patrón de pasarela de política SOA de IBM

Contenido

Capítulo 1. Visión general de la política SOA 1
La arquitectura de política SOA 1
Ciclo de vida de política SOA 4
Estándares de políticas 5

Capítulo 2. Visión general del patrón . . 9

Capítulo 3. Iniciación al patrón de pasarela de política SOA de IBM. . . . 11
Cómo descargar e instalar los patrones 12
Verifique el patrón instalado. 13
Configuración del acceso de usuario 14

Capítulo 4. Patrones, componentes y paquetes script 17
Patrones 17
Ejemplo del tiempo de ejecución básico de la pasarela de política SOA 18
Maestro de gobierno de pasarela de política SOA 20
Tiempo de ejecución básico de la pasarela de política SOA 22
Tiempo de ejecución avanzado de pasarela de política SOA 24
Componentes. 27
Componente DB2 Enterprise. 27
Componente DB2 Enterprise HADR Primary . . 31
Componente DB2 Enterprise HADR Standby . . 34
Componente Servidor WSRR autónomo 38
Componenente Gestor de despliegue de WSRR 42
Componente Nodos personalizados de WSRR . . 44
Paquetes de scripts 47
Script: SOA Policy Gateway 2.0.0.0 - Dominio DataPower 47
Script: SOA Policy Gateway 2.0.0.0 - Promoción 50
Script: SOA Policy Gateway 2.0.0.0 - Ejemplo . . 52
Script: SOA Policy Gateway 2.0.0.0 - Seguridad 56

Capítulo 5. Trabajar con el patrón de pasarela de política SOA de IBM . . . 61
Planificación de la configuración del patrón y los requisitos previos del patrón 61
Configuración de DataPower para el patrón de pasarela de política SOA de IBM 63
Seguridad para los patrones patrón de pasarela de política SOA de IBM 63
Configuración de LDAP para el ejemplo. . . . 70
Despliegue de patrones 72
Despliegue del patrón Ejemplo del tiempo de ejecución básico de la pasarela de política SOA . 73
Despliegue del patrón Maestro de gobierno de pasarela de política SOA 74
Despliegue del patrón Tiempo de ejecución básico de la pasarela de política SOA 75
Despliegue del patrón Tiempo de ejecución avanzado de pasarela de política SOA 77
Verificación del despliegue 78
Caso de ejemplo: añadir un tiempo de ejecución adicional al patrón 78
Clonación y personalización del patrón de pasarela de política SOA de IBM 79
Despliegue con varios dominios DataPower . . 80
La aplicación de ejemplo 81
Visión general de los artefactos de WSRR del ejemplo. 82
Ejecución de los casos de prueba de ejemplo . . 83
Ampliación de la aplicación de ejemplo 89
Exploración adicional del ejemplo 93
El dominio DataPower de ejemplo. 94

Capítulo 6. Cómo trabajar con la instancia desplegada 103
Administración de instancias desplegadas 103
Conexión a WSRR - Business Space 104
Conexión a WSRR - Consola del registro de servicios 105
Configuración de Business Space para utilizarlo por primera vez 105
Configuración de patrones después del despliegue 106
Cambios de los valores de LDAP para la aplicación de ejemplo 107
Valores de DN de certificado para certificados de DataPower 107
Modificación de las claves LTPA 107
Añadir o eliminar certificados DataPower para el almacén de WSRR 108
Configuración del punto de aplicación de políticas 108
Utilización del patrón Tiempo de ejecución básico de la pasarela de política SOA 110
Utilización del patrón Tiempo de ejecución avanzado de pasarela de política SOA 111
Objetos DataPower creados en los patrones Tiempo de ejecución básico y Tiempo de ejecución avanzado. 112
Creación y gobierno de servicios 112
Políticas 113
Creación de nuevas políticas 118
Gestión de políticas 119
Gestión del ciclo de vida de la política 120
Políticas adjuntas a un servicio 121

Capítulo 7. Resolución de problemas 123
Resolución de problemas con el despliegue . . . 123
Resolución de problemas en la instancia desplegada 126
Recopilación de información de diagnóstico . . . 127

Capítulo 8. Mantenimiento y soporte 129

Añadir un arreglo de emergencia al catálogo . . . 129
Aplicación de un arreglo de emergencia 130

Capítulo 9. Appendices 131

Avisos 131
Información de interfaz de programación . . . 133
Marcas registradas. 133
Envío de comentarios a IBM 133

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. Los métodos de la arquitectura orientada a servicios (SOA) ayudan a las empresas a identificar y focalizar los servicios clave de la empresa. Al añadir políticas, se añaden puntos de control y se agilizan la tecnología empresarial y la tecnología de lainformación. Como resultado, SOA resulta más consumible, se mejora el tiempo de generación de valor para los usuarios empresariales con costes reducidos para sus proyectos y se acelera la adopción de soluciones SOA.

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 creación 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 este patrón, el PAP se consigue utilizando WSRR y el PEP se consigue utilizando WebSphere DataPower.

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

- **Punto de creación 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. Incluye un repositorio para almacenar políticas. En este patrón, esto se logra mediante WSRR.
- **Punto de aplicación de políticas**: es un punto funcional que se ejecuta en el middleware. Realiza lo siguiente:
  - 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 realmente se aplican las políticas y entran en vigor, dependiendo de la etapa del ciclo de vida:
    - Durante el diseño, el registro de servicios y el propio repositorio son los puntos 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, esto se logra mediante WebSphere DataPower.

- **Punto de decisión de política**: evalúa las solicitudes de los participantes por comparación con políticas relevantes o contratos y atributos. Entrega una decisión de autorización, elegibilidad o validación para proporcionar resultados calculados.
- **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**: es 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. Esto incluye:
  - 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.

  Nota: Este patrón no incluye supervisión.

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 del patrón accionable de la política SOA se muestra en la Figura 1 en la página 3 y se describe a continuación.

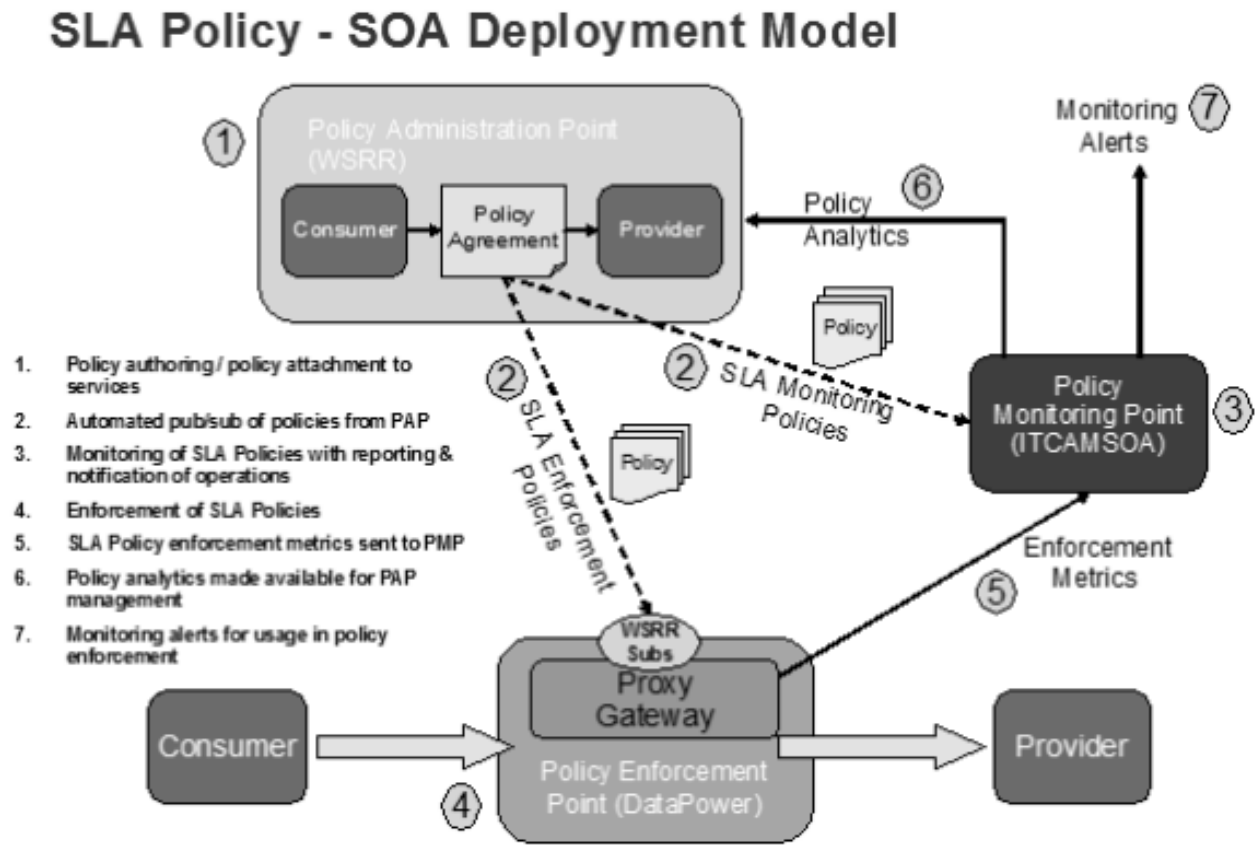


Figura 1. Política de Acuerdo de nivel de servicio (SLA): el modelo de despliegue de SOA

1. Las políticas se crean y después se adjuntan a servicios que necesitan esa política. Normalmente, esto sigue el orden siguiente:
   a. El conjunto de servicios se carga o crea en el repositorio de servicios. Esto forma parte del punto de creación de políticas.
   b. El conjunto de políticas necesarias se crea en el punto de creación de políticas utilizando el ciclo de vida de la política:
      1) 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 creación de políticas a los puntos de aplicación de políticas y el punto de supervisión de política:

   Nota: Este patrón no incluye supervisión mediante ITCAM para SOA.
   a. Como parte de la configuración, ITCAM para SOA se suscribe a la política de supervisión desde WSRR. Esto se produce una sola vez.
   b. Como parte de la configuración, se crean pasarelas de proxy en cada dispositivo de WebSphere Data Power que tenga transacciones de servicio con aplicación de políticas. Esto se lleva a cabo una sola vez y se añade o se modifica, según sea necesario.
   c. Como parte de la configuración, cada pasarela proxy del dispositivo se suscribe a políticas de WSRR para servicios de los que es responsable. Esto se lleva a cabo una sola vez y se añade o se modifica, según sea necesario.

d. Como parte de la configuración, WebSphere DataPower se configura de modo que las políticas se puedan compartir con otros dispositivos de un clúster. Esto se lleva a cabo una sola vez y se añade o se modifica, según sea necesario.
e. ITCAM para SOA descarga las políticas de supervisión a medida que se publican.
f. ITCAM para SOA convierte las políticas en la representación interna denominada políticas de situación.
g. WebSphere DataPower descarga los WSDL para los servicios de los que es responsable.
h. WebSphere DataPower descarga las políticas para los servicios de los que es responsable, cuando se lo notifica WSRR.
i. WebSphere DataPower convierte las políticas internas en la representación WebSphere DataPower interna con el formato de objetos SLM.

3. Supervisión de políticas SOA con operaciones de generación de informes y notificaciones:
   a. Las políticas de supervisión están activas en ITCAM para la política de situación SOA.
   b. ITCAM para SOA recibe información de supervisión y coloca esta información en los espacios de trabajo.

   Nota: No se proporciona supervisión en este patrón.
4. Aplicación de políticas SOA:
   a. La aplicación de políticas está activa en los diferentes dispositivos WebSphere DataPower.
   b. WebSphere DataPower recibe las transacciones de servicios y aplica políticas para dicho servicio de consumidor y para el proveedor de servicios.
5. El punto de aplicación de políticas envía estadísticas de aplicación de políticas SOA al punto de supervisión de políticas.

   Nota: Este patrón no incluye supervisión.
6. El punto de supervisión de políticas envía sucesos de supervisión al punto de creación de políticas:
   a. Se configuran sucesos en el punto de creación de políticas que se necesita supervisar desde el punto de supervisión de políticas. Esto se lleva a cabo una sola vez y se añade o se modifica, según sea necesario.
   b. 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.

   Nota: Este patrón no incluye supervisión.
7. Supervisión de alertas:
   a. 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 de mediación se gobiernan utilizando el ciclo de vida de política SOA. Inicialmente se define 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 la política aplicable 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/WSMediationPolicy1.6-20120124.pdf.

El modelo de datos de WS-Policy incluye:

- **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. 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 anterior sería que una invocación de un servicio web firmará o cifrará 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.

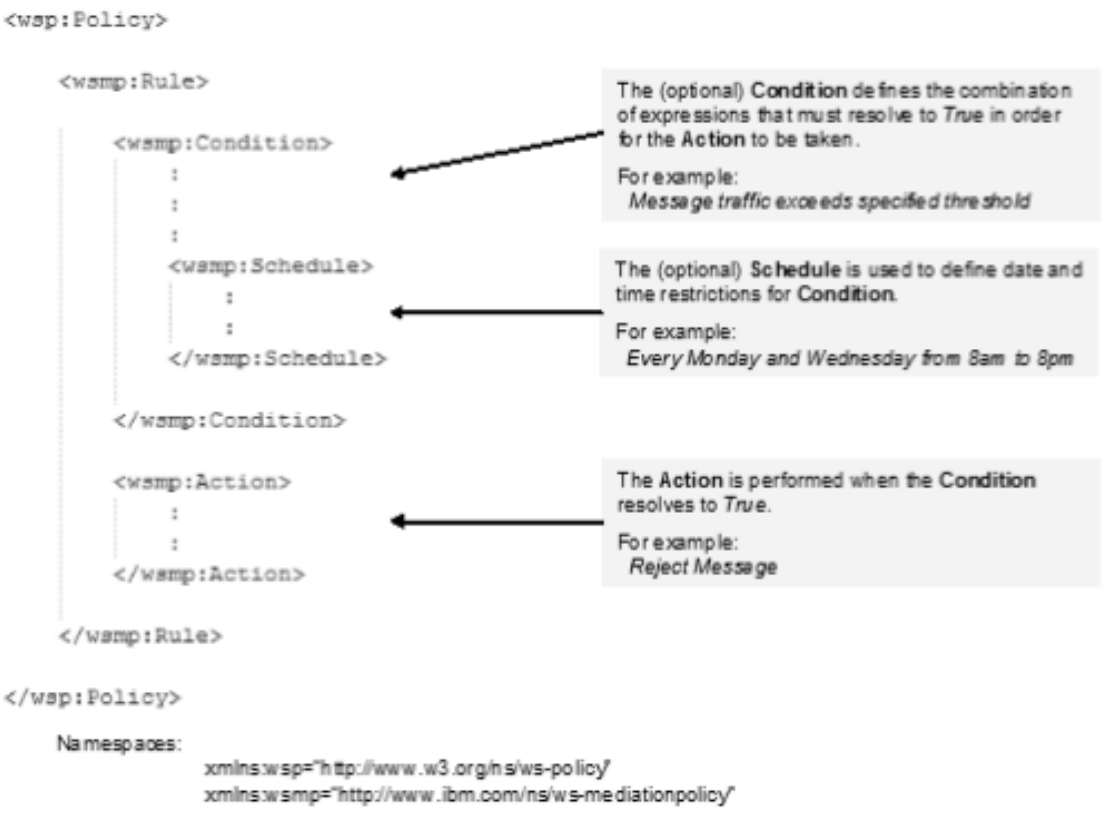


Figura 3. Visión general de la estructura de la política

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>` seguido del 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 de pasarela de política SOA de IBM es un conjunto de patrones de sistema virtual que proporcionan un punto de aplicación de políticas y un punto de administración de políticas. 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 es proporcionado por el dispositivo WebSphere DataPower en el que se crea un dominio durante el despliegue del patrón de sistema virtual.

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 ello, puede utilizar definiciones de nivel de servicio (SLD) y acuerdos de nivel de servicio (SLA). Este patrón permite definir políticas para la SLD y el SLA de un modo administrado, definido, gobernado y utilizado de forma eficaz. Los tipos de política se utilizan en este patrón incluyen lo siguiente:

- **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 los medios para aplicar políticas de seguridad de control de accesos de XACML. Estas políticas no están gobernadas dentro del punto de administración de políticas en este momento.

El patrón patrón de pasarela de política SOA de IBM contiene los patrones de sistema virtual siguientes:

- Ejemplo del tiempo de ejecución básico de la pasarela de política SOA
- Maestro de gobierno de pasarela de política SOA
- Tiempo de ejecución básico de la pasarela de política SOA
- Tiempo de ejecución avanzado de pasarela de política SOA

Los cuatro patrones de sistema virtual trabajan conjuntamente para proporcionar un entorno de gobierno de servicios de varias etapas. El patrón de pasarela de política SOA de IBM también permite proporcionar varios dominios DataPower configurados al entorno de gobierno durante el despliegue del patrón. Combinadas, se proporcionan las topologías de despliegue siguientes:

- Despliegue autónomo
- Despliegue piloto
- Despliegue de producción completo

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

Se puede configurar manualmente el patrón de sistema virtual desplegado para incluir la supervisión con ITCAM para SOA Versión 7. Esto proporciona una supervisión básica de sucesos y amplía el soporte de política para incluir políticas de supervisión. Las políticas de supervisión permiten definir situaciones de suceso dentro del Punto de creación de políticas (PAP) y asociarlas a una definición de servicio, lo que permite que el supervisor actúe cuando se produce la situación de suceso.

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. Los métodos de la arquitectura orientada a servicios (SOA) ayudan a las empresas a identificar y focalizar los servicios clave de la empresa. Al añadir políticas, se añaden puntos de control y se agilizan la tecnología empresarial y la tecnología de lainformación. Como resultado, SOA resulta más consumible, se mejora el tiempo de generación de valor para los usuarios empresariales con costes reducidos para sus proyectos y se acelera la adopción de soluciones SOA.

“Tiempo de ejecución básico de la pasarela de política SOA ” en la página 22
El Tiempo de ejecución básico de la pasarela de política SOA proporciona un modo sencillo de proporcionar un tiempo de ejecución que se puede utilizar de forma autónoma o integrada con un patrón de Maestro de gobierno de pasarela de política SOA desplegado. El patrón Tiempo de ejecución básico de la pasarela de política SOA da soporte al despliegue de un dominio de DataPower que se ha configurado para comunicarse con el servidor de tiempo de ejecución de WSRR suministrado en el patrón.

“Ejemplo del tiempo de ejecución básico de la pasarela de política SOA” en la página 18
El Ejemplo del tiempo de ejecución básico de la pasarela de política SOA suministra un Tiempo de ejecución básico de la pasarela de política SOA con una interfaz y aplicación de ejemplo que muestra las políticas soportadas actualmente en este release.

“Maestro de gobierno de pasarela de política SOA” en la página 20
El patrón Maestro de gobierno de pasarela de política SOA 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.

“Tiempo de ejecución avanzado de pasarela de política SOA” en la página 24
El patrón Tiempo de ejecución avanzado de pasarela de política SOA incluye más opciones de alta disponibilidad y se debe utilizar con el patrón Maestro de gobierno de pasarela de política SOA.

Capítulo 3. Iniciación al patrón de pasarela de política SOA de IBM

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 comprender lo que se describe en este escenario, las razones por las que una empresa puede desear seguir el escenario, los roles de usuario implicados y una visión general de las posibilidades que se entregan con el producto.

Antes de empezar

Puede utilizar el patrón de pasarela de política SOA de IBM de IBM en IBM PureApplication System o en el dispositivo IBM Workload Deployer.

