLow. La unidad depende del wsme:Operator especificado.

  Cuando wsme:Operator es HighLow, define el umbral bajo, mientras que wsme:Value define el umbral alto. El umbral especificado debe ser menor que el umbral de wsme:Value. Cuando no se especifica el límite predeterminado es 0.

  Cuando wsme:Operator es TokenBucket define el tamaño máximo de desbordamiento, o el número máximo de señales del grupo, mientras que el valor especifica la velocidad con que se rellena el grupo, en número de señales por intervalo. Cuando no se especifica el límite predeterminado es 0 y TokenBucket será entonces equivalente a una operación GreaterThan.

Acciones de la política de mediación

El elemento Acción de mediación especifica las acciones que se deben realizar. Aunque la sintaxis permite muchas combinaciones, no todas ellas tienen sentido, y cuando se especifican acciones conflictivas, tal como solicitar que un mensaje se

ponga en la cola y se rechace, el comportamiento es rechazado por el punto de creación de políticas. Las acciones de la política de mediación son:

- **QueueMessage**: esta acción especifica que las transacciones se pondrán en cola cuando se cumpla la condición lógica. El proceso de mensajes no se vuelve a comenzar hasta que no se vuelva a cumplir la condición lógica. La metodología de puesta en cola y los tiempos de espera excedidos asociados son los definidos por el punto de aplicación de políticas, en este caso WebSphere DataPower. Cuando se especifican varias acciones dentro de un mismo elemento Acción, QueueMessage debe ser la primera acción.
- **RejectMessage**: esta acción especifica que las transacciones se rechazan cuando se cumpla la condición lógica. Las transacciones continuarán siendo rechazadas hasta que no se cumpla la condición lógica. Cuando se rechazan las transacciones, se devuelve un error SOAP al servicio de cliente (consumidor). Cuando se especifican varias acciones dentro de un mismo elemento Acción, RejectMessage debe ser la primera acción. QueueMessage y RejectMessage se excluyen mutuamente.
- **Notify**: este elemento opcional especifica que se cree una notificación cuando se cumpla la condición lógica. Para DataPower, se graba un mensaje en el registro del sistema DataPower.
- **RouteMessage**: este elemento opcional especifica que los mensajes se direccionen hacia al destino de punto final especificado cuando se cumpla la condición lógica. Los mensajes se siguen direccionando al punto final especificado hasta que no se cumpla la condición lógica.
  - **EndPoint**: este parámetro es necesario cuando se especifica una acción RouteMessage. El valor de punto final soportado puede ser una dirección IP, nombre de host o host virtual, tal como un grupo de equilibradores de carga.
- **ValidateMessage**: este elemento opcional especifica que los mensajes se validan utilizando las gramáticas especificadas. Los mensajes se rechazan cuando la validación falle. Se debe especificar XSD o WSDL como subparámetro si se especifica ValidateMessage. SCOPE es opcional, y si no se especifica, se utiliza SOAPBody para la validación.
  - **XSD**: especifica que los mensajes se validan con el esquema XML identificado por el URI que contiene.
  - **WSDL**: especifica que los mensajes se validan con la descripción de servicios web (WSDL) identificada por el URI que contiene.
  - **SCOPE**: especifica qué parte del mensaje se valida. En la tabla siguiente se muestran los valores posibles y su significado:

Tabla 21. Elementos de ValidateMessage

Valor	Descripción
SOAPBody	El contenido del elemento Body de SOAP, sin ningún proceso especial de errores de SOAP. (Valor predeterminado)
SOAPBodyOrDetails	El contenido del elemento de detalles para los errores de SOAP y, de lo contrario, el contenido de Body.
SOAPEnvelope	Todo el mensaje SOAP, incluido el sobre.
SOAPIgnoreFaults	No hay validación si el mensaje es un error de SOAP, de lo contrario, el contenido de Body de SOAP.

- **ExecuteXSL**: especifica que se realizará una transformación XSL con la hoja de estilo y parámetros especificados. Las transacciones se rechazarán cuando falle la

ejecución. Se debe especificar la información de la hoja de estilo, mientras que los parámetros son opcionales, y se deben especificar según sea necesario mediante la hoja de estilo especificada.