Procedimiento

Para utilizar el patrón de pasarela de política SOA de IBM, realice los siguientes pasos:

1. Descargue e instale el patrón de pasarela de política SOA de IBM. Para obtener más información acerca de cómo descargar los paquetes desde Passport Advantage, consulte “Cómo descargar e instalar los patrones” en la página 12.
2. Opcional: Configure el acceso de usuario. Para obtener más información, consulte “Configuración del acceso de usuario” en la página 14.
3. Configure y despliegue el patrón.
   a. Acepte las licencias de la imagen del sistema virtual importadas para WSRR.
   b. Acepte todos los acuerdos de licencia en DB2 Enterprise.
   c. Despliegue el patrón:
      1) Determine la topología de despliegue. Para obtener más información, consulte Information Center de IBM WebSphere Service Registry and Repository, Versión 8.0 - Despliegue de topologías.
      2) Si utiliza una topología de despliegue autónomo, despliegue un solo patrón de tiempo de ejecución básico sin ninguna promoción configurada.
      3) Por otras topologías, primero despliegue el patrón del maestro de gobierno de la pasarela de política SOA. Esto proporciona un entorno de gobierno para servicios y políticas.
      4) Una vez desplegado correctamente el patrón de Maestro de gobierno, seleccione el tipo de entorno de ejecución que necesita. En un entorno de prueba o de transacción un tiempo de ejecución básico suele ser suficiente. En un entorno de producción, seleccione el entorno de tiempo de ejecución avanzado. Los tiempos de ejecución se pueden registrar en la configuración de promoción del perfil de habilitación de gobierno para el Maestro de gobierno. Las opciones de promoción incluyen producción, transición, o ninguna promoción para la configuración de promoción manual.

      Para obtener más información, consulte “Despliegue de patrones” en la página 72.

d. Verifique que el despliegue. Consulte el apartado “Verificación del despliegue” en la página 78.
e. Proteja el entorno WSRR. Para obtener más información sobre la planificación y configuración de la seguridad de WSRR, consulte el Information Center de IBM WebSphere Service Registry and Repository Versión 8.0.
f. Configure el dominio de DataPower suministrado. Para obtener más información, consulte “Gestión de la seguridad” en la página 64.

4. Utilice la instancia desplegada. Para obtener más información, consulte Capítulo 6, “Cómo trabajar con la instancia desplegada”, en la página 103.

Cómo descargar e instalar los patrones

El patrón de pasarela de política SOA de IBM para utilizar con IBM Workload Deployer Version 3.1.0.2 o IBM PureApplication System está empaquetado para su descarga desde Passport Advantage.

Antes de empezar

Son necesarios 10 GB de espacio disponible para el archivo `CI9G9ML.gz` y de 10 a 14 GB adicionales para los archivos extraídos.

El archivo `CI9G9ML.gz` se debe descargar en un sistema donde se ejecuta Linux o Microsoft Windows. Java™ Runtime Environment (JRE) Versión 6 también debe estar instalado antes de iniciar la instalación del patrón. Puede descargar esta versión para Linux desde la dirección siguiente: http://www.ibm.com/developerworks/java/jdk/linux/download.html.

Acerca de esta tarea

El patrón de pasarela de política SOA de IBM está empaquetado en el archivo `CI9G9ML.tar.gz`. Este archivo contiene los archivos OVA (Open Virtual Archive), los archivos de paquetes de scripts y los archivos de definiciones de patrones.

Procedimiento

Para descargar las imágenes del patrón de pasarela de política SOA de IBM 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 archivo se denomina `CI9G9ML.tar.gz`.
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 `CI9G9ML.tar.gz`.
4. Extraiga el contenido del archivo `CI9G9ML.tar.gz` en el sistema de archivos local. En Linux, el mandato de extracción es el siguiente: En Linux, el mandato de extracción es el siguiente:

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

   En Windows, utilice software de extracción para extraer el contenido de `CI9G9ML.tar.gz`.
5. Asegúrese de que los siguientes archivos extraídos tienen permiso de ejecución en los sistemas Linux:

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

6. Vaya al directorio `instalación`:
   ```
   cd installer
   ```
7. Para instalar el patrón de pasarela de política SOA de IBM en el dispositivo de nube, ejecute el instalador. El nombre del mandato es `installer.bat` en Microsoft Windows o `installer` en Linux. Escriba el mandato siguiente: `instalador -h <host> -u <nombreusuario> -p <contraseña>`, donde `<host>` es el dispositivo de nube, y el nombre de usuario y la contraseña son las credenciales del administrador de la nube. Por ejemplo:
   ```
   ./installer -h apiliwd.rchland.ibm.com -u cbadmin -p cbadmin
   ```
8. Cuando se le solicite, acepte la licencia del patrón de pasarela de política SOA de IBM.
   a. En Microsoft Windows: después de aceptar el acuerdo de licencia, si una línea nueva en la terminal muestra `>>>`, escriba `quit()` y pulse la tecla Intro. Repita el paso 7.
9. 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 2.0.0.0 - Governance Master" ...
   Import pattern "SOA Policy Gateway 2.0.0.0 - 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 de pasarela de política SOA de IBM ya existe en el catálogo, no se sobrescribirá.

Qué hacer a continuación

Acepte las licencias en el dispositivo IBM Workload Deployer o en IBM PureApplication System.

Para validar la instalación, consulte “Verifique el patrón instalado”.

Verifique el patrón instalado

Puede verificar que el patrón se ha instalado correctamente, y aceptar las licencias necesarias para utilizar el patrón.

Antes de empezar

Asegúrese de que todos los pasos de “Cómo descargar e instalar los patrones” en la página 12 se hayan completado.

Acerca de esta tarea

Después de instalar el patrón, puede verificar la instalación del patrón. Para poder utilizar una imagen virtual cualquiera, debe aceptar la licencia necesaria correspondiente a ella.

Procedimiento

Para verificar la instalación del patrón de pasarela de política SOA de IBM, realice los pasos siguientes :

1. Inicie la sesión en la consola IPAS o en la consola IWD del sistema principal donde se ha instalado el patrón.
2. Verifique las imágenes virtuales navegando a `Catálogo -> Imágenes virtuales` y localice: DB2 9.7.5.0 y WebSphere Service Registry and Repository 8.0.0.1. Si no se acepta una licencia, el icono de imagen contendrá un recuadro rojo con una cruz.
   a. Para aceptar una licencia, pulse la imagen para ver sus detalles. El estado actual se visualizará. 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 actual mostrará Sólo lectura y el acuerdo de licencia aparecerá como Aceptado cuando haya terminado.
3. `Vaya a Catálogo -> Paquetes de scripts` y busque:
   - SOA Policy Gateway 2.0.0.0 - Dominio DataPower
   - SOA Policy Gateway 2.0.0.0 - Promoción
   - SOA Policy Gateway 2.0.0.0 - Ejemplo
   - SOA Policy Gateway 2.0.0.0 - Seguridad

   Estos paquetes de scripts están todos incluidos en una instalación realizada correctamente.
4. `Vaya a Patrón -> Sistemas virtuales` y busque:
   - SOA Policy Gateway 2.0.0.0 - Tiempo de ejecución avanzado
   - SOA Policy Gateway 2.0.0.0 - Tiempo de ejecución básico
   - SOA Policy Gateway 2.0.0.0 - Ejemplo de tiempo de ejecución básico
   - SOA Policy Gateway 2.0.0.0 - Maestro de gobierno

   Estos patrones están todos incluidos en una instalación realizada correctamente.

Resultados

Ha verificado la instalación del patrón de pasarela de política SOA de IBM.

Qué hacer a continuación

Si la instalación se ha realizado satisfactoriamente, puede continuar en Capítulo 5, “Trabajar con el patrón de pasarela de política SOA de IBM”, en la página 61. 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 12.

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.

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 interfaz.
     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. En el menú, pulse **Catálogo** > **Imágenes virtuales** para abrir la ventana Imágenes virtuales. Seleccione una imagen virtual del patrón de pasarela de política SOA de IBM de imagen situada en el panel izquierdo y, a continuación, añada los usuarios o el grupo en el panel derecho.

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

IBM Workload Deployer: Gestión de usuarios y grupos

Capítulo 4. Patrones, componentes y paquetes script

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

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.

Componentes

Los componentes describen los componentes que están configurados en una máquina virtual. Cada componente tiene un conjunto de propiedades (parámetros) que se utilizan durante el despliegue para ayudar a definir una configuración global del sistema virtual. Cuando se cargan las imágenes del patrón de pasarela de política SOA de IBM en IBM Workload Deployer, los componentes están incluidos.

Patrones

El patrón patrón de pasarela de política SOA de IBM contiene cuatro patrones:

- Tiempo de ejecución básico de la pasarela de política SOA
- Ejemplo del tiempo de ejecución básico de la pasarela de política SOA
- Tiempo de ejecución avanzado de pasarela de política SOA
- Maestro de gobierno de pasarela de política SOA

Para obtener información detallada acerca de cómo utilizar IBM Workload Deployer para acceder a los patrones existentes o para crear un patrón personalizado, consulte http://publib.boulder.ibm.com/infocenter/worlodep/v3r0m0/topic/com.ibm.worlodep.doc/welcome.html.

Patrones

Una vez cargadas las imágenes virtuales en IBM Workload Deployer o IBM PureApplication System y después de que se haya asignado el acceso correcto a los usuarios, éstos podrán comenzar a trabajar con los patrones de las imágenes.

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.

Tiempo de ejecución básico de la pasarela de política SOA

El Tiempo de ejecución básico de la pasarela de política SOA contiene los siguientes componentes necesarios:

- DB2 Enterprise
- Servidor WSRR autónomo

Ejemplo del tiempo de ejecución básico de la pasarela de política SOA

El Ejemplo del tiempo de ejecución básico de la pasarela de política SOA contiene los siguientes componentes necesarios:

- DB2 Enterprise
- Servidor WSRR autónomo

Tiempo de ejecución avanzado de pasarela de política SOA

El Tiempo de ejecución avanzado de pasarela de política SOA contiene los siguientes componentes necesarios:

- Gestor de despliegue de WSRR
- DB2 Enterprise HADR Primary
- DB2 Enterprise HADR Standby
- Nodo personalizado WSRR

Maestro de gobierno de pasarela de política SOA

El Maestro de gobierno de pasarela de política SOA contiene los siguientes componentes necesarios:

- Gestor de despliegue de WSRR
- DB2 Enterprise HADR Primary
- DB2 Enterprise HADR Standby
- Nodo personalizado WSRR

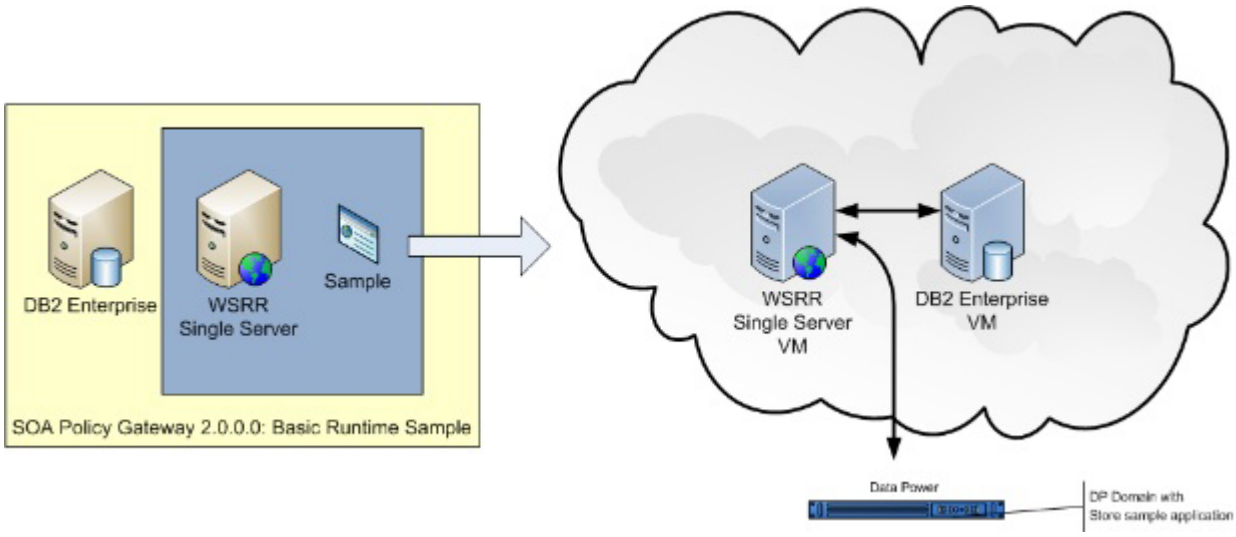
Ejemplo del tiempo de ejecución básico de la pasarela de política SOA

El Ejemplo del tiempo de ejecución básico de la pasarela de política SOA suministra un Tiempo de ejecución básico de la pasarela de política SOA con una interfaz y aplicación de ejemplo que muestra las políticas soportadas actualmente en este release.

El patrón Ejemplo del tiempo de ejecución básico de la pasarela de política SOA requiere los siguientes componentes:

- Servidor WSRR autónomo
- DB2 Enterprise

El patrón Ejemplo del tiempo de ejecución básico de la pasarela de política SOA instala una aplicación de ejemplo en el entorno desplegado. El patrón instala el dominio de ejemplo en DataPower que implementa un servicio simple, 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 81. Instala el dominio de ejemplo dentro de DataPower, instala el WSDL de ejemplo y las Políticas en WSRR y muestra varias políticas para un servicio.



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 las partes del mensaje de respuesta basado en XACML. El XACML no se almacena en WSRR.

Scripts y opciones avanzadas

El patrón Tiempo de ejecución básico de la pasarela de política SOA requiere los siguientes scripts.

En el componente Servidor autónomo de WSRR:

- SOA Policy Gateway 2.0.0.0 - Ejemplo

Consulte los parámetros de componentes y scripts:

- "Parámetros de configuración del componente DB2 Enterprise para el patrón Ejemplo del tiempo de ejecución básico de la pasarela de política SOA" en la página 29
- "Parámetros de configuración del componente Servidor WSRR autónomo para el patrón Ejemplo del tiempo de ejecución básico de la pasarela de política SOA" en la página 41
- "SOA Policy Gateway 2.0.0.0 - Parámetros de configuración del script de ejemplo para el patrón Ejemplo del tiempo de ejecución básico de la pasarela de política SOA" en la página 53

Conceptos relacionados:

"Componente DB2 Enterprise" en la página 27
El componente DB2 Enterprise proporciona algunas opciones de configuración.

"Componente Servidor WSRR autónomo" en la página 38
El componente Servidor WSRR autónomo proporciona algunas opciones de configuración.

"Script: SOA Policy Gateway 2.0.0.0 - Ejemplo" en la página 52
El script Ejemplo configura los parámetros de la aplicación de ejemplo que se utilizarán con el patrón Ejemplo del tiempo de ejecución básico de la pasarela de política SOA.

"La aplicación de ejemplo" en la página 81
La aplicación de ejemplo es un dominio DataPower configurable y un conjunto de artefactos WSRR que se pueden utilizar para demostrar las posibilidades del patrón.

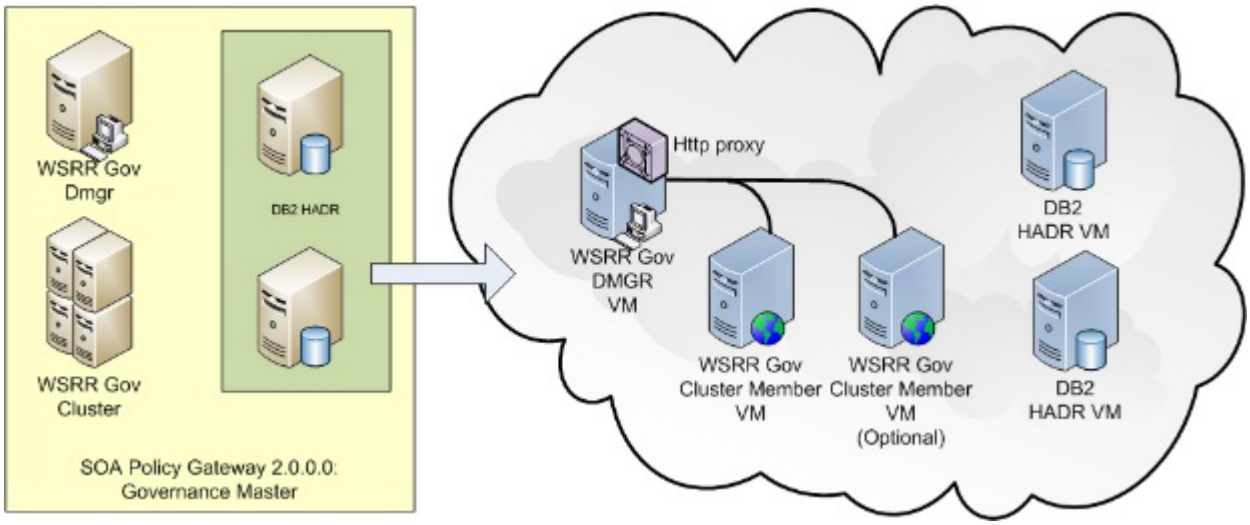
Maestro de gobierno de pasarela de política SOA

El patrón Maestro de gobierno de pasarela de política SOA 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 Maestro de gobierno de pasarela de política SOA 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 utilizados para configurar el patrón Maestro de gobierno son utilizados por los patrones de tiempo de ejecución para configurarse en el Maestro de gobierno. Solamente el patrón Tiempo de ejecución básico de la pasarela de política SOA o Tiempo de ejecución avanzado de pasarela de política SOA se puede configurar en el Maestro de gobierno.



Scripts y opciones avanzadas

El patrón Maestro de gobierno de pasarela de política SOA requiere los scripts siguientes:

- SOA Policy Gateway 2.0.0.0 - Seguridad
- SOA Policy Gateway 2.0.0.0 - Promoción
- SOA Policy Gateway 2.0.0.0 - Dominio DataPower

Consulte los parámetros de componentes y scripts:

- "Parámetros de configuración del componente DB2 Enterprise HADR Primary para el patrón Maestro de gobierno de pasarela de política SOA" en la página 33
- "Parámetros de configuración del componente DB2 Enterprise HADR Standby para el patrón Maestro de gobierno de pasarela de política SOA" en la página 37
- "Parámetros de configuración del componente Gestor de despliegue de WSRR para el patrón Maestro de gobierno de pasarela de política SOA" en la página 43
- "Parámetros de configuración del componente Nodos personalizados de WSRR para el patrón Maestro de gobierno de pasarela de política SOA" en la página 46

Utilizando el patrón de gobierno como un maestro de gobierno

El patrón Maestro de gobierno de pasarela de política SOA 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 Tiempo de ejecución básico de la pasarela de política SOA y Tiempo de ejecución avanzado de pasarela de política SOA se pueden desplegar en esta integración como destinos de promoción. Para obtener más información sobre cómo configurarlo, consulte "Caso de ejemplo: añadir un tiempo de ejecución adicional al patrón" en la página 78.

Conceptos relacionados:

"Componente DB2 Enterprise HADR Primary" en la página 31
El componente DB2 Enterprise HADR Primary proporciona algunas opciones de configuración.

"Componente DB2 Enterprise HADR Standby" en la página 34
El componente DB2 Enterprise HADR Standby proporciona algunas opciones de configuración.

"Componenente Gestor de despliegue de WSRR" en la página 42
Componente Gestor de despliegue de WSRR proporciona algunas opciones de configuración.

"Componente Nodos personalizados de WSRR" en la página 44
El componente Nodos personalizados de WSRR proporciona algunas opciones de configuración.

Información relacionada:

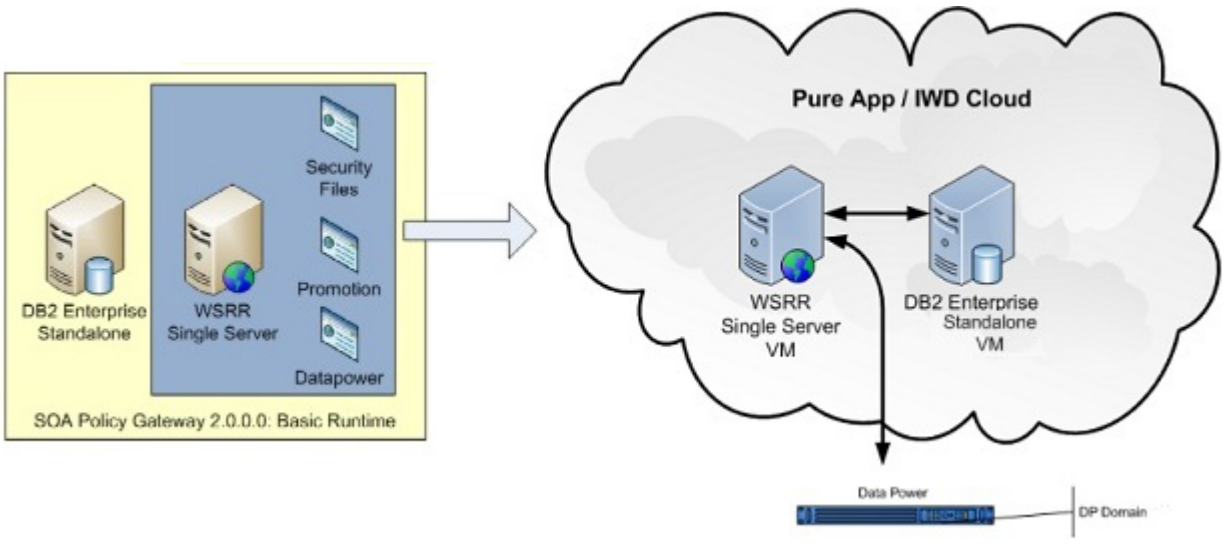
Information Center de IBM WebSphere Service Registry and Repository, Versión 8.0 - Perfil de habilitación de gobierno

Tiempo de ejecución básico de la pasarela de política SOA

El Tiempo de ejecución básico de la pasarela de política SOA proporciona un modo sencillo de proporcionar un tiempo de ejecución que se puede utilizar de forma autónoma o integrada con un patrón de Maestro de gobierno de pasarela de política SOA desplegado. El patrón Tiempo de ejecución básico de la pasarela de política SOA da soporte al despliegue de un dominio de DataPower que se ha configurado para comunicarse con el servidor de tiempo de ejecución de WSRR suministrado en el patrón.

El patrón Tiempo de ejecución básico de la pasarela de política SOA requiere los siguientes componentes:

- Servidor WSRR autónomo
- DB2 Enterprise



Scripts y opciones avanzadas

El patrón Tiempo de ejecución básico de la pasarela de política SOA requiere los siguientes scripts.

En el componente Servidor autónomo de WSRR:

- SOA Policy Gateway 2.0.0.0 - Seguridad
- SOA Policy Gateway 2.0.0.0 - Promoción
- SOA Policy Gateway 2.0.0.0 - Dominio DataPower

Consulte los parámetros de componentes y scripts:

- “Parámetros de configuración del componente del Servidor WSRR autónomo para el patrón Tiempo de ejecución básico de la pasarela de política SOA ” en la página 39
- “Parámetros de configuración del componente DB2 Enterprise para el patrón Tiempo de ejecución básico de la pasarela de política SOA ” en la página 28
- “SOA Policy Gateway 2.0.0.0 - Parámetros de configuración del script de seguridad para el patrón Tiempo de ejecución básico de la pasarela de política SOA ” en la página 57
- “SOA Policy Gateway 2.0.0.0 - Parámetros de configuración del script de promoción para el patrón Tiempo de ejecución básico de la pasarela de política SOA ” en la página 50
- “SOA Policy Gateway 2.0.0.0 - Parámetros de configuración del script del Dominio de DataPowern para el patrón Tiempo de ejecución básico de la pasarela de política SOA ” en la página 48

Promoción del Tiempo de ejecución básico de la pasarela de política SOA en un Tiempo de ejecución de gobierno

Cuando se configura un patrón de Tiempo de ejecución básico 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 básico.

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

- producción
- transición
- otros o Sin definir

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.

Conceptos relacionados:

"La aplicación de ejemplo" en la página 81
La aplicación de ejemplo es un dominio DataPower configurable y un conjunto de artefactos WSRR que se pueden utilizar para demostrar las posibilidades del patrón.

"Componente DB2 Enterprise" en la página 27
El componente DB2 Enterprise proporciona algunas opciones de configuración.

"Componente Servidor WSRR autónomo" en la página 38
El componente Servidor WSRR autónomo proporciona algunas opciones de configuración.

"Script: SOA Policy Gateway 2.0.0.0 - Seguridad" en la página 56
El script Seguridad copia la información de seguridad contenida en un archivo ZIP, que es necesaria para comunicarse con un dispositivo DataPower en el gestor de despliegue o en la máquina WSRR desde un servidor de archivos externo que dé soporte al programa de copia segura (SCP) de Linux.

"Script: SOA Policy Gateway 2.0.0.0 - Promoción" en la página 50
El script de Promoción permite integrar el patrón Tiempo de ejecución básico de la pasarela de política SOA o el patrónTiempo de ejecución avanzado de pasarela de política SOA con un patrón Maestro de gobierno de pasarela de política SOA 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.

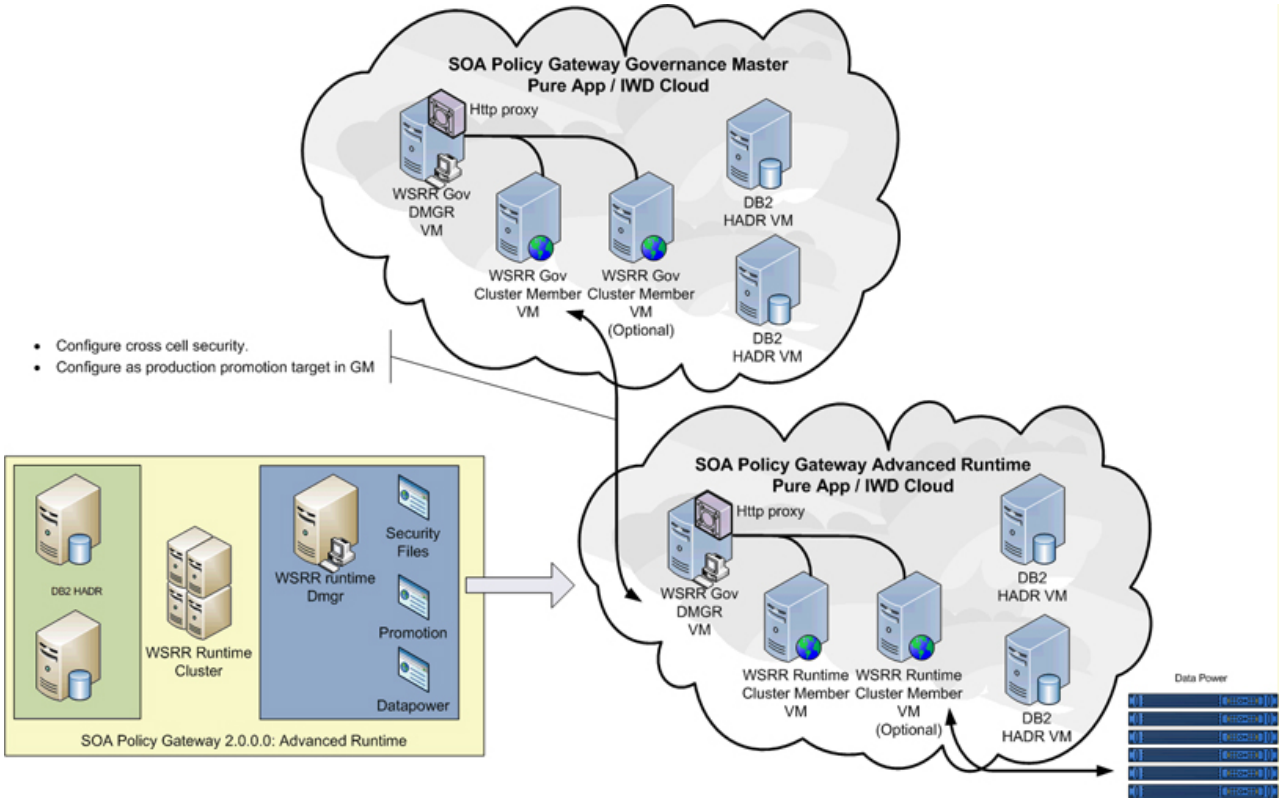
"Script: SOA Policy Gateway 2.0.0.0 - Dominio DataPower" en la página 47
El script del dominio DataPower suministra el dominio DataPower durante el despliegue. El script configura la conexión entre un único dominio DataPower y el tiempo de ejecución de WSRR. Se requiere un script del dominio DataPower para cada dominio DataPower conectado al tiempo de ejecución WSRR.

Tiempo de ejecución avanzado de pasarela de política SOA

El patrón Tiempo de ejecución avanzado de pasarela de política SOA incluye más opciones de alta disponibilidad y se debe utilizar con el patrón Maestro de gobierno de pasarela de política SOA.

El patrón Tiempo de ejecución avanzado de pasarela de política SOA necesita los componentes siguientes:

- DB2 HADR Primary
- DB2 HADR Standby
- Gestor de despliegue de WSRR
- Nodos personalizados de WSRR



Scripts y opciones avanzadas

El patrón Maestro de gobierno de pasarela de política SOA necesita los scripts siguientes en el gestor de despliegue de WSRR:

- SOA Policy Gateway 2.0.0.0 - Seguridad
- SOA Policy Gateway 2.0.0.0 - Promoción
- SOA Policy Gateway 2.0.0.0 - Dominio de DataPower (uno por dominio de DataPower)

Consulte los parámetros de componentes y scripts:

- “Parámetros de configuración del componente DB2 Enterprise HADR Primary para el patrón Tiempo de ejecución avanzado de pasarela de política SOA” en la página 32
- “Parámetros de configuración del componente DB2 Enterprise HADR Standby para el patrón Tiempo de ejecución avanzado de pasarela de política SOA” en la página 35
- “Parámetros de configuración del componente Gestor de despliegue de WSRR para el patrón Tiempo de ejecución avanzado de pasarela de política SOA” en la página 43
- “Parámetros de configuración del componente Nodos personalizados de WSRR para el patrón Tiempo de ejecución avanzado de pasarela de política SOA” en la página 45
- “SOA Policy Gateway 2.0.0.0 - Parámetros de configuración del script de seguridad para el patrón Tiempo de ejecución avanzado de pasarela de política SOA” en la página 58

- "SOA Policy Gateway 2.0.0.0 - Parámetros de configuración del script de promoción para el patrón Tiempo de ejecución avanzado de pasarela de política SOA" en la página 51
- "SOA Policy Gateway 2.0.0.0 - Parámetros de configuración del script del Dominio de DataPower para el patrón Tiempo de ejecución avanzado de pasarela de política SOA" en la página 49

Promoción del Tiempo de ejecución avanzado de pasarela de política SOA en un Tiempo de ejecución 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
- otro o "Sin definir"

Estas opciones se corresponden con los niveles proporcionados por el perfil de habilitación de gobierno en WSRR. Si se ha alterado el perfil de gobierno del maestro de gobierno, utilice "otro" como nivel de promoción. 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.

Conceptos relacionados:

"Componente DB2 Enterprise HADR Primary" en la página 31
El componente DB2 Enterprise HADR Primary proporciona algunas opciones de configuración.

"Componente DB2 Enterprise HADR Standby" en la página 34
El componente DB2 Enterprise HADR Standby proporciona algunas opciones de configuración.

"Componenente Gestor de despliegue de WSRR" en la página 42
Componente Gestor de despliegue de WSRR proporciona algunas opciones de configuración.

"Componente Nodos personalizados de WSRR" en la página 44
El componente Nodos personalizados de WSRR proporciona algunas opciones de configuración.

"Script: SOA Policy Gateway 2.0.0.0 - Seguridad" en la página 56
El script Seguridad copia la información de seguridad contenida en un archivo ZIP, que es necesaria para comunicarse con un dispositivo DataPower en el gestor de despliegue o en la máquina WSRR desde un servidor de archivos externo que dé soporte al programa de copia segura (SCP) de Linux.

"Script: SOA Policy Gateway 2.0.0.0 - Promoción" en la página 50
El script de Promoción permite integrar el patrón Tiempo de ejecución básico de la pasarela de política SOA o el patrónTiempo de ejecución avanzado de pasarela de política SOA con un patrón Maestro de gobierno de pasarela de política SOA 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.

"Script: SOA Policy Gateway 2.0.0.0 - Dominio DataPower" en la página 47
El script del dominio DataPower suministra el dominio DataPower durante el despliegue. El script configura la conexión entre un único dominio DataPower y el tiempo de ejecución de WSRR. Se requiere un script del dominio DataPower para cada dominio DataPower conectado al tiempo de ejecución WSRR.

Componentes

El patrón de pasarela de política SOA de IBM 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 9.7.5 se describen en la tabla siguiente:

Tabla 2. Parámetros configurables

Nombre del parámetro	Descripción
CPU virtuales	El número de procesadores virtuales asignado a la máquina virtual representada por este componente.
Tamaño de la memoria (MB)	La cantidad de memoria asignada a esta máquina virtual, en megabytes.
Contraseña (db2inst1)	La contraseña para el ID de usuario db2inst1 del sistema operativo. 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.
Verificar contraseña	Verifica la contraseña db2inst1.

Tabla 2. Parámetros configurables (continuación)

Nombre del parámetro	Descripción
Contraseña (db2fenc1)	Contraseña del ID de usuario utilizada para ejecutar funciones definidas por el usuario (UDF) y procedimientos almacenados fuera del panel del espacio de dirección utilizado por la base de datos DB2. El usuario delimitado es un usuario bajo el que se pueden ejecutar algunos procedimientos almacenados (procedimientos almacenados "delimitados") con una autorización reducida en el sistema operativo. Esto puede ayudarle a evitar que procedimientos almacenados delimitados sobrescriban archivos de instancia porque el sistema operativo lo impedirá.
Verificar contraseña	Verifica la contraseña db2fenc1.
Contraseña (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. El usuario predeterminado es dasusr1 y el grupo predeterminado es dasadm1. 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.
Verificar contraseña	Verifica la contraseña dasusr1.
Contraseña (root)	La contraseña para el ID de usuario root. Es la contraseña del sistema operativo de la máquina virtual representada por este componente 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.

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

Parámetros de configuración del componente DB2 Enterprise para el patrón Tiempo de ejecución básico de la pasarela de política SOA

Antes de desplegar el patrón, se deben configurar los parámetros necesarios sin un valor predeterminado.

Tabla 3. Parámetros configurables

Nombre del parámetro	Necesario	Valor predeterminado	Descripción
CPU virtuales	Sí	1	El número de procesadores virtuales asignado a la máquina virtual representada por este componente.
Tamaño de la memoria (MB)	Sí	2048	La cantidad de memoria asignada a esta máquina virtual, en megabytes.
Contraseña (db2inst1)	Sí		La contraseña para el ID de usuario db2inst1 del sistema operativo. 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.
Verificar contraseña	Sí		Verifica la contraseña db2inst1.

Tabla 3. Parámetros configurables (continuación)

Nombre del parámetro	Necesario	Valor predeterminado	Descripción
Contraseña (db2fenc1)	Sí		Contraseña del ID de usuario utilizada para ejecutar funciones definidas por el usuario (UDF) y procedimientos almacenados fuera del panel del espacio de dirección utilizado por la base de datos DB2. El usuario delimitado es un usuario bajo el que se pueden ejecutar algunos procedimientos almacenados (procedimientos almacenados "delimitados") con una autorización reducida en el sistema operativo. Esto puede ayudarle a evitar que procedimientos almacenados delimitados sobrescriban archivos de instancia porque el sistema operativo lo impedirá.
Verificar contraseña	Sí		Verifica la contraseña db2fenc1.
Contraseña (dasusr1)	Sí		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. El usuario predeterminado es dasusr1 y el grupo predeterminado es dasadm1. 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.
Verificar contraseña	Sí		Verifica la contraseña dasusr1.
Contraseña (root)	Sí		La contraseña para el ID de usuario root. Es la contraseña del sistema operativo de la máquina virtual representada por este componente en el patrón.
Verificar contraseña	Sí		Verifica la contraseña root.
Contraseña (virtuser)	Sí		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	Sí		Verifica la contraseña virtuser.

Parámetros de configuración del componente DB2 Enterprise para el patrón Ejemplo del tiempo de ejecución básico de la pasarela de política SOA

En el Ejemplo del tiempo de ejecución básico de la pasarela de política SOA, los valores predeterminados están preconfigurados para todos los parámetros.

Tabla 4. Parámetros configurados

Nombre del parámetro	Necesario	Valor predeterminado	Descripción
CPU virtuales	Sí	1	El número de procesadores virtuales asignado a la máquina virtual representada por este componente.
Tamaño de la memoria (MB)	Sí	2048	La cantidad de memoria asignada a esta máquina virtual, en megabytes.
Contraseña (db2inst1)	Sí	contraseña	La contraseña para el ID de usuario db2inst1 del sistema operativo. 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.
Verificar contraseña	Sí	contraseña	Verifica la contraseña db2inst1.
Contraseña (db2fenc1)	Sí	contraseña	Contraseña del ID de usuario utilizada para ejecutar funciones definidas por el usuario (UDF) y procedimientos almacenados fuera del panel del espacio de dirección utilizado por la base de datos DB2. El usuario delimitado es un usuario bajo el que se pueden ejecutar algunos procedimientos almacenados (procedimientos almacenados "delimitados") con una autorización reducida en el sistema operativo. Esto puede ayudarle a evitar que procedimientos almacenados delimitados sobrescriban archivos de instancia porque el sistema operativo lo impedirá.
Verificar contraseña	Sí	contraseña	Verifica la contraseña db2fenc1.
Contraseña (dasusr1)	Sí	contraseña	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. El usuario predeterminado es dasusr1 y el grupo predeterminado es dasadm1. 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.
Verificar contraseña	Sí	contraseña	Verifica la contraseña dasusr1.

Tabla 4. Parámetros configurados (continuación)

Nombre del parámetro	Necesario	Valor predeterminado	Descripción
Contraseña (root)	Sí	contraseña	La contraseña para el ID de usuario root. Es la contraseña del sistema operativo de la máquina virtual representada por este componente en el patrón.
Verificar contraseña	Sí	contraseña	Verifica la contraseña root.
Contraseña (virtuser)	Sí	contraseña	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	Sí	contraseña	Verifica la contraseña virtuser.

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 5. Parámetros configurables

Nombre del parámetro	Descripción
CPU virtuales	El número de procesadores virtuales asignado a la máquina virtual representada por este componente.
Tamaño de la memoria (MB)	La cantidad de memoria asignada a esta máquina virtual, en megabytes.
Contraseña (db2inst1)	La contraseña para el ID de usuario db2inst1 del sistema operativo. 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.
Verificar contraseña	Verifica la contraseña db2inst1.
Contraseña (db2fenc1)	Contraseña del ID de usuario utilizada para ejecutar funciones definidas por el usuario (UDF) y procedimientos almacenados fuera del panel del espacio de dirección utilizado por la base de datos DB2. El usuario delimitado es un usuario bajo el que se pueden ejecutar algunos procedimientos almacenados (procedimientos almacenados "delimitados") con una autorización reducida en el sistema operativo. Esto puede ayudarle a evitar que procedimientos almacenados delimitados sobrescriban archivos de instancia porque el sistema operativo lo impedirá.
Verificar contraseña	Verifica la contraseña db2fenc1.
Contraseña (dasusr1)	La contraseña del ID de usuario del servidor de administración de DB2 que se utiliza para ejecutar el servidor de administración de DB2 en su sistema. El usuario predeterminado es dasusr1 y el grupo predeterminado es dasadm1. 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.
Verificar contraseña	Verifica la contraseña dasusr1.
Contraseña (root)	La contraseña para el ID de usuario root. Es la contraseña del sistema operativo de la máquina virtual representada por este componente en el patrón.

Tabla 5. Parámetros configurables (continuación)

Nombre del parámetro	Descripción
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.

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

Parámetros de configuración del componente DB2 Enterprise HADR Primary para el patrón Tiempo de ejecución avanzado de pasarela de política SOA

Antes de desplegar el patrón, se deben configurar los parámetros necesarios sin un valor predeterminado.