– **Stylesheet**: especifica que la operación de transformación utiliza la hoja de estilo especificada por el URI contenido. La hoja de estilo DEBE ser un archivo XSLT.
– **Parameter**: este elemento repetitivo opcional especifica un parámetro de hoja de estilo que se utilizará para la operación ExecuteXSL.
  - **Name**: este atributo es necesario para cada parámetro correspondiente y especifica el nombre del parámetro.
  - **Value**: este atributo es necesario para cada parámetro Name correspondiente y especifica el valor del parámetro.

Creación de nuevas políticas de mediación

Puede crear nuevas políticas de mediación utilizando la interfaz de usuario de Business Space. Cuando cree las políticas de mediación, especifique las condiciones y las acciones para la política.

Antes de empezar

Para obtener más información acerca de cómo acceder a Business Space, consulte “Conexión a WSRR - Business Space” en la página 82.

Se debe crear el espacio de gobierno SOA para poder crear políticas. Si no existe el espacio de gobierno SOA, consulte “Configuración de Business Space para utilizarlo por primera vez” en la página 83 y siga los pasos para crear el espacio.

También debe configurar Business Space para crear las políticas de mediación WS-MediationPolicy 1.7 desde el widget Acciones. Consulte, widget Acciones del registro de servicio

Acerca de esta tarea

Creación de nuevas políticas utilizando el espacio de gobierno SOA.

Procedimiento

1. Abra el espacio de gobierno SOA:
   a. Pulse **Ir a espacios**. Aparece el diálogo Ir a espacios.
   b. Pulse el espacio correspondiente a los usuarios del gobierno SOA. El nombre específico depende de lo que se haya especificado al crear el espacio.
2. En el separador Visión general, pulse **Crear una política de mediación**.
3. Escriba un nombre descriptivo y una descripción opcional.
4. Añada condiciones y acciones según sea necesario. Para obtener más información sobre condiciones y acciones, consulte “Políticas” en la página 92 y Information Center de IBM WebSphere Service Registry and Repository, Versión 8.0 - Creación de una política de mediación.
5. Pulse **Finalizar**.

Resultados

Se crea la política y se almacena en WSRR. Para ver el documento de políticas de la política que ha creado, seleccione el documento de políticas en el widget del

navegador del registro de servicios. Como alternativa, busque el nombre especificado, incluida la terminación `.xml`. El documento de política se visualizará en el widget Detalle del registro de servicio, en el lado derecho.

Conceptos relacionados:

"Políticas" en la página 92
Detalles de implementación para utilizar WSRR como el punto de creación de políticas y WebSphere DataPower como punto de aplicación de políticas al crear políticas de mediación.

Información relacionada:

Information Center de IBM WebSphere Service Registry and Repository, Versión 8.0 - Creación de una política de mediación

Creación de nuevas políticas de supervisión

Puede crear políticas de supervisión nuevas utilizando la interfaz de usuario web WSRR. Cuando cree las políticas de supervisión, especifique las condiciones y las acciones para la política.

Antes de empezar

Para obtener información sobre cómo acceder a la interfaz de usuario web de WSRR, consulte "Conexión a WSRR - Interfaz de usuario web WSRR" en la página 84.

Procedimiento

1. Abra la interfaz de usuario web de WSRR.
2. Pulse **Ver** > **Documentos del servicio** > **Documentos de política** y en la vista de recopilación pulse **Nuevo**.
3. De la lista de marcos de políticas disponible seleccione **Supervisión**. Pulse **Siguiente**. De este modo se crea un documento de política que contiene una expresión de política raíz.
4. Escriba un nombre descriptivo y una descripción opcional.
5. Pulse el separador Política, pulse **Editar documento de políticas**, y añada condiciones y acciones según sea necesario. Para obtener más información sobre condiciones y acciones, siga los enlaces relacionados.
6. Pulse **Publicar**.

Resultados

Se crea la política y se almacena en WSRR. Puede ver el documento de política para la política en Business Space, seleccione el documento de políticas en el widget del navegador del registro de servicios. Como alternativa, busque el nombre especificado, incluida la terminación `.xml`. El documento de política se visualizará en el widget Detalle del registro de servicio, en el lado derecho.