Tabla 6. Parámetros configurables

Nombre del parámetro	Necesario	Valor predeterminado	Descripción
CPU virtuales	Sí	1	El número de procesadores virtuales asignado a la máquina virtual representada por este componente.
Tamaño de la memoria (MB)	Sí	2048	La cantidad de memoria asignada a esta máquina virtual, en megabytes.
Contraseña (db2inst1)	Sí		La contraseña para el ID de usuario db2inst1 del sistema operativo. 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.
Verificar contraseña	Sí		Verifica la contraseña db2inst1.
Contraseña (db2fenc1)	Sí		Contraseña del ID de usuario utilizada para ejecutar funciones definidas por el usuario (UDF) y procedimientos almacenados fuera del panel del espacio de dirección utilizado por la base de datos DB2. El usuario delimitado es un usuario bajo el que se pueden ejecutar algunos procedimientos almacenados (procedimientos almacenados "delimitados") con una autorización reducida en el sistema operativo. Esto puede ayudarle a evitar que procedimientos almacenados delimitados sobrescriban archivos de instancia porque el sistema operativo lo impedirá.
Verificar contraseña	Sí		Verifica la contraseña db2fenc1.

Tabla 6. Parámetros configurables (continuación)

Nombre del parámetro	Necesario	Valor predeterminado	Descripción
Contraseña (dasusr1)	Sí		La contraseña del ID de usuario del servidor de administración de DB2 que se utiliza para ejecutar el servidor de administración de DB2 en su sistema. El usuario predeterminado es dasusr1 y el grupo predeterminado es dasadm1. 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.
Verificar contraseña	Sí		Verifica la contraseña dasusr1.
Contraseña (root)	Sí		La contraseña para el ID de usuario root. Es la contraseña del sistema operativo de la máquina virtual representada por este componente en el patrón.
Verificar contraseña	Sí		Verifica la contraseña root.
Contraseña (virtuser)	Sí		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	Sí		Verifica la contraseña virtuser.

Parámetros de configuración del componente DB2 Enterprise HADR Primary para el patrón Maestro de gobierno de pasarela de política SOA

Antes de desplegar el patrón, se deben configurar los parámetros necesarios sin un valor predeterminado.

Tabla 7. Parámetros configurables

Nombre del parámetro	Necesario	Valor predeterminado	Descripción
CPU virtuales	Sí	1	El número de procesadores virtuales asignado a la máquina virtual representada por este componente.
Tamaño de la memoria (MB)	Sí	2048	La cantidad de memoria asignada a esta máquina virtual, en megabytes.
Contraseña (db2inst1)	Sí		La contraseña para el ID de usuario db2inst1 del sistema operativo. 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.
Verificar contraseña	Sí		Verifica la contraseña db2inst1.

Tabla 7. Parámetros configurables (continuación)

Nombre del parámetro	Necesario	Valor predeterminado	Descripción
Contraseña (db2fenc1)	Sí		Contraseña del ID de usuario utilizada para ejecutar funciones definidas por el usuario (UDF) y procedimientos almacenados fuera del panel del espacio de dirección utilizado por la base de datos DB2. El usuario delimitado es un usuario bajo el que se pueden ejecutar algunos procedimientos almacenados (procedimientos almacenados "delimitados") con una autorización reducida en el sistema operativo. Esto puede ayudarle a evitar que procedimientos almacenados delimitados sobrescriban archivos de instancia porque el sistema operativo lo impedirá.
Verificar contraseña	Sí		Verifica la contraseña db2fenc1.
Contraseña (dasusr1)	Sí		La contraseña del ID de usuario del servidor de administración de DB2 que se utiliza para ejecutar el servidor de administración de DB2 en su sistema. El usuario predeterminado es dasusr1 y el grupo predeterminado es dasadm1. 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.
Verificar contraseña	Sí		Verifica la contraseña dasusr1.
Contraseña (root)	Sí		La contraseña para el ID de usuario root. Es la contraseña del sistema operativo de la máquina virtual representada por este componente en el patrón.
Verificar contraseña	Sí		Verifica la contraseña root.
Contraseña (virtuser)	Sí		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	Sí		Verifica la contraseña virtuser.

Componente DB2 Enterprise HADR Standby

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

Tabla 8. Parámetros configurables

Nombre del parámetro	Descripción
CPU virtuales	El número de procesadores virtuales asignado a la máquina virtual representada por este componente.
Tamaño de la memoria (MB)	La cantidad de memoria asignada a esta máquina virtual, en megabytes.
Contraseña (db2inst1)	La contraseña para el ID de usuario db2inst1 del sistema operativo. 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.
Verificar contraseña	Verifica la contraseña db2inst1.
Contraseña (db2fenc1)	Contraseña del ID de usuario utilizada para ejecutar funciones definidas por el usuario (UDF) y procedimientos almacenados fuera del panel del espacio de dirección utilizado por la base de datos DB2. El usuario delimitado es un usuario bajo el que se pueden ejecutar algunos procedimientos almacenados (procedimientos almacenados "delimitados") con una autorización reducida en el sistema operativo. Esto puede ayudarle a evitar que procedimientos almacenados delimitados sobrescriban archivos de instancia porque el sistema operativo lo impedirá.
Verificar contraseña	Verifica la contraseña db2fenc1.
Contraseña (dasusr1)	La contraseña del ID de usuario del servidor de administración de DB2 que se utiliza para ejecutar el servidor de administración de DB2 en su sistema. El usuario predeterminado es dasusr1 y el grupo predeterminado es dasadm1. 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.
Verificar contraseña	Verifica la contraseña dasusr1.
Contraseña (root)	La contraseña para el ID de usuario root. Es la contraseña del sistema operativo de la máquina virtual representada por este componente 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.

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

Parámetros de configuración del componente DB2 Enterprise HADR Standby para el patrón Tiempo de ejecución avanzado de pasarela de política SOA

Antes de desplegar el patrón, se deben configurar los parámetros necesarios sin un valor predeterminado.

Tabla 9. Parámetros configurables

Nombre del parámetro	Necesario	Valor predeterminado	Descripción
CPU virtuales	Sí	1	El número de procesadores virtuales asignado a la máquina virtual representada por este componente.

Tabla 9. Parámetros configurables (continuación)

Nombre del parámetro	Necesario	Valor predeterminado	Descripción
Tamaño de la memoria (MB)	Sí	2048	La cantidad de memoria asignada a esta máquina virtual, en megabytes.
Contraseña (db2inst1)	Sí		La contraseña para el ID de usuario db2inst1 del sistema operativo. 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.
Verificar contraseña	Sí		Verifica la contraseña db2inst1.
Contraseña (db2fenc1)	Sí		Contraseña del ID de usuario utilizada para ejecutar funciones definidas por el usuario (UDF) y procedimientos almacenados fuera del panel del espacio de dirección utilizado por la base de datos DB2. El usuario delimitado es un usuario bajo el que se pueden ejecutar algunos procedimientos almacenados (procedimientos almacenados "delimitados") con una autorización reducida en el sistema operativo. Esto puede ayudarle a evitar que procedimientos almacenados delimitados sobrescriban archivos de instancia porque el sistema operativo lo impedirá.
Verificar contraseña	Sí		Verifica la contraseña db2fenc1.
Contraseña (dasusr1)	Sí		La contraseña del ID de usuario del servidor de administración de DB2 que se utiliza para ejecutar el servidor de administración de DB2 en su sistema. El usuario predeterminado es dasusr1 y el grupo predeterminado es dasadm1. 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.
Verificar contraseña	Sí		Verifica la contraseña dasusr1.
Contraseña (root)	Sí		La contraseña para el ID de usuario root. Es la contraseña del sistema operativo de la máquina virtual representada por este componente en el patrón.
Verificar contraseña	Sí		Verifica la contraseña root.

Tabla 9. Parámetros configurables (continuación)

Nombre del parámetro	Necesario	Valor predeterminado	Descripción
Contraseña (virtuser)	Sí		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	Sí		Verifica la contraseña virtuser.

Parámetros de configuración del componente DB2 Enterprise HADR Standby para el patrón Maestro de gobierno de pasarela de política SOA

Antes de desplegar el patrón, se deben configurar los parámetros necesarios sin un valor predeterminado.

Tabla 10. Parámetros configurables

Nombre del parámetro	Necesario	Valor predeterminado	Descripción
CPU virtuales	Sí	1	El número de procesadores virtuales asignado a la máquina virtual representada por este componente.
Tamaño de la memoria (MB)	Sí	2048	La cantidad de memoria asignada a esta máquina virtual, en megabytes.
Contraseña (db2inst1)	Sí		La contraseña para el ID de usuario db2inst1 del sistema operativo. 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.
Verificar contraseña	Sí		Verifica la contraseña db2inst1.
Contraseña (db2fenc1)	Sí		Contraseña del ID de usuario utilizada para ejecutar funciones definidas por el usuario (UDF) y procedimientos almacenados fuera del panel del espacio de dirección utilizado por la base de datos DB2. El usuario delimitado es un usuario bajo el que se pueden ejecutar algunos procedimientos almacenados (procedimientos almacenados "delimitados") con una autorización reducida en el sistema operativo. Esto puede ayudarle a evitar que procedimientos almacenados delimitados sobrescriban archivos de instancia porque el sistema operativo lo impedirá.
Verificar contraseña	Sí		Verifica la contraseña db2fenc1.

Tabla 10. Parámetros configurables (continuación)

Nombre del parámetro	Necesario	Valor predeterminado	Descripción
Contraseña (dasusr1)	Sí		La contraseña del ID de usuario del servidor de administración de DB2 que se utiliza para ejecutar el servidor de administración de DB2 en su sistema. El usuario predeterminado es dasusr1 y el grupo predeterminado es dasadm1. 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.
Verificar contraseña	Sí		Verifica la contraseña dasusr1.
Contraseña (root)	Sí		La contraseña para el ID de usuario root. Es la contraseña del sistema operativo de la máquina virtual representada por este componente en el patrón.
Verificar contraseña	Sí		Verifica la contraseña root.
Contraseña (virtuser)	Sí		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	Sí		Verifica la contraseña virtuser.

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 11. Parámetros configurados

Nombre del parámetro	Descripción
CPU virtuales	El número de procesadores virtuales asignado a la máquina virtual representada por este componente.
Tamaño de la memoria (MB)	La cantidad de memoria asignada a esta máquina virtual, en megabytes.
Contraseña (root)	La contraseña para el ID de usuario root. Es la contraseña del sistema operativo de la máquina virtual representada por este componente en el patrón.
Verificar contraseña	Verifica la entrada de usuario para la Contraseña (root).
Nombre de usuario administrativo de WebSphere	El nombre de usuario del administrador del entorno WebSphere.
Contraseña administrativa de WebSphere	La contraseña de usuario del administrador del entorno WebSphere.

Tabla 11. Parámetros configurados (continuación)

Nombre del parámetro	Descripción
Verificar contraseña	Verifica la entrada de usuario de la contraseña administrativa de WebSphere.
Reservar memoria física	La memoria física reservada para uso exclusivo de esta máquina virtual.

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

Parámetros de configuración del componente del Servidor WSRR autónomo para el patrón Tiempo de ejecución básico de la pasarela de política SOA

Antes de desplegar el patrón, se deben configurar los parámetros necesarios sin un valor predeterminado.

Tabla 12. Parámetros configurables

Nombre del parámetro	Necesario	Valor predeterminado	Descripción
CPU virtuales	Sí	1	El número de procesadores virtuales asignado a la máquina virtual representada por este componente.
Tamaño de la memoria (MB)	Sí	4096	La cantidad de memoria asignada a esta máquina virtual, en megabytes.
Reservar memoria física	Sí	False	La memoria física reservada para uso exclusivo de esta máquina virtual.

Tabla 12. Parámetros configurables (continuación)

Nombre del parámetro	Necesario	Valor predeterminado	Descripción
Nombre de célula	Sí	SOAPolicyBaseCell	Nombre de célula WebSphere en la máquina virtual en el patrón de ejecución básico.
Nombre de nodo	Sí	SOAPolicyBaseNode	Nombre de nodo WebSphere en la máquina virtual en el patrón de ejecución básico.
Contraseña (root)	Sí		La contraseña para el ID de usuario root. Es la contraseña del sistema operativo de la máquina virtual representada por este componente en el patrón.
Verificar contraseña	Sí		Verifica la entrada de usuario para la Contraseña (root).

Tabla 12. Parámetros configurables (continuación)

Nombre del parámetro	Necesario	Valor predeterminado	Descripción
Nombre de usuario administrativo de WebSphere	Sí	virtuser	El nombre de usuario del administrador del entorno WebSphere.
Contraseña administrativa de WebSphere	Sí		La contraseña de usuario del administrador del entorno WebSphere.
Verificar contraseña	Sí		Verifica la entrada de usuario de la contraseña administrativa de WebSphere.

Parámetros de configuración del componente Servidor WSRR autónomo para el patrón Ejemplo del tiempo de ejecución básico de la pasarela de política SOA

En el Ejemplo del tiempo de ejecución básico de la pasarela de política SOA, los valores predeterminados están preconfigurados para todos los parámetros.

Tabla 13. Parámetros configurados

Nombre del parámetro	Necesario	Valor predeterminado	Descripción
CPU virtuales	Sí	1	El número de procesadores virtuales asignado a la máquina virtual representada por este componente.
Tamaño de la memoria (MB)	Sí	4096	La cantidad de memoria asignada a esta máquina virtual, en megabytes.
Reservar memoria física	Sí	False	La memoria física reservada para uso exclusivo de esta máquina virtual.

Tabla 13. Parámetros configurados (continuación)

Nombre del parámetro	Necesario	Valor predeterminado	Descripción
Contraseña (root)	Sí	contraseña	La contraseña para el ID de usuario root. Es la contraseña del sistema operativo de la máquina virtual representada por este componente en el patrón.
Verificar contraseña	Sí	contraseña	Verifica la entrada de usuario para la Contraseña (root).
Nombre de usuario administrativo de WebSphere	Sí	virtuser	El nombre de usuario del administrador del entorno WebSphere.
Contraseña administrativa de WebSphere	Sí	contraseña	La contraseña de usuario del administrador del entorno WebSphere.
Verificar contraseña	Sí	contraseña	Verifica la entrada de usuario de la contraseña administrativa de WebSphere.

Componenente 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 14. Parámetros configurables

Nombre del parámetro	Descripción
CPU virtuales	El número de procesadores virtuales asignado a la máquina virtual representada por este componente.
Tamaño de la memoria (MB)	La cantidad de memoria asignada a esta máquina virtual, en megabytes.
Reservar CPU físicas	Las CPU físicas reservadas para uso exclusivo de esta máquina virtual.
Reservar memoria física	La memoria física reservada para uso exclusivo de esta máquina virtual.
Nombre de célula	El nombre de célula de WebSphere para el patrón Tiempo de ejecución avanzado.
Nombre de nodo	El nombre de nodo del nodo WebSphere que reside en la máquina virtual del Gestor de despliegue del patrón Tiempo de ejecución avanzado.
Contraseña (root)	La contraseña para el ID de usuario root. Es la contraseña del sistema operativo de la máquina virtual representada por este componente en el patrón.
Verificar contraseña	Verifica la entrada de usuario para la Contraseña (root).
Nombre de usuario administrativo de WebSphere	El nombre de usuario del administrador del entorno WebSphere.
Contraseña administrativa de WebSphere	La contraseña de usuario del administrador del entorno WebSphere.
Verificar contraseña	Verifica la entrada de usuario de la contraseña administrativa de WebSphere.

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

Parámetros de configuración del componente Gestor de despliegue de WSRR para el patrón Tiempo de ejecución avanzado de pasarela de política SOA

Antes de desplegar el patrón, se deben configurar los parámetros necesarios sin un valor predeterminado.

Tabla 15. Parámetros configurables

Nombre del parámetro	Necesario	Valor predeterminado	Descripción
CPU virtuales	Sí	1	El número de procesadores virtuales asignado a la máquina virtual representada por este componente.
Tamaño de la memoria (MB)	Sí	2048	La cantidad de memoria asignada a esta máquina virtual, en megabytes.
Reservar CPU físicas	Sí	False	Las CPU físicas reservadas para uso exclusivo de esta máquina virtual.
Reservar memoria física	Sí	False	La memoria física reservada para uso exclusivo de esta máquina virtual.
Nombre de célula	Sí	SOAPolicyAdvancedCell	El nombre de célula de WebSphere para el patrón Tiempo de ejecución avanzado.
Nombre de nodo	Sí	SOAPolicyAdvancedNode	El nombre de nodo del nodo WebSphere que reside en la máquina virtual del Gestor de despliegue del patrón Tiempo de ejecución avanzado.
Contraseña (root)	Sí		La contraseña para el ID de usuario root. Es la contraseña del sistema operativo de la máquina virtual representada por este componente en el patrón.
Verificar contraseña	Sí		Verifica la entrada de usuario para la Contraseña (root).
Nombre de usuario administrativo de WebSphere	Sí	virtuser	El nombre de usuario del administrador del entorno WebSphere.
Contraseña administrativa de WebSphere	Sí		La contraseña de usuario del administrador del entorno WebSphere.
Verificar contraseña	Sí		Verifica la entrada de usuario de la contraseña administrativa de WebSphere.

Parámetros de configuración del componente Gestor de despliegue de WSRR para el patrón Maestro de gobierno de pasarela de política SOA

Antes de desplegar el patrón, se deben configurar los parámetros necesarios sin un valor predeterminado.

Tabla 16. Parámetros configurables

Nombre del parámetro	Necesario	Valor predeterminado	Descripción
CPU virtuales	Sí	1	El número de procesadores virtuales asignado a la máquina virtual representada por este componente.
Tamaño de la memoria (MB)	Sí	2048	La cantidad de memoria asignada a esta máquina virtual, en megabytes.
Reservar CPU físicas	Sí	False	Las CPU físicas reservadas para uso exclusivo de esta máquina virtual.
Reservar memoria física	Sí	False	La memoria física reservada para uso exclusivo de esta máquina virtual.
Nombre de célula	Sí	SOAPolicyGMCell	El nombre de célula de WebSphere para el patrón Tiempo de ejecución avanzado.
Nombre de nodo	Sí	SOAPolicyGMNode	El nombre de nodo del nodo WebSphere que reside en la máquina virtual del Gestor de despliegue del patrón Tiempo de ejecución avanzado.
Contraseña (root)	Sí		La contraseña para el ID de usuario root. Es la contraseña del sistema operativo de la máquina virtual representada por este componente en el patrón.
Verificar contraseña	Sí		Verifica la entrada de usuario para la Contraseña (root).
Nombre de usuario administrativo de WebSphere	Sí	virtuser	El nombre de usuario del administrador del entorno WebSphere.
Contraseña administrativa de WebSphere	Sí		La contraseña de usuario del administrador del entorno WebSphere.
Verificar contraseña	Sí		Verifica la entrada de usuario de la contraseña administrativa de WebSphere.

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 17. Parámetros configurables

Nombre del parámetro	Descripción
CPU virtuales	El número de procesadores virtuales asignado a la máquina virtual representada por este componente.
Tamaño de la memoria (MB)	La cantidad de memoria asignada a esta máquina virtual, en megabytes.
Reservar CPU físicas	Las CPU físicas reservadas para uso exclusivo de esta máquina virtual.
Reservar memoria física	La memoria física reservada para uso exclusivo de esta máquina virtual.
Nombre de célula	Se omite el valor de nombre de célula de la configuración del componente Nodos personalizados. Se utiliza el nombre de célula especificado en la configuración del componente Gestor de despliegue.
Nombre de nodo	El nombre de nodo del nodo WebSphere 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. Es la contraseña del sistema operativo de la máquina virtual representada por este componente en el patrón.
Verificar contraseña	Verifica la entrada de usuario para la Contraseña (root).
Nombre de usuario administrativo de WebSphere	El nombre de usuario del administrador del entorno WebSphere.
Contraseña administrativa de WebSphere	La contraseña de usuario del administrador del entorno WebSphere.
Verificar contraseña	Verifica la entrada de usuario de la contraseña administrativa de WebSphere.

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

Parámetros de configuración del componente Nodos personalizados de WSRR para el patrón Tiempo de ejecución avanzado de pasarela de política SOA

Antes de desplegar el patrón, se deben configurar los parámetros necesarios sin un valor predeterminado.

Tabla 18. Parámetros configurables

Nombre del parámetro	Necesario	Valor predeterminado	Descripción
CPU virtuales	Sí	2	El número de procesadores virtuales asignado a la máquina virtual representada por este componente.
Tamaño de la memoria (MB)	Sí	4096	La cantidad de memoria asignada a esta máquina virtual, en megabytes.
Reservar CPU físicas	Sí	False	Las CPU físicas reservadas para uso exclusivo de esta máquina virtual.
Reservar memoria física	Sí	False	La memoria física reservada para uso exclusivo de esta máquina virtual.

Tabla 18. Parámetros configurables (continuación)

Nombre del parámetro	Necesario	Valor predeterminado	Descripción
Nombre de nodo	Sí	SOAPolicyAdvancedNode	El nombre de nodo del nodo WebSphere que reside en la máquina virtual del nodo personalizado del patrón Tiempo de ejecución avanzado.
Contraseña (root)	Sí		La contraseña para el ID de usuario root. Es la contraseña del sistema operativo de la máquina virtual representada por este componente en el patrón.
Verificar contraseña	Sí		Verifica la entrada de usuario para la Contraseña (root).
Nombre de usuario administrativo de WebSphere	Sí	virtuser	El nombre de usuario del administrador del entorno WebSphere.
Contraseña administrativa de WebSphere	Sí		La contraseña de usuario del administrador del entorno WebSphere.
Verificar contraseña	Sí		Verifica la entrada de usuario de la contraseña administrativa de WebSphere.

Parámetros de configuración del componente Nodos personalizados de WSRR para el patrón Maestro de gobierno de pasarela de política SOA

Antes de desplegar el patrón, se deben configurar los parámetros necesarios sin un valor predeterminado.

Tabla 19. Parámetros configurables

Nombre del parámetro	Necesario	Valor predeterminado	Descripción
CPU virtuales	Sí	2	El número de procesadores virtuales asignado a la máquina virtual representada por este componente.
Tamaño de la memoria (MB)	Sí	4096	La cantidad de memoria asignada a esta máquina virtual, en megabytes.
Reservar CPU físicas	Sí	False	Las CPU físicas reservadas para uso exclusivo de esta máquina virtual.
Reservar memoria física	Sí	False	La memoria física reservada para uso exclusivo de esta máquina virtual.
Nombre de nodo	Sí	SOAPolicyGMNode	El nombre de nodo del nodo WebSphere que reside en la máquina virtual del nodo personalizado del patrón Tiempo de ejecución avanzado.

Tabla 19. Parámetros configurables (continuación)

Nombre del parámetro	Necesario	Valor predeterminado	Descripción
Contraseña (root)	Sí		La contraseña para el ID de usuario root. Es la contraseña del sistema operativo de la máquina virtual representada por este componente en el patrón.
Verificar contraseña	Sí		Verifica la entrada de usuario para la Contraseña (root).
Nombre de usuario administrativo de WebSphere	Sí	virtuser	El nombre de usuario del administrador del entorno WebSphere.
Contraseña administrativa de WebSphere	Sí		La contraseña de usuario del administrador del entorno WebSphere.
Verificar contraseña	Sí		Verifica la entrada de usuario de la contraseña administrativa de WebSphere.

Paquetes de scripts

Existen 4 paquetes de scripts que se proporcionan con el patrón de pasarela de política SOA de IBM.

Los paquetes de script que se incluyen con este patrón son los siguientes:

- SOA Policy Gateway 2.0.0.0 - Dominio DataPower
- SOA Policy Gateway 2.0.0.0 - Promoción
- SOA Policy Gateway 2.0.0.0 - Ejemplos
- SOA Policy Gateway 2.0.0.0 - Seguridad

Script: SOA Policy Gateway 2.0.0.0 - Dominio DataPower

El script del dominio DataPower suministra el dominio DataPower durante el despliegue. El script configura la conexión entre un único dominio DataPower y el tiempo de ejecución de WSRR. Se requiere un script del dominio DataPower para cada dominio DataPower conectado al tiempo de ejecución WSRR.

Parámetros

Tabla 20. Parámetros configurables

Nombre del parámetro	Descripción
DataPower_hostname	El nombre de host del dispositivo DataPower en el que se instalará la aplicación de ejemplo.
DataPower_XML_mgmt_port	El puerto utilizado para la interfaz de gestión XML de DataPower, generalmente es 5550.
Datapower_admin_id	El ID del usuario administrativo con los permisos adecuados para utilizar la interfaz de gestión XML.
DataPower_admin_password	La contraseña de DataPower_admin_id.
Verificar contraseña	Verifica la entrada de usuario de DataPower_admin_password.

Tabla 20. Parámetros configurables (continuación)

Nombre del parámetro	Descripción
New_DataPower_domain	El nuevo nombre de dominio que se debe crear en el dispositivo DataPower. No debe coincidir con ningún dominio existente, de lo contrario, el paquete script fallará o concluirá su ejecución. El valor no puede contener espacios.
securityFileCleanUp	Determina si el archivo `DomainZipFile.zip` y el certificado WSRR que se ha cargado en DataPower se suprimen de la instancia de WSRR donde se ejecutan los paquetes script. Si este archivo no se elimina, será un riesgo de seguridad si los certificados permanecieran en la instancia.

SOA Policy Gateway 2.0.0.0 - Parámetros de configuración del script del Dominio de DataPowern para el patrón Tiempo de ejecución básico de la pasarela de política SOA

Antes de desplegar el patrón, se deben configurar los parámetros necesarios sin un valor predeterminado.

Tabla 21. Parámetros configurables

Nombre del parámetro	Necesario	Valor predeterminado	Descripción
DataPower_hostname	Sí		El nombre de host del dispositivo DataPower en el que se instalará la aplicación de ejemplo.
DataPower_XML_mgmt_port	Sí	5550	El puerto utilizado para la interfaz de gestión XML de DataPower, generalmente es 5550.
Datapower_admin_id	Sí		El ID del usuario administrativo con los permisos adecuados para utilizar la interfaz de gestión XML.
DataPower_admin_password	Sí		La contraseña de DataPower_admin_id.
Verificar contraseña	Sí		Verifica la entrada de usuario de DataPower_admin_password.
New_DataPower_domain	Sí		El nuevo nombre de dominio que se debe crear en el dispositivo DataPower. No debe coincidir con ningún dominio existente, de lo contrario, el paquete script fallará o concluirá su ejecución. El valor no puede contener espacios.

Tabla 21. Parámetros configurables (continuación)

Nombre del parámetro	Necesario	Valor predeterminado	Descripción
Remove_security_files	Sí	true	Determina si el archivo `DomainZipFile.zip` y el certificado WSRR que se ha cargado en DataPower se suprimen de la instancia de WSRR donde se ejecutan los paquetes script. Si este archivo no se elimina, será un riesgo de seguridad si los certificados permanecieran en la instancia.

SOA Policy Gateway 2.0.0.0 - Parámetros de configuración del script del Dominio de DataPower para el patrón Tiempo de ejecución avanzado de pasarela de política SOA

Antes de desplegar el patrón, se deben configurar los parámetros necesarios sin un valor predeterminado.

Tabla 22. Parámetros configurables

Nombre del parámetro	Necesario	Valor predeterminado	Descripción
DataPower_hostname	Sí		El nombre de host del dispositivo DataPower en el que se instalará la aplicación de ejemplo.
DataPower_XML_mgmt_port	Sí	5550	El puerto utilizado para la interfaz de gestión XML de DataPower, generalmente es 5550.
Datapower_admin_id	Sí		El ID del usuario administrativo con los permisos adecuados para utilizar la interfaz de gestión XML.
DataPower_admin_password	Sí		La contraseña de DataPower_admin_id.
Verificar contraseña	Sí		Verifica la entrada de usuario de DataPower_admin_password.
New_DataPower_domain	Sí		El nuevo nombre de dominio que se debe crear en el dispositivo DataPower. No debe coincidir con ningún dominio existente, de lo contrario, el paquete script fallará o concluirá su ejecución. El valor no puede contener espacios.

Tabla 22. Parámetros configurables (continuación)

Nombre del parámetro	Necesario	Valor predeterminado	Descripción
Remove_security_files	Sí	true	Determina si el archivo `DomainZipFile.zip` y el certificado WSRR que se ha cargado en DataPower se suprimen de la instancia de WSRR donde se ejecutan los paquetes script. Si este archivo no se elimina, será un riesgo de seguridad si los certificados permanecieran en la instancia.

Script: SOA Policy Gateway 2.0.0.0 - Promoción

El script de Promoción permite integrar el patrón Tiempo de ejecución básico de la pasarela de política SOA o el patrónTiempo de ejecución avanzado de pasarela de política SOA con un patrón Maestro de gobierno de pasarela de política SOA 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 23. Parámetros configurables

Nombre del parámetro	Descripción
WSRR_GOV_DMGR_hostname	El nombre de host del gestor de despliegue para el clúster WSRR.
WSRR_GOV_DMGR_cellname	El nombre de la célula de WebSphere para el clúster WSRR.
WSRR_GOV_admin_user	El ID de administración para la célula de Gobierno de WebSphere WSRR.
WSRR_GOV_admin_password	Contraseña del ID de administración para la célula de Gobierno de WebSphere 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 cual 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.

SOA Policy Gateway 2.0.0.0 - Parámetros de configuración del script de promoción para el patrón Tiempo de ejecución básico de la pasarela de política SOA

Antes de desplegar el patrón, se deben configurar los parámetros necesarios sin un valor predeterminado.

Tabla 24. Parámetros configurables

Nombre del parámetro	Necesario	Valor predeterminado	Descripción
WSRR_GOV_DMGR_hostname	Sí		El nombre de host del gestor de despliegue para el clúster WSRR.
WSRR_GOV_DMGR_cellname	Sí		El nombre de la célula de WebSphere para el clúster WSRR.

Tabla 24. Parámetros configurables (continuación)

Nombre del parámetro	Necesario	Valor predeterminado	Descripción
WSRR_GOV_admin_user	Sí		El ID de administración para la célula de Gobierno de WebSphere WSRR.
WSRR_GOV_admin_password	Sí		Contraseña del ID de administración para la célula de Gobierno de WebSphere WSRR.
Verificar contraseña	Sí		Verifica los datos de entrada del usuario para WSRR_admin_password.
Promotion_environment	Sí		El valor debe ser Transición, Producción o Sin definir. Estos valores distinguen entre mayúsculas y minúsculas, y deben coincidir exactamente.
LTPA_key_password	Sí		En el paquete Script, se exporta y utiliza una clave LTPA, la cual 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	Sí		Verifica los datos de entrada del usuario para LTPA_key_password.

SOA Policy Gateway 2.0.0.0 - Parámetros de configuración del script de promoción para el patrón Tiempo de ejecución avanzado de pasarela de política SOA

Antes de desplegar el patrón, se deben configurar los parámetros necesarios sin un valor predeterminado.

Tabla 25. Parámetros configurables

Nombre del parámetro	Necesario	Valor predeterminado	Descripción
WSRR_GOV_DMGR_hostname	Sí		El nombre de host del gestor de despliegue para el clúster WSRR.
WSRR_GOV_DMGR_cellname	Sí		El nombre de la célula de WebSphere para el clúster WSRR.
WSRR_GOV_admin_user	Sí		El ID de administración para la célula de Gobierno de WebSphere WSRR.
WSRR_GOV_admin_password	Sí		Contraseña del ID de administración para la célula de Gobierno de WebSphere WSRR.
Verificar contraseña	Sí		Verifica los datos de entrada del usuario para WSRR_admin_password.
Promotion_environment	Sí		El valor debe ser Transición, Producción o Sin definir. Estos valores distinguen entre mayúsculas y minúsculas, y deben coincidir exactamente.

Tabla 25. Parámetros configurables (continuación)

Nombre del parámetro	Necesario	Valor predeterminado	Descripción
LTPA_key_password	Sí		En el paquete Script, se exporta y utiliza una clave LTPA, la cual 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	Sí		Verifica los datos de entrada del usuario para LTPA_key_password.

Script: SOA Policy Gateway 2.0.0.0 - Ejemplo

El script Ejemplo configura los parámetros de la aplicación de ejemplo que se utilizarán con el patrón Ejemplo del tiempo de ejecución básico de la pasarela de política SOA.

Parámetros

Nota: cualquier parámetro que necesite el valor Sin definir distingue entre mayúsculas y minúsculas.

Tabla 26. Parámetros configurables

Nombre del parámetro	Descripción
SCP_host	El nombre de host del servidor de SCP que contiene el archivo `DomainZipFile.zip`.
SCP_user	El nombre de usuario que se ha de utilizar para conectarse al servidor de SCP.
SCP_password	La contraseña que se ha de utilizar para conectarse al servidor de SCP.
Verificar contraseña	Verifica la entrada de usuario de SCP_admin_password.
SCP_zip_location	La ubicación del URI del archivo `DomainZipFile.zip`. Por ejemplo, `/files/DomainZipFile.zip`.
CLIENT_PUBLIC_KEY_file	Nombre del archivo de certificados PEM utilizado para conectar con el puerto de la interfaz de gestión XML de dispositivos DataPower. Utilice el valor “Sin definir” para la autenticación de servidor solamente y para no utilizar SSL.
CLIENT_PUBLIC _KEY_password	Contraseña del certificado público utilizado para conectar con el puerto de la interfaz de gestión XML de dispositivos DataPower. El valor es “Sin definir” si no se utiliza ninguna contraseña.
Verificar contraseña	Verifica la entrada de usuario para CLIENT_PUBLIC_KEY_password.
CLIENT_PRIVATE_KEY_file	El nombre del archivo de claves PEM utilizado para conectarse al puerto de la interfaz de gestión XML de dispositivos DataPower. Esto es necesario para la autenticación mutua. Utilice el valor “Sin definir” para la autenticación de servidor solamente y para no utilizar SSL.

Tabla 26. Parámetros configurables (continuación)

Nombre del parámetro	Descripción
CLIENT_PRIVATE_KEY_password	Contraseña del archivo de claves utilizado para conectar con el puerto de la interfaz de gestión XML de dispositivos DataPower. Esto es necesario para la autenticación mutua. El valor es “Sin definir” si no se utiliza ninguna contraseña.
Verificar contraseña	Verifica los datos de entrada del usuario para CLIENT_PRIVATE_KEY_password.
CLI_FILE_file	El nombre del archivo CLI contenido en el archivo `DomainZipFile.zip`. Este CLI se ejecuta el fina de la instalación del dominio y de la configuración del servidor WSRR.
Verificar contraseña	Verifica la entrada de usuario para LTPA_KEY_password.
DataPower_hostname	El nombre de host del dispositivo DataPower en el que se instalará la aplicación de ejemplo.
DataPower_XML_mgmt_port	El puerto utilizado para la interfaz de gestión XML de DataPower.
DataPower_admin_id	El ID del usuario administrativo con los permisos adecuados para utilizar la interfaz de gestión XML.
DataPower_admin_password	La contraseña de DataPower_admin_id.
Verificar contraseña	Verifica la entrada de usuario de DataPower_admin_password.
SOAPolicySample_DataPower_domain	El nombre de dominio de ejemplo. No debe coincidir con ningún dominio existente en el dispositivo DataPower.
SamplePolicySample_starting_port	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 utilizarán los puertos 62000-62004. El script no realiza ninguna comprobación de si los puertos están libres.
LDAP_hostname	El ejemplo utiliza un servidor LDAP, este es el nombre de host de dicho servidor.
LDAP_port	El puerto no seguro del servidor LDAP. Normalmente es 389.
LDAP_password	La contraseña utilizada al enlazar con el LDAP_DN.
Verificar contraseña	Verifica la entrada de usuario de LDAP_admin_password.
LDAP_DN	El nombre distinguido utilizado para enlazar con el LDAP. Por ejemplo, cn=root,dc=ibm.com.

SOA Policy Gateway 2.0.0.0 - Parámetros de configuración del script de ejemplo para el patrón Ejemplo del tiempo de ejecución básico de la pasarela de política SOA

Antes de desplegar el patrón, se deben configurar los parámetros necesarios sin un valor predeterminado.

Nota: cualquier parámetro que necesite el valor Sin definir distingue entre mayúsculas y minúsculas.

Tabla 27. Parámetros configurables

Nombre del parámetro	Necesario	Valor predeterminado	Descripción
SCP_host	Sí		El nombre de host del servidor de SCP que contiene el archivo `DomainZipFile.zip`.
SCP_user	Sí		El nombre de usuario que se ha de utilizar para conectarse al servidor de SCP.
SCP_password	Sí		La contraseña que se ha de utilizar para conectarse al servidor de SCP.
Verificar contraseña	Sí		Verifica la entrada de usuario de SCP_admin_password.
SCP_zip_location	Sí		La ubicación del URI del archivo `DomainZipFile.zip`. Por ejemplo, `/files/DomainZipFile.zip`.
CLIENT_PUBLIC_KEY_file	Sí		Nombre del archivo de certificados PEM utilizado para conectar con el puerto de la interfaz de gestión XML de dispositivos DataPower. Utilice el valor “Sin definir” para la autenticación de servidor solamente y para no utilizar SSL.
CLIENT_PUBLIC _KEY_password	Sí		Contraseña del certificado público utilizado para conectar con el puerto de la interfaz de gestión XML de dispositivos DataPower. El valor es “Sin definir” si no se utiliza ninguna contraseña.
Verificar contraseña	Sí		Verifica la entrada de usuario para CLIENT_PUBLIC_KEY_password.
CLIENT_PRIVATE_KEY_file	Sí		El nombre del archivo de claves PEM utilizado para conectarse al puerto de la interfaz de gestión XML de dispositivos DataPower. Esto es necesario para la autenticación mutua. Utilice el valor “Sin definir” para la autenticación de servidor solamente y para no utilizar SSL.

Tabla 27. Parámetros configurables (continuación)

Nombre del parámetro	Necesario	Valor predeterminado	Descripción
CLIENT_PRIVATE_KEY_password	Sí		Contraseña del archivo de claves utilizado para conectar con el puerto de la interfaz de gestión XML de dispositivos DataPower. Esto es necesario para la autenticación mutua. El valor es "Sin definir" si no se utiliza ninguna contraseña.
Verificar contraseña	Sí		Verifica los datos de entrada del usuario para CLIENT_PRIVATE_KEY_password.
DataPower_hostname	Sí		El nombre de host del dispositivo DataPower en el que se instalará la aplicación de ejemplo.
DataPower_XML_mgmt_port	Sí	5550	El puerto utilizado para la interfaz de gestión XML de DataPower.
DataPower_admin_id	Sí		El ID del usuario administrativo con los permisos adecuados para utilizar la interfaz de gestión XML.
DataPower_admin_password	Sí		La contraseña de DataPower_admin_id.
Verificar contraseña	Sí		Verifica la entrada de usuario de DataPower_admin_password.
SOAPolicySample_DataPower_domain	Sí	SOAPolicySample	El nombre de dominio de ejemplo. No debe coincidir con ningún dominio existente en el dispositivo DataPower.
SOAPolicySample_starting_port	Sí	62001	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 utilizarán los puertos 62000-62004. El script no realiza ninguna comprobación de si los puertos están libres.
LDAP_hostname	Sí		El ejemplo utiliza un servidor LDAP, este es el nombre de host de dicho servidor.
LDAP_port	Sí	389	El puerto no seguro del servidor LDAP. Normalmente es 389.

Tabla 27. Parámetros configurables (continuación)

Nombre del parámetro	Necesario	Valor predeterminado	Descripción
LDAP_password	Sí		La contraseña utilizada al enlazar con el LDAP_DN.
Verificar contraseña	Sí		Verifica la entrada de usuario de LDAP_admin_password.
LDAP_DN	Sí		El nombre distinguido utilizado para enlazar con el LDAP. Por ejemplo, cn=root,dc=ibm.com.

Script: SOA Policy Gateway 2.0.0.0 - Seguridad

El script Seguridad copia la información de seguridad contenida en un archivo ZIP, que es necesaria para comunicarse con un dispositivo DataPower en el gestor de despliegue o en la máquina WSRR desde un servidor de archivos externo que dé soporte al programa de copia segura (SCP) de Linux.

El archivo de seguridad que se copia contiene lo siguiente:

- Certificado de acceso DPC
- Certificado público de acceso DPC
- Clave privada DPC
- Script DP CLI
- Carpeta de la cadena de certificados

El script de la interfaz de línea de mandatos (CLI) para DataPower le permite configurar un dominio desplegado durante la fase de despliegue del patrón.

Nota: Los certificados de seguridad confidenciales se deben suprimir del servidor de archivos externo después del despliegue.