Conceptos relacionados:

"Políticas" en la página 92
Detalles de implementación para utilizar WSRR como el punto de creación de políticas y WebSphere DataPower como punto de aplicación de políticas al crear políticas de mediación.

Información relacionada:

Tareas de creación de políticas

Trabajo con la herramienta de creación de políticas

Gestión de políticas

Las políticas se pueden editar o eliminar utilizando la interfaz de usuario de Business Space.

Antes de empezar

Configure el espacio de gobierno SOA. Para obtener más información, consulte “Configuración de Business Space para utilizarlo por primera vez” en la página 83.

Procedimiento

1. Para abrir el documento de política de la política, seleccione el documento de política en el widget del navegador del registro de servicios situado en la parte inferior izquierda de la pantalla. Como alternativa, busque el nombre especificado, incluida la terminación `.xml`. El documento de política se visualizará en el widget Detalle del registro de servicio, en el lado derecho.
2. Para cambiar los detalles de la política:
   a. Pulse el icono Editar en este widget para editar el documento de política. Se visualiza una ventana con opciones para editar los detalles de la política.
   b. Si la política tiene condiciones o acciones, éstas se visualizarán. Cree y modifique las condiciones y las acciones según sea necesario.
   c. Pulse **Finalizar** para guardar y cerrar el editor de políticas. El widget de detalles del registro de servicios se renovará para mostrar los cambios realizados.
3. Para suprimir la política:
   a. Cambie la política a un estado de gobierno que permita la edición o supresión del documento de política. Para obtener más información sobre la transición de una política a través del ciclo de vida de la política SOA, consulte “Gestión del ciclo de vida de la política”.
   b. Pulse **Acción** > **Suprimir**. La opción Suprimir figura en el menú.
   c. Seleccione **Suprimir** para suprimir la política.
   d. Pulse **Sí** para confirmar la supresión.

Información relacionada:

Information Center de IBM WebSphere Service Registry and Repository, Versión 8.0

Information Center de IBM WebSphere Service Registry and Repository, Versión 8.0 - Políticas del perfil de habilitación de gobierno

Gestión del ciclo de vida de la política

Las políticas se pueden cambiar de un estado de gobierno a otro utilizando la interfaz de usuario de Business Space. Las políticas deben estar en el estado Aprobado para que DataPower las aplique.

Acerca de esta tarea

Para obtener más información sobre gobiernos, consulte “Ciclo de vida de política SOA” en la página 5.

Procedimiento

Para cambiar una política a un estado diferente del ciclo de vida, complete los pasos siguientes. Repita estos pasos tantas veces como sea necesario para alcanzar el estado de ciclo de vida deseado:

1. En Business Space, abra el documento de política seleccionando el documento en el widget del navegador del registro de servicios. Como alternativa, busque el nombre especificado, incluida la terminación `.xml`. El documento de política se visualizará en el widget Detalle del registro de servicio. La propiedad **Estado de gobierno** muestra el estado de gobierno actual del perfil.
2. Pulse **Acción**. Se mostrará una lista de las transiciones posibles de ciclo de vida junto con otras operaciones posibles.
3. Seleccione la transición de ciclo de vida necesaria para mover la política al estado necesario. Se actualizará la propiedad **Estado de gobierno** de la política para mostrar el nuevo estado de ciclo de vida.

Conceptos relacionados:

"Ciclo de vida de política SOA" en la página 5
Las políticas se gobiernan utilizando el ciclo de vida de política SOA. El ciclo de vida se inicia con definición de la política, luego se despliega durante la producción y finalmente se deja de utilizar cuando ya no es necesaria.

Información relacionada:

Information Center de IBM WebSphere Service Registry and Repository, Versión 8.0 - Ciclo de vida de la política SOA

Políticas adjuntas a un servicio

Se pueden adjuntar políticas a un servicio utilizando WSRR.

Para obtener más información, consulte Information Center de IBM WebSphere Service Registry and Repository, Versión 8.0 - Tareas de adjuntos de política.

Capítulo 7. Resolución de problemas

Obtenga ayuda acerca del diagnóstico de los problemas que pueda experimentar antes, durante y después del despliegue del patrón.

Utilice los enlaces para buscar temas relevantes para un problema con los patrones.

Resolución de problemas con el despliegue

Puede resolver problemas comunes que surjan al desplegar patrones en el Patrón IBM SOA Policy Gateway.

Error de conexión con el dispositivo DataPower externo durante el despliegue

Pruebe las siguientes soluciones:

- Consulte al administrador de DataPower si el usuario y la contraseña son válidos:
  - En la interfaz gráfica de usuario web DataPower, compruebe si existe el usuario mediante **Panel de control** > **Gestionar cuentas de usuario**.
  - Compruebe que la cuenta exista.
  - Compruebe que el usuario tenga el privilegio de utilizar la interfaz de gestión XML por ejemplo, de administrador del sistema.
  - Puede que el administrador de DataPower deba comprobar si la cuenta de usuario está habilitada en los valores de agente de usuario, por ejemplo, los valores de autenticación básica.
- Compruebe que el nombre de host de DataPower sea correcto.
- Compruebe que la interfaz de gestión XML de DataPower está habilitada.

Resolución de un error para el dominio ya existente

Pruebe la solución siguiente:

- En el Panel de control de DataPower, abra los Dominios de aplicación. Compruebe si el dominio ya existe.

Resolución de un error de solapamiento de puertos para la aplicación de ejemplo

Si uno de los servicios de ejemplo no está disponible, compruebe si los puertos de su dominio están en conflicto con otros dominios.

Pruebe las siguientes soluciones:

- Inicie la sesión en DataPower y cambie al dominio de ejemplo. A continuación, abra el panel de control y pulse el icono de cortafuegos XML. Compruebe que los cortafuegos XML están todos en estado activo.
- Busque el manejador frontal HTTP. Compruebe que el manejador frontal HTTP individual esté estado activo.

Resolución de un error de promoción

Pueden surgir muchos problemas durante la promoción, incluido un error de conexión con el maestro de gobierno durante el despliegue.

Pruebe las siguientes soluciones:

- Compruebe los parámetros:
  - Compruebe el usuario de la célula WSRR del maestro de gobierno.
  - Compruebe la contraseña del usuario de la célula WSRR del maestro de gobierno.
  - Compruebe el nombre de host de la célula del maestro de gobierno WSRR.
  - Compruebe el nombre de la célula del maestro de gobierno WSRR.
- Compruebe el intercambio de certificados de firmante:
  - Vaya al almacén de confianza predeterminado de la célula del maestro de gobierno y asegúrese de que hay una entrada de certificado para el gestor de despliegue o el servidor autónomo del entorno de ejecución.
  - Vaya a cada entorno de ejecución, examine el almacén CellDefaultTrust (para el entorno ND) o NodeDefaultTrustStore (para servidores autónomos WSRR) y compruebe que existe un certificado para el gestor de despliegue del maestro de gobierno.
  - Exporte las claves LTPA desde ambas células utilizando la misma contraseña, y compruebe que sean iguales (por ejemplo, los bytes).
- Asegúrese de que el archivo de propiedades de promoción contiene secciones de servidor con el host y el puerto correctos, y la información de usuario y la contraseña. Esta información se puede encontrar en la consola para el Gobierno ServiceRegistry Maestro:
  - Vaya a GovernanceMasterDMgrHost o ServiceRegistry y cambie a la perspectiva de configuración. En la sección Acciones, busque **Promoción** y abra el archivo de propiedades de promoción. Para cada entorno debería haber elementos XML para cada servidor en el nodo o clúster WSRR de transición. Si existe un clúster de producción o nodo, debe haber entradas server:port para cada uno, y además debe haber información de usuario y contraseña.
- Compruebe que la versión de servicio y el punto final de servicio SOAP tienen la clasificación para la transición y la producción.
  - En la consola del registro de servicio, seleccione la perspectiva de gobierno SOA. Abra la versión de servicio, y seleccione el separador Clasificaciones. Transición y producción deben estar habilitados.

Resolución de errores de la CLI personalizada

Pruebe las siguientes soluciones:

- Examine el archivo defaultLog para ver si hay mensajes de error en el dominio DataPower.
- Habilite la depuración de la CLI y compruebe los registros antes de cualquier ejecución adicional de la CLI.