Parámetros

Tabla 28. Parámetros configurables

Nombre del parámetro	Descripción
SCP_host	El nombre de host del servidor de SCP que contiene el archivo `DomainZipFile.zip`.
SCP_user	El nombre de usuario que se ha de utilizar para conectarse al servidor de SCP.
SCP_password	La contraseña que se ha de utilizar para conectarse al servidor de SCP.
Verificar contraseña	Verifica la entrada de usuario de SCP_admin_password.
SCP_zip_location	La ubicación del URI del archivo `DomainZipFile.zip`, por ejemplo, `/files/DomainZipFile.zip`.
CLIENT_PUBLIC_KEY_file	El nombre del archivo de certificados PEM utilizado para conectarse al puerto de la interfaz de gestión XML de dispositivos DataPower.
CLIENT_PUBLIC_KEY_password	La contraseña del certificado de cliente utilizado para conectarse al puerto de la interfaz de gestión XML de dispositivos DataPower. Esto es necesario, si está disponible, para la autenticación mutua. Este valor es “Sin definir” si no se utiliza ninguna contraseña.

Tabla 28. Parámetros configurables (continuación)

Nombre del parámetro	Descripción
CLIENT_PRIVATE_KEY_file	El nombre del archivo de claves PEM utilizado para conectarse al puerto de la interfaz de gestión XML de dispositivos DataPower. Esto es necesario para la autenticación mutua.
CLIENT_PRIVATE_KEY_password	La contraseña del archivo de claves utilizado para conectarse al puerto de la interfaz de gestión XML de dispositivos DataPower. Esto es necesario para la autenticación mutua. Este valor es "Sin definir" si no se utiliza ninguna contraseña.
CLI_file	El nombre del archivo CLI contenido en el archivo `DomainZipFile.zip`. Este CLI se ejecuta al final de la instalación del dominio y de la configuración del servidor WSRR.

SOA Policy Gateway 2.0.0.0 - Parámetros de configuración del script de seguridad para el patrón Tiempo de ejecución básico de la pasarela de política SOA

Antes de desplegar el patrón, se deben configurar los parámetros necesarios sin un valor predeterminado.

Tabla 29. Parámetros configurables

Nombre del parámetro	Necesario	Valor predeterminado	Descripción
SCP_host	Sí		El nombre de host del servidor de SCP que contiene el archivo `DomainZipFile.zip`.
SCP_user	Sí		El nombre de usuario que se ha de utilizar para conectarse al servidor de SCP.
SCP_password	Sí		La contraseña que se ha de utilizar para conectarse al servidor de SCP.
Verificar contraseña	Sí		Verifica la entrada de usuario de SCP_admin_password.
SCP_zip_location	Sí		La ubicación del URI del archivo `DomainZipFile.zip`, por ejemplo, `/files/DomainZipFile.zip`.
CLIENT_PUBLIC_KEY_file	Sí		El nombre del archivo de certificados PEM utilizado para conectarse al puerto de la interfaz de gestión XML de dispositivos DataPower.
CLIENT_PUBLIC_KEY_password	Sí		La contraseña del certificado de cliente utilizado para conectarse al puerto de la interfaz de gestión XML de dispositivos DataPower. Esto es necesario, si está disponible, para la autenticación mutua. Este valor es "Sin definir" si no se utiliza ninguna contraseña.

Tabla 29. Parámetros configurables (continuación)

Nombre del parámetro	Necesario	Valor predeterminado	Descripción
CLIENT_PRIVATE_KEY_file	Sí		El nombre del archivo de claves PEM utilizado para conectarse al puerto de la interfaz de gestión XML de dispositivos DataPower. Esto es necesario para la autenticación mutua.
CLIENT_PRIVATE_KEY_password	Sí		La contraseña del archivo de claves utilizado para conectarse al puerto de la interfaz de gestión XML de dispositivos DataPower. Esto es necesario para la autenticación mutua. Este valor es "Sin definir" si no se utiliza ninguna contraseña.
CLI_file	Sí	Sin definir	El nombre del archivo CLI contenido en el archivo `DomainZipFile.zip`. Este CLI se ejecuta al final de la instalación del dominio y de la configuración del servidor WSRR.

SOA Policy Gateway 2.0.0.0 - Parámetros de configuración del script de seguridad para el patrón Tiempo de ejecución avanzado de pasarela de política SOA

Antes de desplegar el patrón, se deben configurar los parámetros necesarios sin un valor predeterminado.

Tabla 30. Parámetros configurables

Nombre del parámetro	Necesario	Valor predeterminado	Descripción
SCP_zip_location	Sí		La ubicación del URI del archivo `DomainZipFile.zip`, por ejemplo, `/files/DomainZipFile.zip`.
SCP_host	Sí		El nombre de host del servidor de SCP que contiene el archivo `DomainZipFile.zip`.
SCP_user	Sí		El nombre de usuario que se ha de utilizar para conectarse al servidor de SCP.
SCP_password	Sí		La contraseña que se ha de utilizar para conectarse al servidor de SCP.
Verificar contraseña	Sí		Verifica la entrada de usuario de SCP_admin_password.
CLIENT_PUBLIC_KEY_file	Sí		El nombre del archivo de certificados PEM utilizado para conectarse al puerto de la interfaz de gestión XML de dispositivos DataPower.

Tabla 30. Parámetros configurables (continuación)

Nombre del parámetro	Necesario	Valor predeterminado	Descripción
CLIENT_PUBLIC_KEY_password	Sí		La contraseña del certificado de cliente utilizado para conectarse al puerto de la interfaz de gestión XML de dispositivos DataPower. Esto es necesario, si está disponible, para la autenticación mutua. Este valor es “Sin definir” si no se utiliza ninguna contraseña.
CLIENT_PRIVATE_KEY_file	Sí		El nombre del archivo de claves PEM utilizado para conectarse al puerto de la interfaz de gestión XML de dispositivos DataPower. Esto es necesario para la autenticación mutua.
CLIENT_PRIVATE_KEY_password	Sí		La contraseña del archivo de claves utilizado para conectarse al puerto de la interfaz de gestión XML de dispositivos DataPower. Esto es necesario para la autenticación mutua. Este valor es “Sin definir” si no se utiliza ninguna contraseña.
CLI_file	Sí	Sin definir	El nombre del archivo CLI contenido en el archivo `DomainZipFile.zip`. Este CLI se ejecuta al final de la instalación del dominio y de la configuración del servidor WSRR.

Capítulo 5. Trabajar con el patrón de pasarela de política SOA de IBM

El patrón de pasarela de política SOA de IBM proporciona una definición de patrón para el despliegue repetible de la topología de que consta el producto. Cada patrón proporciona una función específica dentro del patrón de pasarela de política SOA de IBM y contiene varias imágenes para dar soporte a cada patrón. Los patrones deben estar configurados antes del despliegue en función de las necesidades empresariales.

Como parte del proceso de despliegue, configure los parámetros de los componentes. Para obtener más información, consulte "Despliegue de patrones" en la página 72.

Tareas relacionadas:

Capítulo 3, "Iniciación al patrón de pasarela de política SOA de IBM", en la página 11
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 comprender lo que se describe en este escenario, las razones por las que una empresa puede desear seguir el escenario, los roles de usuario implicados y una visión general de las posibilidades que se entregan con el producto.

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

El patrón de pasarela de política SOA de IBM proporciona un medio para proporcionar, de forma rápida y fiable, un entorno para gobernar definiciones de servicio y políticas, y aplicar esas políticas. Determine las necesidades de gobierno y los recursos necesarios.

Para desplegar el entorno, prepare el dispositivo DataPower para la administración remota y obtenga los recursos necesarios para comunicarse de forma segura con el dispositivo. Para probar el entorno, despliegue el Ejemplo del tiempo de ejecución básico de la pasarela de política SOA, lo cual comprueba que el entorno está configurado correctamente para el despliegue y muestra la aplicación de las políticas. Después de validar el entorno, se determina la configuración de gobierno y ejecución deseada del patrón de pasarela de política SOA de IBM utilizando los métodos recomendados de WSRR. El despliegue del patrón comienza con el maestro de gobierno, seguido por los patrones de ejecución configurados en la forma deseada.

Preparación y despliegue del patrón de pasarela de política SOA de IBM

Prepare DataPower y obtenga los archivos de seguridad:

1. Prepare el dispositivo DataPower para la administración remota. Para obtener más información, consulte "Configuración de DataPower para el patrón de pasarela de política SOA de IBM" en la página 63.
2. Si el dispositivo DataPower es seguro, lea la sección de seguridad de DataPower, y obtenga los archivos de seguridad de DataPower necesarios para comunicarse con él.

3. Compruebe que un sistema DataPower situado en el entorno de nube se puede comunicar con el dispositivo y que el dispositivo se puede comunicar con un sistema desplegado.

Se puede utilizar el Ejemplo del tiempo de ejecución básico de la pasarela de política SOA para demostrar las características del patrón antes de crear un despliegue de producción. Si es necesario utilizar el Ejemplo de tiempo de ejecución básico, complete los pasos siguientes:

1. Proporcione un servidor de SCP en Linux que sea accesible desde un sistema desplegado existente en la nube. SCP es el mandato de copia de seguridad. El servidor SCP proporciona un medio de albergar los archivos de seguridad externos al patrón para que no sea necesario modificar el patrón para cada configuración de seguridad.
2. Proporcione un servidor LDAP para albergar los ID de seguridad utilizados por la aplicación de ejemplo implementada en DataPower. Para obtener más información, consulte "Configuración de LDAP para el ejemplo" en la página 70.
3. Despliegue el patrón Ejemplo del tiempo de ejecución básico de la pasarela de política SOA para validar la infraestructura. Para obtener más información, consulte "Despliegue del patrón Ejemplo del tiempo de ejecución básico de la pasarela de política SOA" en la página 73.
4. Cuando la utilización del ejemplo se ha completado, el servidor LDAP no es necesario.

Haga los preparativos para el despliegue de producción:

1. Determine la escala necesaria para el despliegue. Determine los tamaños de clúster para el Maestro de gobierno y los despliegues de tiempo de ejecución.

   Nota: Cuando un clúster está desplegado, no se puede ampliar con otro miembro de clúster.
2. Defina el nombre de célula y el ID de usuario administrativo y contraseña del Maestro de gobierno.
3. Albergue el archivo de seguridad `DomainZipFile.zip` de DataPower en un servidor SCP. Para obtener más información, consulte "Creación del archivo `DomainZipFile.zip` de seguridad" en la página 64.

Despliegue el Maestro de gobierno para el entorno de producción:

1. Despliegue de un patrón de Maestro de gobierno de pasarela de política SOA. Espere a que finalice el despliegue antes de desplegar patrones de ejecución del entorno de producción. Para obtener más información, consulte "Despliegue del patrón Maestro de gobierno de pasarela de política SOA" en la página 74.

Despliegue los patrones de ejecución del entorno de producción:

1. Determine si es necesario un entorno en clúster o autónomo.
2. Si es necesario más de un dominio de DataPower, clone el patrón Tiempo de ejecución básico o Tiempo de ejecución avanzado y añada paquetes script de DataPower al clon para cada dominio necesario.

   Nota: No se pueden añadir más dominios de DataPower una vez completada esta configuración.
   Para obtener más información, consulte "Despliegue con varios dominios DataPower" en la página 80.

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 Maestro de gobierno de pasarela de política SOA” en la página 75.
4. Determine si el tiempo de ejecución será de transición, producción, u otro.
5. Despliegue el patrón Tiempo de ejecución básico o Tiempo de ejecución avanzado. Para obtener más información, consulte “Despliegue del patrón Tiempo de ejecución avanzado de pasarela de política SOA” en la página 77 o “Despliegue del patrón Tiempo de ejecución básico de la pasarela de política SOA ” en la página 75.
6. Espere a que finalice totalmente el despliegue antes de desplegar otro tiempo de ejecución.

Cuando finalice el despliegue de los tiempos de ejecución:

1. El servidor de archivos SCP ya no es necesario.
2. WSRR y la seguridad de WebSphere se pueden actualizar a una configuración de seguridad diferente de la configuración predeterminada. Para obtener más información, consulte “Gestión de la seguridad” en la página 64.
3. El dominio DataPower está listo para la configuración de la pasarela.

Configuración de DataPower para el patrón de pasarela de política SOA de IBM

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

Procedimiento

1. Inicie una sesión en el dispositivo DataPower como administrador.
2. Busque `Interfaz de gestión XML`.
3. Asegúrese de que su estado sea 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 de pasarela de política SOA de IBM

Los clientes necesitan diferentes niveles de seguridad entre WSRR y DataPower, especialmente en lo relacionado con SSL. El patrón de pasarela de política SOA de IBM permite 3 niveles de comunicación SSL entre los scripts de configuración y DataPower cuando se utilizan los patrones Tiempo de ejecución básico de la pasarela de política SOA , Ejemplo del tiempo de ejecución básico de la pasarela de política SOA y Tiempo de ejecución avanzado de pasarela de política SOA.

Si SSL no es necesario

Si no necesita utilizar SSL, no se proporcionan la clave pública y las claves privadas del cliente curl y se dejan como “Sin definir”.

Nota: Si no se utiliza SSL, los datos enviados a DataPower no se cifran, incluida la información de usuario y la contraseña. Esto supone una vulnerabilidad para la seguridad. Las contraseñas utilizadas en las llamadas SOMA a DataPower no permiten el cifrado y por tanto se transfieren sin cifrar al dispositivo DataPower. Por lo tanto, la autenticación en el extremo servidor se utiliza a un nivel mínimo para garantizar la seguridad.

Autenticación mutua entre las aplicaciones DataPower y los scripts de los patrones Básico y Avanzado

Si necesita que haya autenticación mutua entre las aplicaciones DataPower y los scripts de los patrones Básico y Avanzado:

- Se deben proporcionar la clave pública y las claves privadas del cliente curl.

Gestión 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 crear un entorno realmente seguro, debe protegerlo con técnicas de seguridad estándar de WebSphere.

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

Creación del archivo `DomainZipFile.zip` de seguridad

Cree el archivo `DomainZipFile.zip` de seguridad para el patrón Tiempo de ejecución básico de la pasarela de política SOA , el patrón Tiempo de ejecución avanzado de pasarela de política SOA y el patrón Ejemplo del tiempo de ejecución básico de la pasarela de política SOA.

Procedimiento

Cree el archivo `DomainZipFile.zip` utilizando las reglas siguientes:

1. La estructura del archivo `DomainZipFile.zip` debe ser la siguiente:

   Nota: Sólo es necesaria la estructura de directorios, los nombres de archivos individuales pueden seguir la denominación de archivos de su elección. No obstante, todos los certificados y archivos de claves deben tener el formato PEM.

   Nota: La utilización del nombre de host de DataPower en la vía de acceso permite utilizar certificados diferentes para diferentes dispositivos DataPower.

Tabla 31. Archivos necesarios para los patrones Básico y Avanzado

Nombre del archivo, ubicación referida al directorio raíz	**Notas**
`CurlClientPublicKeyFile.crt`	Sólo es necesario si se utiliza la autenticación mutua. En formato PEM únicamente.
`CurlClientPrivateKeyFile.key`	Sólo es necesario si se utiliza la autenticación mutua.
`/dataPowerHostName/certificate1.crt`	Certificados de DataPower que se han de cargar en WSRR. Necesita que la cadena de certificados completa esté en formato PEM. Certificados de DataPower que se han de cargar en WSRR. Debe incluir únicamente el contenido siguiente: `------BEGINCERTIFICATE---- to -----END CERTIFICATE-----` La extensión del archivo debe ser `.crt` o `.pem`.
`/dataPowerHostName/certificate2.crt`	La extensión del archivo debe ser `.crt` o `.pem`.
`/dataPowerHostName/certificate3.crt`	La extensión del archivo debe ser `.crt` o `.pem`.

2. Para el patrón Tiempo de ejecución avanzado de pasarela de política SOA únicamente, añada el archivo `cli` que se debe ejecutar (opcional):

Tabla 32. Archivos adicionales necesarios para el patrón Avanzado

Nombre del archivo, ubicación referida al directorio raíz	**Notas**
`/cli.cli`	Archivo CLI que se ejecutará al final de la configuración del dominio DataPower.

3. Coloque el archivo `DomainZipFile.zip` en la ubicación del servidor SCP. Debido a la naturaleza confidencial de los archivos, se recomienda suprimir el archivo después de la configuración. Los scripts de configuración del patrón suprimirán todos los archivos del archivo `DomainZipFile.zip`, así como la copia del archivo `DomainZipFile.zip` que se crea utilizando SCP desde el entorno SCP.
4. Anote la información siguiente del servidor SCP:
   - El nombre de host SCP.
   - La vía de acceso SCP del archivo `DomainZipFile.zip`.
   - El usuario SCP y la contraseña.

Utilización del archivo `DomainZipFile`

Casos de uso del archivo `DomainZipFile` para diferentes niveles de seguridad en patrones.

El archivo `DomainZipFile.zip` se puede utilizar en los patrones Tiempo de de ejecución básico, Tiempo de ejecución básico con ejemplo y Tiempo de ejecución avanzado.

No es necesario SSL para conectar los paquetes script de patrón con el dispositivo DataPower. Si no utiliza SSL, no es necesario que cree un archivo `DomainZipFile.zip`, a menos que necesite un script cli para personalizar el dominio DataPower creado por el patrón. En este caso, si no utiliza autenticación de servidor como mínimo, los datos no se cifrarán. Este es un riesgo de seguridad porque la información de usuario y contraseña se pasa a DataPower durante el cliente de scripts a través de una conexión http, y esto está protegido por los certificados en el archivo `DomainZipFile.zip` .

Si el host DataPower no está configurado para validar el certificado de cliente, no es necesario que utilice la autenticación mutua entre el cliente de script y el dispositivo DataPower. Es recomendable que utilice la autenticación de servidor como mínimo.

Los casos de ejemplo de este tema describen diferentes niveles de seguridad.

Son posibles los casos siguientes:

Caso 1: No es necesario ningún SSL

Caso 2: No es necesario ningún SSL, pero es necesario un script cli para personalizar el dominio

Caso 3: es necesaria la autenticación de servidor del certificado de DataPower por el cliente de script

Caso 4: es necesaria autenticación mutua con el dispositivo DataPower

Caso 1: No es necesario ningún SSL

Se recomienda, por las razones de seguridad descritas, que esta opción sólo se utilice en situaciones de desarrollo. Si no desea utilizar ningún SSL:

1. Establezca los parámetros de SCP_host en "Sin definir". Si está utilizando los patrones Tiempo de ejecución básico o Tiempo de ejecución avanzado, SCP_host está en el script SOA Policy Gateway 2.0.0.0 - Security Package. Si está utilizando el patrón Tiempo de ejecución básico con ejemplo, SCP_host está en el script SOA Policy Gateway 2.0.0.0. Esto define el script en el patrón de forma que no obtiene el archivo `DomainZipFile.zip` utilizando SCP.
2. Establezca los parámetros siguientes en "Sin definir" en los mismos paquetes script del paso 1:
   - CLIENT_PUBLIC_KEY_file
   - CLIENT_PUBLIC_KEY_password
   - Verificar contraseña
   - CLIENT_PRIVATE_KEY_file
   - CLIENT_PRIVATE_KEY_password
   - Verificar contraseña

Caso 2: No es necesario ningún SSL, pero es necesario un script cli para personalizar el dominio

Se recomienda, por las razones de seguridad descritas, que esta opción sólo se utilice en situaciones de desarrollo. Si no desea utilizar SSL, pero necesita un script cli:

1. Establezca los parámetros de SCP_host en "Sin definir". Si está utilizando los patrones Tiempo de ejecución básico o Tiempo de ejecución avanzado, SCP_host está en el script SOA Policy Gateway 2.0.0.0 - Security Package. Si está utilizando el patrón Tiempo de ejecución básico con ejemplo, SCP_host está en el script SOA Policy Gateway 2.0.0.0. Esto define el script en el patrón de forma que no obtiene el archivo `DomainZipFile.zip` utilizando SCP.
2. Establezca los parámetros siguientes en Sin definir en los mismos paquetes script del paso 1:
   - CLIENT_PUBLIC_KEY_file
   - CLIENT_PUBLIC_KEY_password
   - Verificar contraseña

- CLIENT_PRIVATE_KEY_file
- CLIENT_PRIVATE_KEY_password
- Verificar contraseña

Nota: Si SCP_host es "Sin definir", no necesita un archivo `DomainZipFile.zip`, a menos que tenga un script cli que desee ejecutar en los patrones Tiempo de ejecución básico y Tiempo de ejecución avanzado.