Resolución de problemas en la instancia desplegada

Puede resolver problemas comunes en la instancia desplegada.

Conexiones fallidas con el servidor LDAP o el puerto StoreWSP de DataPower

Podría haber un problema en los valores de dominio si los archivos de registro de DataPower muestran un error de conexión con LDAP o la pasarela StoreWSP y si está utilizando el alias de host; por ejemplo, `xyz` en lugar del nombre de host completo `xyz.company.com` para uno de los parámetros siguientes contenidos en el paquete script:

- El nombre de host de DataPower
- El nombre de host de LDAP

Pruebe la solución siguiente:

1. En la Consola de administración de DataPower, conmute al dominio predeterminado.
2. Busque `Configurar valores de DNS`.
3. Pulse el separador Buscar dominios.
4. Compruebe que el dominio; por ejemplo, `company.com`, está en la lista. Si no está en la lista, pulse `Añadir` y añádalo a la lista.

Problemas con la supervisión

Si la supervisión no está disponible en los nodos desplegados, debe verificar que los servicios compartidos necesarios se estén ejecutando. Vaya a **Instancias** > **Servicios compartidos**

Verifique que Supervisión del sistema y Supervisión del sistema para WebSphere DataPower se ejecutan en el mismo grupo de nubes que sus instancias desplegadas. Para la supervisión de WSRR, compruebe también que la Supervisión del sistema para WebSphere Application Server se esté ejecutando en el grupo de nubes.

Recopilación de información de diagnóstico

Puede utilizar archivos de registro como ayuda para encontrar y resolver problemas. Los archivos de registro se almacenan en el dispositivo y se pueden ver desde la interfaz de usuario o se pueden descargar en el sistema de archivos local.

Procedimiento

Para recoger información de diagnóstico, complete los pasos siguientes:

1. Examine las instancias virtuales:
   a. Pulse **Instancias** > **Sistema virtual**.
   b. Seleccione la instancia en la lista de instancias que aparece en la ventana Instancias del sistema virtual.
2. Para la máquina virtual de WSRR:
   a. En la sección **Máquinas virtuales**, expanda la máquina virtual de WSRR y compruebe si hay errores en la sección **Paquetes script**. Si cualquiera de los paquetes script tiene errores, pulse los enlaces de archivo de registro correspondientes a **remote_std_out.log** y **remote_std_err.log** situados junto a los nombres de los paquetes de script.
   b. Inicie una sesión en la instancia de WSRR y examine los errores del servidor.

c. Consulte las guías de resolución de problemas de WSRR: http://pic.dhe.ibm.com/infocenter/sr/v8r0/topic/com.ibm.sr.doc/cwsr_troubleshootingandsupport.html

3. Para DataPower:
   a. Obtenga el archivo **default.log** del dominio creado por el patrón.
   b. Obtenga el archivo **default.log** del dominio predeterminado.
4. Para problemas de supervisión, recopile estos registros de los nodos de WSRR y Base OS (excluyendo los nodos personalizados de WSRR):
   - `/0config/0config.log`
   - `/opt/IBM/maestro/ITCAMSOADP/lx8266/d4/KD4/logs/*` (x86)
   - `/opt/IBM/maestro/ITCAMSOADP/aix523/d4/KD4/logs/*` (Power)

Capítulo 8. Mantenimiento y soporte

Puede realizar funciones de mantenimiento tales como aplicar arreglos de emergencia.

Añadir un arreglo de emergencia al catálogo

Los arreglos temporales y fixpacks se aplican a las instancias del sistema virtual como arreglos de emergencia. Puede añadir arreglos de emergencia al catálogo para aplicarlos a las imágenes virtuales.

Antes de empezar

Debe tener asignado el permiso *Crear nuevo contenido de catálogo* o el rol de *Administrador* de dispositivos de IBM Workload Deployer con los permisos completos para realizar estos pasos.

Acerca de esta tarea

Los arreglos los proporciona IBM o un proveedor de imágenes y deben descargarse. Los arreglos nuevos se descargan desde la central de arreglos de IBM. A continuación, los arreglos se transfieren al catálogo y se pueden aplicar a todas las instancias de sistema virtual aplicables.

Procedimiento

Realice los pasos siguientes para añadir un arreglo de emergencia al catálogo.

1. Localice y descargue el arreglo (o arreglos) de emergencia desde la central de arreglos.
2. Opcional: Puede añadir varios arreglos temporales a la vez. Para añadir varios arreglos a la vez, descargue los archivos comprimidos desde la central de arreglos y empaquételos en un único archivo comprimido.
3. En el menú, seleccione **Catálogo** > **Arreglos de emergencia**.
4. Pulse el icono Añadir en el panel izquierdo.
5. Escriba un nombre para el arreglo. Si lo desea, también puede añadir una descripción del arreglo que está añadiendo. En el panel izquierdo de la ventana Arreglos de emergencia se muestra el arreglo, y en el panel derecho se muestra la información del arreglo.
6. Vaya a la ubicación donde ha almacenado el arreglo y pulse **Cargar**. Para mayor seguridad, solo se pueden transferir archivos .zip, .tgz y .pak. También se da soporte a Red Hat RPM.
7. Complete la información sobre el arreglo. Puede otorgar acceso a los usuarios y proporcionar una valoración de gravedad. Utilice el campo **Aplicable a** para especificar la imagen virtual o imágenes virtuales a las que se aplica este arreglo.

Resultados

El arreglo de emergencia se encuentra en el catálogo y está disponible para ser aplicado a las imágenes del sistema virtual.

Aplicación de un arreglo de emergencia

Los arreglos temporales y fixpacks se aplican a las instancias del sistema virtual como arreglos de emergencia. Puede aplicar arreglos de emergencia para las imágenes del sistema virtual.

Antes de empezar

Para realizar estos pasos, debe tener asignado acceso total para la instancia del sistema virtual o tener asignado el rol de administración de dispositivos con permisos totales. La instancia de sistema virtual debe estar iniciada para planificar o aplicar el servicio. El arreglo de emergencia debe estar añadido al catálogo antes de que pueda aplicarse al sistema virtual.

Acerca de esta tarea

Cuando se añade un arreglo de emergencia, debe definir las imágenes virtuales a las que se puede aplicar el arreglo. La lista de arreglos disponibles cuando se planifica una solicitud de servicio se crea utilizando todos los arreglos aplicables a la imagen virtual utilizada para crear la instancia de sistema virtual. Si ya se ha aplicado un arreglo al sistema virtual, puede verlo en la lista **Historial** y no se incluye en la lista de arreglos disponibles.

Nota: Debe cerrar todos los procesos de WSRR y WAS antes de instalar un arreglo de emergencia. Inicie sesión utilizando SSH en todos los nodos WSRR, y cierre los procesos con los mandatos **`stopServer.sh`** y **`stopNode.sh`** (solo nodos personalizados).

Procedimiento

Complete los pasos siguientes para aplicar un arreglo temporal.

1. Seleccione una instancia de sistema virtual a la que desee aplicar el arreglo en la ventana Instancias del sistema virtual.
2. Pulse el icono **Aplicar servicio**.
3. Opcional: Planifique la solicitud de servicio. De forma predeterminada, el arreglo se aplica inmediatamente. Para planificar que se aplicará en un momento posterior, pulse **Planificación de servicio** y proporcione la información necesaria.
4. Pulse **Seleccionar nivel de servicio o arreglos**.
5. Pulse **Aplicar arreglos de emergencia** para ver y seleccionar el arreglo a aplicar. El arreglo de emergencia se aplica a todas las máquinas virtuales de la instancia de sistema virtual. El estado de la instancia de sistema virtual muestra que el servicio se ha aplicado en el sistema virtual.
6. Comprobar si hay errores. Compruebe los archivos siguientes para asegurarse de que no se han producido errores durante el proceso de aplicación de los arreglos de emergencia :
   - Remote_std_out.log
   - Remote_std_err.log

   Puede acceder a los archivos de registro desde la ventana Instancias de sistema virtual.

Capítulo 9. Apéndices

Avisos

Esta información se ha creado para productos y servicios ofrecidos en los Estados Unidos.