3. Coloque el archivo de script cli que desee utilizar en la raíz del archivo `DomainZipFile.zip`. A continuación se muestra una estructura de ejemplo del archivo `DomainZipFile.zip`:

   `/cli.cli`

   Este archivo se ejecuta al final del paquete script DataPower Domain. `cli.cli` es un nombre de archivo de ejemplo. El nombre de archivo no debe contener espacios.

Caso 3: es necesaria la autenticación de servidor del certificado de DataPower por el cliente de script

Debe proporcionar todos los certificados de la cadena de certificados de DataPower que protege la interfaz de gestión XML. Para localizar los certificados, complete estos pasos:

1. Examine el perfil de proxy SSL para la interfaz de gestión XML y localice el CryptoProfile. El perfil de cifrado contendrá las credenciales de identificación que contienen los certificados utilizados para proteger la interfaz de gestión XML.
2. Añada estos certificados al archivo `DomainZipFile.zip`.

   El formato es:

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

   Si está utilizando varios dominios, el archivo puede tener dos directorios `dataPowerHostName` diferentes, con los archivos siguientes para cada cadena de certificados de DataPower:

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

   Nota: Los archivos de la cadena de certificados de DataPower deben ser de tipo `.crt` o `.pem` y sólo deben contener el propio certificado. Los nombres de archivo `.crt` o `.pem` utilizados aquí son ejemplos. El nombre de archivo no debe contener espacios.
3. Opcional: Si sólo necesita la autenticación de servidor para el script SOA Policy Gateway 2.0.0.0 - Security Package en los patrones Tiempo de ejecución básico y Tiempo de ejecución avanzado, o el script SOA Policy Gateway 2.0.0.0 - Sample en el patrón Tiempo de ejecución básico con ejemplo, utilice "Sin definir" como valor de los parámetros siguientes en esos scripts:

   - CLIENT_PUBLIC_KEY_file

- CLIENT_PUBLIC_KEY_password
- Verificar contraseña
- CLIENT_PRIVATE_KEY_file
- CLIENT_PRIVATE_KEY_password
- Verificar contraseña

4. Opcional: si es necesario un script cli:

   Coloque el archivo de script cli que desee utilizar en la raíz del archivo `DomainZipFile.zip`. A continuación se muestra una estructura de ejemplo del archivo `DomainZipFile.zip`:

   `/cli.cli`

   Este archivo se ejecuta al final del paquete script DataPower Domain. `cli.cli` es un nombre de archivo de ejemplo. El nombre de archivo no debe contener espacios.

Caso 4: es necesaria autenticación mutua con el dispositivo DataPower

En este caso, el cliente y el servidor DataPower necesitan una validación mutua de certificados. Esto sólo es necesario si el host DataPower está configurado en el perfil de proxy SSL de la interfaz de gestión XML para validar los certificados de los clientes.

1. Añada estos certificados al archivo `DomainZipFile.zip`.

   El formato es:

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

   Nota: Los archivos de la cadena de certificados de DataPower deben ser de tipo `.crt` o `.pem` y sólo deben contener el propio certificado. Los nombres de archivo `.crt` o `.pem` utilizados aquí son ejemplos. El nombre de archivo no debe contener espacios.

   El certificado de cliente y el archivo de claves del cliente puede contener los datos del certificado o archivo de claves antes de la línea del archivo donde se lee: `-----BEGIN CERTIFICATE-----`.

2. Opcional: Si sólo es necesaria la autenticación de servidor para el script SOA Policy Gateway 2.0.0.0 - Security Package en los patrones Tiempo de ejecución básico y Tiempo de ejecución avanzado, o el script SOA Policy Gateway 2.0.0.0 - Sample en el patrón Tiempo de ejecución básico con ejemplo, utilice “Sin definir” como valor de los parámetros siguientes en esos scripts:

   - CLIENT_PUBLIC_KEY_file
   - CLIENT_PRIVATE_KEY_file
   - CLIENT_PRIVATE_KEY_password
   - Verificar contraseña

3. Si no hay ninguna contraseña para el archivo de claves públicas, el valor de lo siguiente puede ser “Sin definir”:

- CLIENT_PUBLIC_KEY_password
- Verificar contraseña

4. Los mandatos curl utilizados por los paquetes script suponen que el tipo de archivo es `.pem`, por lo que **--key-type** y **--cert-type** se establecen en PEM de forma predeterminada. El certificado y los archivos de claves puede contener este contenido antes de la línea `-----BEGIN CERTIFICATE-----` en el certificado o archivo de claves determinado.
5. Opcional: si es necesario un script cli y se utilizan los patrones Tiempo de ejecución básico o Tiempo de ejecución avanzado:

   Coloque el archivo de script cli que desee utilizar en la raíz del archivo `DomainZipFile.zip`. A continuación se muestra una estructura de ejemplo del archivo `DomainZipFile.zip`:

   ```
   /cli.cli
   ```

   Este archivo se ejecuta al final del paquete script DataPower Domain. `cli.cli` es un nombre de archivo de ejemplo. El nombre de archivo no debe contener espacios.

Al seleccionar un caso, ha configurado el nivel adecuado de seguridad, con o sin utilización del archivo `DomainZipFile.zip`.

Certificados DataPower que se han de transferir a WSRR

Puede proporcionar un directorio de certificados en el directorio `dataPowerHostName` del archivo `DomainZipFile.zip`. Este se puede transferir al servidor WSRR Dmgr o al servidor autónomo WSRR.

Cómo proporcionar su propio mecanismo para descargar el archivo `DomainZipFile.zip`

Puede proporcionar su propio `DomainZipFile.zip` sin utilizar el servidor SCP en el paquete de scripts de seguridad.

Procedimiento

Para utilizar otros medios para colocar el archivo en el entorno, debe hacer lo siguiente:

1. El parámetro **`SCP_host`** debe establecerse en Sin definir.
2. Debe crear un paquete de scripts personalizado para crear el archivo `DomainZipFile.zip` en el directorio `/tmp` antes de ejecutar cualquiera de los scripts de patrones de pasarela SOA.
3. Para patrones avanzados, cree el archivo `DomainZipFile.zip` en el directorio `/tmp/security/RetrieveDomainFiles`.
4. Para patrones básicos con ejemplo, cree el archivo `DomainZipFile.zip` en el directorio `/installSample/Retrieve_Domain_Files`.

   Nota: Si el archivo `DomainZipFile.zip` no está presente, el script puede fallar si los parámetros indican que se han utilizado certificados o claves.

Valores CN en los certificados

Los certificados proporcionados como parte del archivo `DomainZipFile.zip` debe tener en cuenta el valor CN del certificado.

La verificación de nombre de host siempre se activa cuando utiliza SSL, por lo tanto, es necesario tener en cuenta lo siguiente cuando se utiliza el certificado en el paquete de script:

- Para los certificados de cliente (clave/pública y privada), no hay forma de saber el host exacto en el que el servidor WSRR o el gestor de despliegue WSRR ejecuta el script. Por lo tanto, el valor CN debe ser lo suficientemente genérico para poder ejecutarlo en cualquier posible host de cliente en el entorno IBM Workload Deployer, por ejemplo, `*nombrecliente*.suempresa.com`.
- Los certificados para las máquinas DataPower máquinas están en directorios individuales en el archivo `DomainZipFile.zip`; por ejemplo:

  ```
  dpHost1/cert1.crt
  dpHost2/certb.crt
  dpHost2/certbc.pem
  ```
- El valor CN para el certificado (el certificado final de la cadena para el host DataPower) debe ser válido para dicho nombre de host, por ejemplo, `dp1.suempresa.com` o `*dp*.suempresa.com`.

Configuración de LDAP para el ejemplo

El ejemplo requiere un LDAP (Lightweight Directory Access Protocol) con algunas entradas específicas.

Acerca de esta tarea

Los elementos y las propiedades se deben definir al configurar el LDAP.

Nota: no cambie estas contraseñas.

Como alternativa a los pasos de configuración manual, extraiga el contenido del siguiente archivo `.zip`, que contiene dos archivos LDIF con los datos de configuración que se proporcionan en esta tarea, y utilice estos archivos para actualizar el servidor LDAP: soaSamples.zip.

Procedimiento

Cree un LDAP con los elementos siguientes:

1. Defina el sufijo:

   ```
   dc=ibm.com
   ```
2. Defina el dominio `dc=ibm.com` con las propiedades siguientes:

   ```
   dn: dc=ibm.com
   dc: ibm.com
   objectclass: domain
   objectclass: top
   ```
3. Defina los contenedores:
   a. Defina los grupos del contenedor:

      ```
      dn: cn=groups,dc=ibm.com
      objectclass: container
      objectclass: top
      cn: groups
      ```
   b. Defina los usuarios del contenedor:

      ```
      dn: cn=users,dc=ibm.com
      objectclass: container
      objectclass: top
      cn: users
      ```
4. Defina los usuarios siguientes:
   a. El usuario ConsumerA con las propiedades siguientes:

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

b. El usuario ConsumerB con las propiedades siguientes:

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

c. El usuario ConsumerX con las propiedades siguientes:

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

5. Defina los grupos siguientes:
   a. Defina el grupo MANAGER con las propiedades siguientes:

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

   b. Defina el grupo Clerk con las propiedades siguientes:

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

   c. Defina el grupo Customer con las propiedades siguientes:

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

6. Asegúrese de recopilar la siguiente información sobre el LDAP antes de ejecutar el ejemplo:
   - El nombre distinguido (DN); por ejemplo `cn=root`.
   - La contraseña; por ejemplo `passw0rd`.
   - El puerto no seguro, por ejemplo, 389.
   - El nombre de host LDAP, por ejemplo, `ldap.customer.com`.

Despliegue de patrones

Desplegar patrones en la nube con IBM Workload Deployer 3.1.0.2 o patrón de pasarela de política SOA de IBM proporciona un entorno activo de IBM PureApplication System. Puede desplegar los patrones predefinidos disponibles con las imágenes del patrón de pasarela de política SOA de IBM o 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.

Acerca de esta tarea

El despliegue de un patrón crea un sistema virtual o un entorno de tiempo de ejecución del patrón de pasarela de política SOA de IBM recién creado, que se ejecuta en la nube.

Procedimiento

Para desplegar los patrón de pasarela de política SOA de IBM, 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 que se está desplegando. Un patrón desplegado es un sistema virtual, o el entorno de tiempo de ejecución del patrón de pasarela de política SOA de IBM 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 Workload Deployer: Gestión de patrones del sistema virtual

IBM PureApplication System: Gestión de patrones del sistema virtual

Despliegue del patrón Ejemplo del tiempo de ejecución básico de la pasarela de política SOA

Cuando se despliega el patrón Ejemplo del tiempo de ejecución básico de la pasarela de política SOA se crea una instancia de sistema virtual en ejecución del patrón.

Antes de empezar

Se deben cumplir estos requisitos previos antes de desplegar el patrón:

- Configure DataPower para el ejemplo; consulte "Configuración de DataPower para el patrón de pasarela de política SOA de IBM" en la página 63.
- Configure la seguridad para el ejemplo; consulte "Seguridad para los patrones patrón de pasarela de política SOA de IBM" en la página 63.
- Configure el servidor SCP para albergar los archivos de seguridad.
- Configure LDAP para el ejemplo; consulte "Configuración de LDAP para el ejemplo" en la página 70.

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 Ejemplo del tiempo de ejecución básico de la pasarela de política SOA, realice los pasos siguientes :

1. Pulse **Patrones** > **Sistemas virtuales**.
2. En la lista Patrones de sistema virtual, seleccione **SOA Policy Gateway 2.0.0.0 - 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. Configure los patrones virtuales. Pulse **Configurar componentes virtuales** y, a continuación, pulse el nombre del componente para abrir el editor para componentes y scripts:

      Nota: Todas las contraseñas para este patrón, excepto el parámetro DataPower_admin_id, toman el valor predeterminado `password`.

      - "Parámetros de configuración del componente DB2 Enterprise para el patrón Ejemplo del tiempo de ejecución básico de la pasarela de política SOA" en la página 29.
      - "Parámetros de configuración del componente Servidor WSRR autónomo para el patrón Ejemplo del tiempo de ejecución básico de la pasarela de política SOA" en la página 41

- "SOA Policy Gateway 2.0.0.0 - Parámetros de configuración del script de ejemplo para el patrón Ejemplo del tiempo de ejecución básico de la pasarela de política SOA" en la página 53

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

Qué hacer a continuación

Para verificar el despliegue, consulte "Verificación del despliegue" en la página 78.

Despliegue del patrón Maestro de gobierno de pasarela de política SOA

Cuando se despliega el patrón Maestro de gobierno de pasarela de política SOA se crea una instancia de sistema virtual en ejecución del patrón.

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 Maestro de gobierno de pasarela de política SOA, realice los pasos siguientes :

1. Pulse **Patrones** > **Sistemas virtuales**.
2. En la lista Patrones de sistema virtual, seleccione **SOA Policy Gateway 2.0.0.0 - Governance Master**.
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. Configure los patrones virtuales. Pulse **Configurar componentes virtuales** y, a continuación, pulse el nombre del componente para abrir el editor del componente.
      - "Parámetros de configuración del componente DB2 Enterprise HADR Primary para el patrón Maestro de gobierno de pasarela de política SOA" en la página 33
      - "Parámetros de configuración del componente Gestor de despliegue de WSRR para el patrón Maestro de gobierno de pasarela de política SOA" en la página 43
      - "Parámetros de configuración del componente Nodos personalizados de WSRR para el patrón Maestro de gobierno de pasarela de política SOA" en la página 46
      - "Parámetros de configuración del componente DB2 Enterprise HADR Standby para el patrón Maestro de gobierno de pasarela de política SOA" en la página 37
5. Pulse **Aceptar** para desplegar el patrón.

Qué hacer a continuación

Para verificar el despliegue, consulte "Verificación del despliegue" en la página 78.

Información sobre el despliegue del Maestro de gobierno de pasarela de política SOA

El Maestro de gobierno se debe desplegar antes de desplegar los patrones Tiempo de ejecución básico de la pasarela de política SOA o Tiempo de ejecución avanzado de pasarela de política SOA.

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. Anote lo siguiente:
   - 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.

   Nota: 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 Tiempo de ejecución básico de la pasarela de política SOA o Tiempo de ejecución avanzado de pasarela de política SOA:
   - WSRR_GOV_DMGR_hostname
   - WSRR_GOV_DMGR_cellname
   - WSRR_GOV_admin_user
   - WSRR_GOV_admin_password

Despliegue del patrón Tiempo de ejecución básico de la pasarela de política SOA

Cuando se despliega el patrón Tiempo de ejecución básico de la pasarela de política SOA se crea una instancia de sistema virtual en ejecución del patrón.

Antes de empezar

Complete los pasos siguientes antes de desplegar el patrón de Tiempo ejecución básico:

- Configure DataPower para el patrón de pasarela de política SOA de IBM; consulte “Configuración de DataPower para el patrón de pasarela de política SOA de IBM” en la página 63.
- Configure la seguridad para el patrón de pasarela de política SOA de IBM; consulte “Seguridad para los patrones patrón de pasarela de política SOA de IBM” en la página 63.
- Configure el servidor SCP para albergar los archivos de seguridad.

- Obtenga la información de despliegue del Maestro de gobierno; consulte "Información sobre el despliegue del Maestro de gobierno de pasarela de política SOA" en la página 75.

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 al mismo tiempo en el patrón Tiempo de ejecución básico de la pasarela de política SOA o el patrón Tiempo de ejecución avanzado de pasarela de política SOA. Esto 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 el patrón Tiempo de ejecución básico de la pasarela de política SOA , realice los pasos siguientes :

1. Pulse **Patrones** > **Sistemas virtuales**.
2. En la lista Patrones de sistema virtual, seleccione **SOA Policy Gateway Basic Runtime 2.0.0.0**.
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. Configure los patrones virtuales. Pulse **Configurar componentes virtuales** y, a continuación, pulse el nombre del componente para abrir el editor para componentes y scripts:
      - "Parámetros de configuración del componente DB2 Enterprise para el patrón Tiempo de ejecución básico de la pasarela de política SOA " en la página 28
      - "Parámetros de configuración del componente del Servidor WSRR autónomo para el patrón Tiempo de ejecución básico de la pasarela de política SOA " en la página 39
      - "SOA Policy Gateway 2.0.0.0 - Parámetros de configuración del script de seguridad para el patrón Tiempo de ejecución básico de la pasarela de política SOA " en la página 57
      - "SOA Policy Gateway 2.0.0.0 - Parámetros de configuración del script de promoción para el patrón Tiempo de ejecución básico de la pasarela de política SOA " en la página 50
      - "SOA Policy Gateway 2.0.0.0 - Parámetros de configuración del script del Dominio de DataPowern para el patrón Tiempo de ejecución básico de la pasarela de política SOA " en la página 48
5. Pulse **Aceptar** para desplegar el patrón.

Qué hacer a continuación

Para verificar el despliegue, consulte "Verificación del despliegue" en la página 78.

Despliegue del patrón Tiempo de ejecución avanzado de pasarela de política SOA

Cuando se despliega el patrón Tiempo de ejecución avanzado de pasarela de política SOA se crea una instancia de sistema virtual en ejecución del patrón.

Antes de empezar

Complete los pasos siguientes antes de desplegar el patrón de Tiempo ejecución avanzado:

- Configure DataPower para el patrón de pasarela de política SOA de IBM; consulte "Configuración de DataPower para el patrón de pasarela de política SOA de IBM" en la página 63.
- Configure la seguridad para el patrón de pasarela de política SOA de IBM; consulte "Seguridad para los patrones patrón de pasarela de política SOA de IBM" en la página 63.
- Configure el servidor SCP para albergar los archivos de seguridad.
- Obtenga la información de despliegue del Maestro de gobierno; consulte "Información sobre el despliegue del Maestro de gobierno de pasarela de política SOA" en la página 75.

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 al mismo tiempo en el patrón Tiempo de ejecución básico de la pasarela de política SOA o el patrón Tiempo de ejecución avanzado de pasarela de política SOA. Esto 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 el patrón Tiempo de ejecución avanzado de pasarela de política SOA, realice los pasos siguientes :

1. Pulse **Patrones** > **Sistemas virtuales**.
2. En la lista Patrones de sistema virtual, seleccione **SOA Policy Gateway 2.0.0.0 - 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. Opcional: Seleccione el entorno y planifique el despliegue.
   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:
      - "Parámetros de configuración del componente DB2 Enterprise HADR Primary para el patrón Tiempo de ejecución avanzado de pasarela de política SOA" en la página 32

- "Parámetros de configuración del componente Gestor de despliegue de WSRR para el patrón Tiempo de ejecución avanzado de pasarela de política SOA" en la página 43
- "SOA Policy Gateway 2.0.0.0 - Parámetros de configuración del script de seguridad para el patrón Tiempo de ejecución avanzado de pasarela de política SOA" en la página 58
- "SOA Policy Gateway 2.0.0.0 - Parámetros de configuración del script de promoción para el patrón Tiempo de ejecución avanzado de pasarela de política SOA" en la página 51
- "SOA Policy Gateway 2.0.0.0 - Parámetros de configuración del script del Dominio de DataPower para el patrón Tiempo de ejecución avanzado de pasarela de política SOA" en la página 49
- "Parámetros de configuración del componente Nodos personalizados de WSRR para el patrón Tiempo de ejecución avanzado de pasarela de política SOA" en la página 45
- "Parámetros de configuración del componente DB2 Enterprise HADR Standby para el patrón Tiempo de ejecución avanzado de pasarela de política SOA" en la página 35

5. Pulse **Aceptar** para realizar el despliegue.

Qué hacer a continuación

Para verificar el despliegue, consulte "Verificación del despliegue".

Verificación del despliegue

Cuando haya desplegado 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 123.
2. Opcional: Si ha desplegado el Ejemplo del tiempo de ejecución básico de la pasarela de política SOA, 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 83.