Es posible que en otros países IBM no ofrezca los productos, los servicios o las características que se describen en este documento. Consulte al representante de IBM de su zona para obtener información acerca de los productos y servicios que están actualmente disponibles en su zona. Cualquier referencia a un producto, programa o servicio de IBM no pretende indicar ni implica que sólo se pueda utilizar este producto, programa o servicio de IBM. En su lugar, se puede utilizar cualquier producto, programa o servicio funcionalmente equivalente que no infrinja ninguno de los derechos de propiedad intelectual de IBM. Sin embargo, es responsabilidad del usuario evaluar y verificar el funcionamiento de cualquier producto, programa o servicio que no sea de IBM.

IBM puede tener patentes o solicitudes de patentes pendientes que cubran el tema principal que se describe en este documento. El suministro de este documento no le otorga ninguna licencia sobre estas patentes. Puede enviar preguntas acerca de licencias por escrito a:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
Estados Unidos

Para realizar consultas sobre licencias relativas a la información de doble byte (DBCS), póngase en contacto con el Departamento de propiedad intelectual de IBM de su país o envíe sus consultas, por escrito, a:

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

El párrafo siguiente no se aplica al Reino Unido ni a ningún otro país donde estas disposiciones contradigan la legislación vigente: INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN "TAL CUAL" SIN NINGÚN TIPO DE GARANTÍA, YA SEA EXPLÍCITA O IMPLÍCITA, INCLUYENDO, PERO SIN LIMITARSE A, LAS GARANTÍAS IMPLÍCITAS DE NO INCUMPLIMIENTO, COMERCIABILIDAD O IDONEIDAD PARA UNA FINALIDAD DETERMINADA. Algunos países no permiten la declaración de limitación de responsabilidad de las garantías expresas o implícitas en determinadas transacciones, por lo que puede esta declaración no se aplique a su caso.

Esta publicación puede contener imprecisiones técnicas o errores tipográficos. La información que ofrece está sometida a modificaciones periódicas, las cuales se van incorporando en ediciones posteriores. IBM se reserva el derecho de realizar mejoras y/o cambios en los productos y/o programas descritos en esta publicación en cualquier momento sin previo aviso.

Cualquier referencia en esta información a sitios Web que no son de IBM se proporciona solamente para su comodidad y no equivale de ninguna manera a una aprobación de esos sitios Web. Los materiales de esos sitios Web no forman parte de los materiales de este producto de IBM y la utilización de esos sitios Web se realiza bajo la responsabilidad exclusiva del usuario.

IBM puede utilizar o distribuir cualquier información que el usuario le proporcione de la manera que considere adecuada sin incurrir en ninguna obligación con el usuario.

Los propietarios de licencia de este programa que deseen tener información sobre el mismo con el fin de poder: (i) intercambiar información entre programas creados de forma independiente y otros programas (incluido éste) y (ii) utilizar de forma mutua la información que se ha intercambiado, deberán ponerse en contacto con:

IBM Corporation
Software Interoperability Coordinator, Department 49XA
3605 Highway 52 N
Rochester, MN 55901
Estados Unidos

Esta información puede estar disponible, bajo las condiciones y los términos adecuados, incluyendo en algunos casos, el pago de una cuota.

IBM proporciona el programa bajo licencia descrito en esta información y todo el material con licencia disponible para el mismo bajo los términos del Acuerdo de cliente de IBM, el Acuerdo de licencia de programa internacional de IBM o cualquier acuerdo equivalente entre las dos partes.

Cualquier información de rendimiento contenida aquí fue determinada en un entorno controlado. Por consiguiente, los resultados obtenidos en otros entornos operativos pueden variar significativamente. Pueden haberse realizado algunas mediciones en sistemas en nivel de desarrollo y no existen garantías de que estas mediciones sean las mismas en sistemas disponibles para todos los usuarios. Además, es posible que algunas mediciones se haya estimado mediante extrapolación. Los resultados reales pueden variar. Los usuarios de este documento deben verificar los datos aplicables para su entorno específico.

La información referente a productos que no son de IBM se ha obtenido de los suministradores de estos productos, sus anuncios publicados u otras fuentes disponibles para el público. IBM no ha probado esos productos y no puede confirmar la precisión del rendimiento, la compatibilidad ni ninguna otra afirmación relacionada con los productos no IBM. Las preguntas acerca de las posibilidades de productos que no son de IBM deben dirigirse a los suministradores de estos productos.

Todas las declaraciones referentes a acciones e intenciones futuras de IBM pueden cambiar o ser retiradas sin previo aviso y solamente representan objetivos.

Esta información contiene ejemplos de datos e informes utilizados en operaciones cotidianas de negocios. Para ilustrarlos de la manera más completa posible, los ejemplos incluyen nombres de personas, compañías, marcas y productos. Todos estos nombres son ficticios y cualquier parecido con nombres y direcciones utilizadas por una empresa de negocios real es mera coincidencia.

LICENCIA DE COPYRIGHT:

Esta información contiene programas de aplicación de ejemplo en lenguaje fuente, que ilustran cómo se realiza la programación en diversas plataformas operativas. Puede copiar, modificar y distribuir estos programas de ejemplo de cualquier modo sin realizar ningún pago a IBM, con el fin de desarrollar, utilizar, comercializar o distribuir programas de aplicación que se ajusten a la interfaz de programación de aplicaciones para la plataforma operativa para la que se han escrito los programas de ejemplo. Estos ejemplos no se han probado a fondo en todas las condiciones. Por consiguiente, IBM no puede garantizar ni implicar la fiabilidad, la capacidad de servicio o el funcionamiento de estos programas.

Si ve esta información en copia software, es posible que no aparezcan las fotografías y las ilustraciones en color.

Información de interfaz de programación

La información de interfaz de programación, si se proporciona, está destinada a ayudarle a crear software de aplicación para utilizar con este programa.

Sin embargo, este información puede contener también información de diagnosis, modificación y ajuste. La información de diagnosis, modificación y ajuste se proporciona para ayudarle a depurar el software de aplicación.

Importante: No utilice esta información de diagnóstico, modificación y ajuste como una interfaz de programación porque está sujeta a cambios.

Marcas registradas

IBM, el logotipo de IBM, ibm.com, son marcas registradas de IBM Corporation, registradas en muchas jurisdicciones en todo el mundo. Existe una lista actual de marcas registradas de IBM en la Web bajo “Copyright and trademark information” www.ibm.com/legal/copytrade.shtml. Otros nombres de productos y de servicios pueden ser marcas registradas de IBM o de otras compañías.

Este producto incluye software desarrollado por Eclipse Project (http://www.eclipse.org/).

Java y todas las marcas comerciales y los logotipos basados en Java son marcas registradas de Oracle y/o sus asociados.

Envío de comentarios a IBM

Si existe algún aspecto de este manual que le agrada especialmente o que no le agrada en absoluto, utilice uno de los métodos que se indican a continuación para enviar sus comentarios a IBM.

No dude en enviarnos comentarios sobre aquello que considere un error o una omisión, así como comentarios sobre la precisión, la organización, el tema o la exhaustividad de este manual.

Limite sus comentarios a la información de este manual y a la forma de presentar la información.

Para realizar comentarios sobre las funciones de los productos o sistemas IBM, póngase en contacto con el representante de IBM o con el concesionario de IBM autorizado.

Cuando se envía información a IBM, se otorga a IBM un derecho no exclusivo para utilizar o distribuir la información de cualquier manera que considere adecuada, sin incurrir en ninguna obligación hacia el usuario.

Puede enviar los comentarios a IBM de cualquiera de estas formas:

- Por correo, a esta dirección:

  User Technologies Department (MP095)
  IBM United Kingdom Laboratories
  Hursley Park
  WINCHESTER,
  Hampshire
  SO21 2JN
  Reino Unido
- Por fax:
  - Desde fuera del Reino Unido, después del código de acceso internacional utilice 44-1962-816151
  - Desde el Reino Unido, utilice 01962-816151
- De forma electrónica, utilice el ID de red apropiado:
  - Intercambio de correo de IBM: GBIBM2Q9 at IBMMAIL
  - IBMLink: HURSLEY(IDRCF)
  - Internet: idrcf@hursley.ibm.com

Independientemente del método que utilice, asegúrese de incluir:

- El título y el número de pedido de la publicación
- El tema al que se aplican los comentarios
- Su nombre y dirección/número de teléfono/número de fax/ID de red.