Caso de ejemplo: añadir un tiempo de ejecución adicional al patrón

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. Esto significa que existen estados y transiciones que son específicos de los entornos de transición y producción, lo que permite realizar una promoción controlada hacia estos entornos definiendo sistemas de destino en el archivo de configuración de la promoción. Esto 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 entornos adicionales, 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 61.

Procedimiento

1. Despliegue el Maestro de gobierno de pasarela de política SOA predefinido. Para obtener más información, consulte "Despliegue del patrón Maestro de gobierno de pasarela de política SOA" en la página 74.
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 Tiempo de ejecución básico de la pasarela de política SOA o Tiempo de ejecución avanzado de pasarela de política SOA con los detalles del Maestro de gobierno. Para obtener más información, consulte "Información sobre el despliegue del Maestro de gobierno de pasarela de política SOA" en la página 75.

   Nota: El valor de entorno de promoción debe estar establecido en "Sin definir".
4. Despliegue el Tiempo de ejecución básico de la pasarela de política SOA o Tiempo de ejecución avanzado de pasarela de política SOA predefinido Para obtener más información, consulte "Despliegue del patrón Tiempo de ejecución básico de la pasarela de política SOA " en la página 75 y "Despliegue del patrón Tiempo de ejecución avanzado de pasarela de política SOA" en la página 77.

Clonación y personalización del patrón de pasarela de política SOA de IBM

El patrón de pasarela de política SOA de IBM no se puede editar. Si la topología proporcionada en los patrones de sistema virtual del patrón de pasarela de política SOA de IBM no proporcionan la función que necesita, puede clonar el patrón y editarlo para crear patrones nuevos.

Acerca de esta tarea

Para personalizar los patrones, puede realizar lo siguiente:

- Añada dominios adicionales de DataPower. Para obtener más información, consulte "Despliegue con varios dominios DataPower" en la página 80.
- Aumente el tamaño de clúster predeterminado. Para obtener más información, consulte Centro de información de IBM Workload Deployer, Versión 3.1.

  Nota: Cuando aumente el tamaño de clúster, aumente también el tamaño de memoria del gestor de despliegue de WSRR.
- Seleccione el modo de obtener el archivo de seguridad comprimido en el servidor. Para obtener más información, consulte "Gestión de la seguridad" en la página 64.

- Defina y bloquee sus propios valores predeterminados; por ejemplo, el ID de administrador de DataPower. Para obtener más información sobre el bloqueo de parámetros, consulte Centro de información de IBM Workload Deployer, Versión 3.1.
- Utilice un mecanismo propio para descargar el archivo `DomainZipFile.zip`. Para obtener más información, consulte "Cómo proporcionar su propio mecanismo para descargar el archivo `DomainZipFile.zip`" en la página 69.

Procedimiento

Para clonar los patrones para editarlos y crear patrones nuevos, siga los pasos siguientes:

1. En el panel izquierdo de la ventana Patrón, seleccione el patrón que se debe clonar.
2. Pulse el icono Clonar y proporcione un nombre para el nuevo patrón. También puede proporcionar información adicional, tal como una descripción.
3. Seleccione el nuevo patrón y pulse el icono Editar para cambiar la configuración. Puede añadir y eliminar componentes y configurarlos, aumentar o disminuir el número de algunos componentes o cambiar el orden en el que se despliegan algunos componentes.

Qué hacer a continuación

Asegúrese de que todos los componentes necesarios están correctamente configurados para el tipo de patrón que ha creado. Puede desplegar el patrón cuando se haya completado la configuración.

Información relacionada:

IBM Workload Deployer: Gestión de patrones del sistema virtual

IBM PureApplication System: Gestión de patrones del sistema virtual

Despliegue con varios dominios DataPower

Los patrones Tiempo de ejecución básico de la pasarela de política SOA y Tiempo de ejecución avanzado de pasarela de política SOA se pueden clonar y personalizar para incluir varios dominios DataPower.

Procedimiento

1. Clone el patrón Tiempo de ejecución básico de la pasarela de política SOA o Tiempo de ejecución avanzado de pasarela de política SOA. Para obtener más información, consulte "Clonación y personalización del patrón de pasarela de política SOA de IBM" en la página 79.
2. Para editar el patrón, pulse **Editar**.
3. Expanda la sección **Scripts**.
4. Para cada dominio adicional que se deba añadir, arrastre y suelte el paquete script **SOA Policy Gateway 2.0.0.0 DataPower Domain** en la parte del gestor de despliegue de WSRR para el patrón Tiempo de ejecución avanzado, o en la parte autónoma de WSRR para el patrón de Tiempo de ejecución básico.
5. Pulse **Edición finalizada**.
6. Despliegue el patrón, especificando la información siguiente para cada dominio añadido:
   - DataPower_hostname
   - DataPower_XML_mgmt_port

- DataPower_admin_id
- DataPower_admin_password
- Verificar contraseña
- New_DataPower_domain
- securityFileCleanUp

  Nota: Cuando se utilizan varios dominios, el último dominio debe tener el valor securityFileCleanUp establecido en **true**, y todos los demás dominios debe tener el valor establecido en **false**.

Para obtener más información sobre el despliegue de los patrones, consulte "Despliegue del patrón Tiempo de ejecución básico de la pasarela de política SOA " en la página 75 o "Despliegue del patrón Tiempo de ejecución avanzado de pasarela de política SOA" en la página 77.

La aplicación de ejemplo

La aplicación de ejemplo es un dominio DataPower configurable y un conjunto de artefactos WSRR que se pueden utilizar para demostrar las posibilidades del patrón.

El escenario básico de la aplicación de ejemplo es una aplicación de inventario para una tienda (almacén). Existe un servicio web de tienda que tiene tres operaciones:

- purchase
- findInventory
- returnProduct

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

- Validación por comparación con Store.wsdl. Esto supone que la validación de DataPower está desactivada.
- Rechazar si existen más de 5 mensajes en 90 segundos. Este es un valor umbral bajo para demostraciones sencillas.

Los consumidores del servicio tienen actualmente dos acuerdos de nivel de servicio (SLA): Gold y Anonymous. Si el contexto del cliente en la cabecera HTTP es Gold, se le direcciona inmediatamente hacia el punto final alternativo. Si es Anonymous, esto es, actualmente no es Gold, se le direcciona hacia el punto final Store Mock Service, que tiene un valor de precio diferente para el artículo.

El escenario también realiza la autorización para la operación findInventory, de acuerdo con la pertenencia a un grupo de usuarios. La Figura 5 en la página 82 muestra el flujo de la aplicación, donde cada cuadro representa una pasarela DataPower diferente.

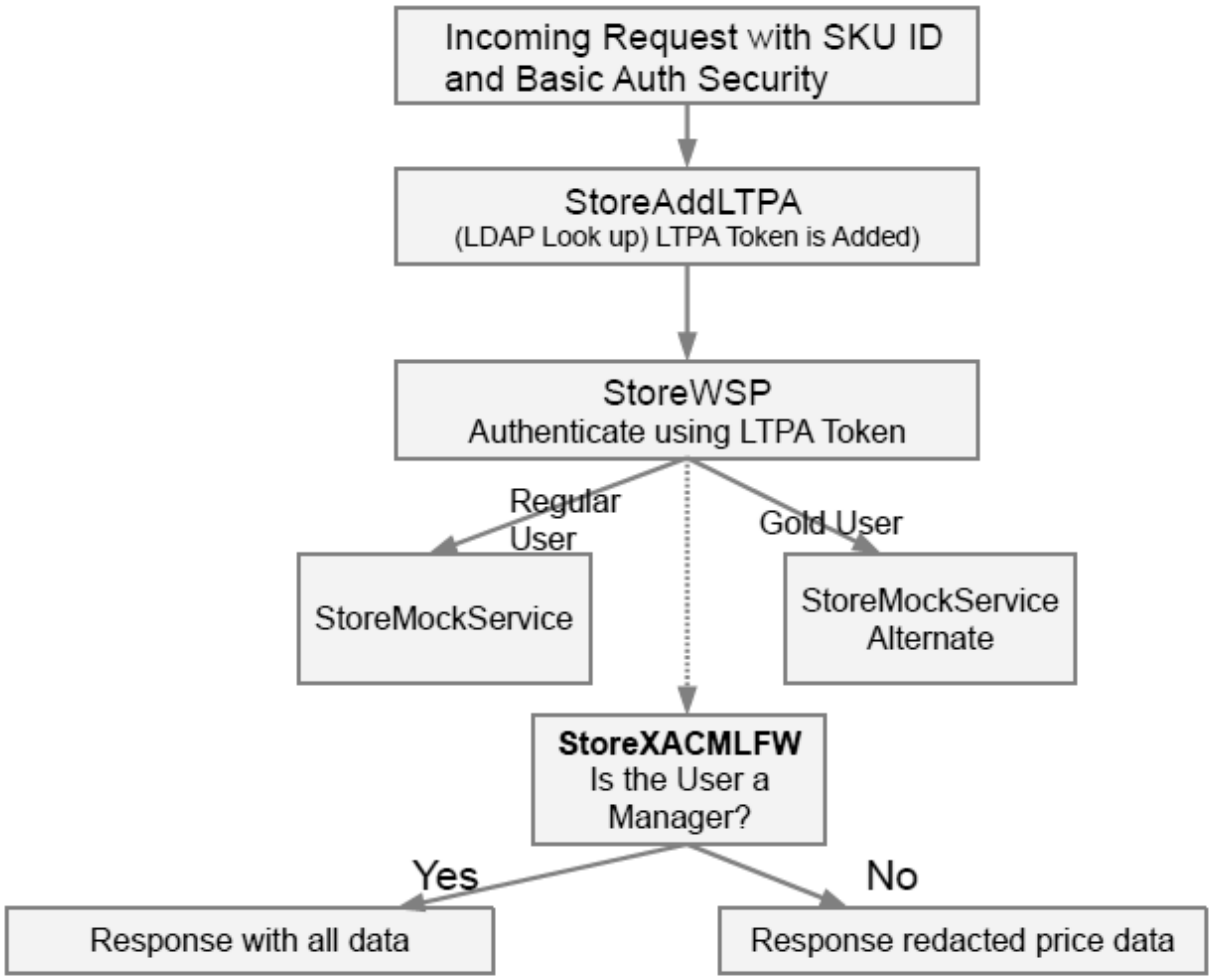


Figura 5. Diagrama de flujo de la aplicación de ejemplo

Tareas relacionadas:

"Clonación y personalización del patrón de pasarela de política SOA de IBM" en la página 79
El patrón de pasarela de política SOA de IBM no se puede editar. Si la topología proporcionada en los patrones de sistema virtual del patrón de pasarela de política SOA de IBM no proporcionan la función que necesita, puede clonar el patrón y editarlo para crear patrones nuevos.

Visión general de los artefactos de WSRR del ejemplo

Los artefactos de WSRR describen la operación de depósito.

Existen funciones empresariales básicas para Warehouse, el cual forma parte de la organización de almacén más amplia de Bob. La versión de servicio, Store V1.0, representa el servicio Store. La definición de nivel de servicio (SLD) de Store tiene dos acuerdos de nivel de servicio (SLA): uno para usuarios Gold que encamina los usuarios hacia un servicio alternativo preferido y un SLA de usuario anónimo que es para todos los demás usuarios y que simplemente registra una notificación en DataPower indicando que se ha realizado la solicitud. La SLD de Store también tiene otras dos políticas de ejemplo 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.

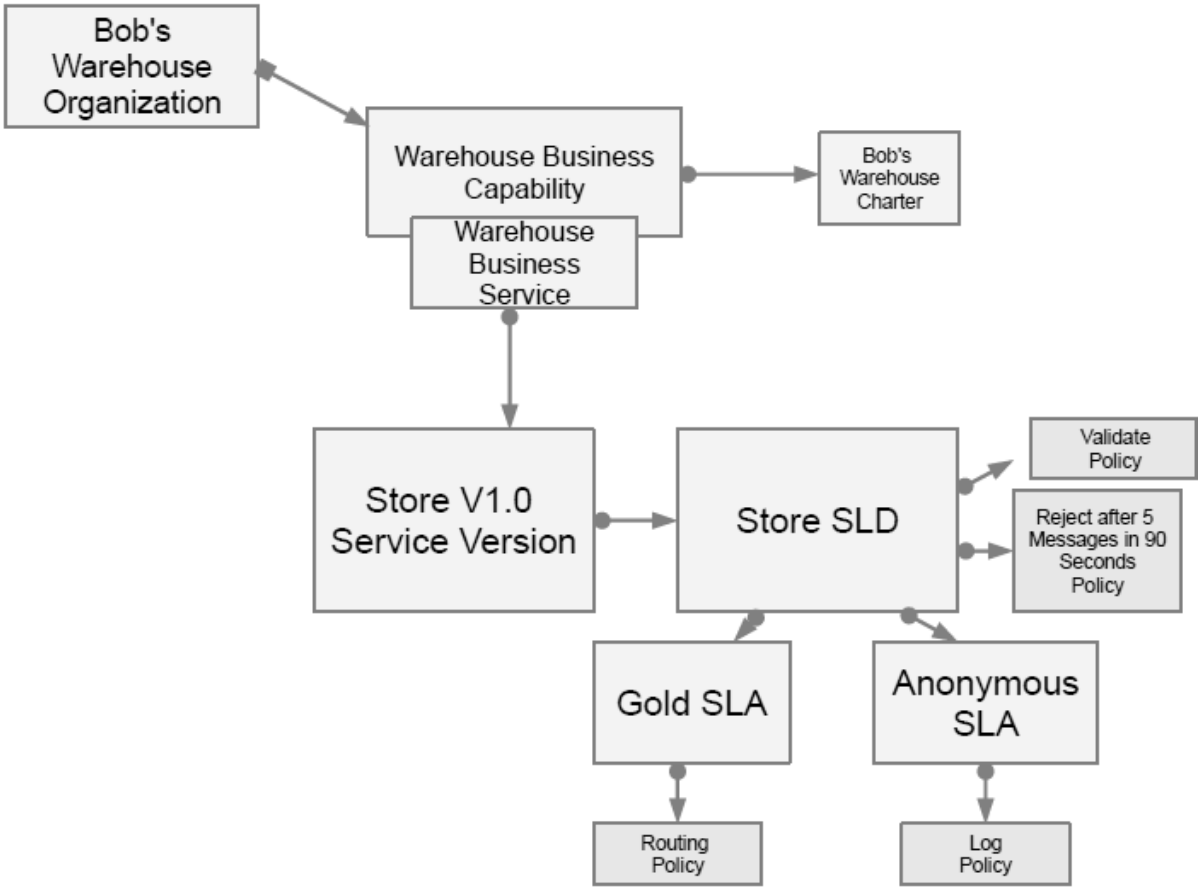


Figura 6. El dominio de ejemplo

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 Ejemplo del tiempo de ejecución básico de la pasarela de política SOA desplegado. Hay seis variaciones de prueba que puede ejecutar en la línea de mandatos para la aplicación de ejemplo.

Para desplegar el tiempo de ejecución de ejemplo básico, consulte "Despliegue del patrón Ejemplo del tiempo de ejecución básico de la pasarela de política SOA" en la página 73.

Nota: el valor de `SamplePolicySample_starting_port` que se utiliza en los ejemplos de XML siguientes se encuentra en los archivos de registro del Ejemplo del tiempo de ejecución básico de la pasarela de política SOA.

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 hacer esto, 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. Se abrirá la pantalla de prueba para la aplicación de ejemplo implementada en DataPower.
4. Las opciones son:
   - **Enviar estándar**: envía una solicitud findInventory al servicio Store. El ID de contexto es un usuario "Silver" . Un resultado exitoso es `Part: SKU10 Price: 461.73`.
   - **Enviar direccionado**: envía una solicitud findInventory al servicio Store. El ID de contexto es un usuario "Gold", por lo que la solicitud se direcciona hacia una implementación Gold del servicio. Un resultado exitoso es `Part: GOLDSKU10 Price: 461.73`.
   - **Enviar no válido**: envía una solicitud con una carga útil no válida. La política de validación solicita que DataPower valide la solicitud. Un resultado exitoso será este mensaje de respuesta de DataPower: `"Error interno (del cliente)"`.
   - **ID de usuario = ConsumerA**: para las llamadas cuyo ID de usuario es ConsumerA, se aplica la política XACML para que sólo los Gestores puedan ver el precio. Se escribirá el valor de Precio en el mensaje de respuesta. Un resultado exitoso contiene `Precio: 0,0`.
   - **Muchas solicitudes estándar**: si se realizan más de 5 solicitudes en el intervalo de 90 segundos, se aplica la política de rechazo. Una respuesta satisfactoria, que muestra la aplicación de la política, es: `Rechazado: "Rechazado (del cliente)"`.
5. Abra la consola de WSRR y explore el servicio y las políticas. Para obtener más información, consulte .

Para ejecutar los casos de prueba de la aplicación de ejemplo utilizando la línea de mandatos:

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 anterior está contenido en el archivo `silver.xml`, ejecute el mandato curl siguiente:

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

En este ejemplo, ConsumerX es Manager, por lo tanto, se visualizará la información de precio completo como 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. Ejecute el mandato curl:

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

Como se puede observar, la respuesta tiene redactado un precio y éste es 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

El SLA ContextId se utiliza para desencadenar la política de direccionamiento. En este caso, el SLA para los Clientes Gold tiene el valor de "Gold" en el SLA. El siguiente es el contenido de la solicitud de ejemplo con Gold como contextIdentifier:

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

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

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

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.wsl 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 se ejecuta la solicitud curl siguiente:

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

Se genera el error siguiente:

```
<?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

Política de mediación incluida en el rechazo de las pruebas de ejemplo cuando el número de mensajes es 5 al cabo de 90 segundos. Ejecute el mandato siguiente 6 veces:

```
curl -k --data-bin @./silver.xml -H "Content-Type: text/xml" -u ConsumerX:passw0rd
http://<yourDataPowerHostName>.com:<SamplePolicySample_starting_port+4>/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, como se muestra a continuación:

```
<?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 generará el error siguiente:

```
<?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: puede ver este error más pronto si ha ejecutado otras pruebas dentro del intervalo de 90 segundos.

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

Cuando contextId no es “Gold”, no hay ningún SLA correlacionado y se utiliza el SLA Anónimo. La política de mediación para el SLA Anónimo es iniciar sesión o avisar. Esto requiere que se habilite la modalidad de depuración para el dominio de ejemplo. Ejecute el siguiente mandato:

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

En este caso ConsumerX es Manager, por lo tanto, se visualizará la información de precio completo, como se muestra a continuación:

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
<soapenv:Header>
<KD4NS:KD4SoapHeaderV2
xmlns:KD4NS="http://www.ibm.com/KD4Soap">AFIAAgAkZmExODgzNTQtY2Q1ZC0zYjU0L
WEyMzItZGM3MmEzNWY0MTAzACRmYWVjYjA1Mi1jMWUxLTMyODEtOWY3Ni0wY2IxNm
RhMDc4MjkAAw==</KD4NS:KD4SoapHeaderV2></soapenv:Header><soapenv:Body><b:fin
dInventoryResponse xmlns:a="http://company.ibm.com/"
xmlns:b="http://company.ibm.com/store">
<findInventoryRes>
<sku>SKU10</sku>
<price>461.73</price>
<inventory>460</inventory>
<msrp>923.46</msrp>
<supplierID>IBM</supplierID>
</findInventoryRes>
</b:findInventoryResponse>
</soapenv:Body>
</soapenv:Envelope>
```

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 ('LogEveryTim
```

Nota: el registro cronológico debe estar establecido en la modalidad de depuración para ver este mensaje. En otro caso, pulse el icono de resolución de problemas en la consola web de DataPower. En la sección Registro, cambie el valor de Nivel de registro a "depuración" y pulse **Establecer nivel de registro**.

Para encontrar el registro, seleccione **Archivos** y **Administración de archivos** > **Gestión de archivos**. El registro se encuentra en la carpeta `logtemp` con el nombre `default-log`. Debido a que el archivo de registro se reinicia, puede ser necesario colocar el archivo de registro en una ventana de navegador web antes de ejecutar la prueba y renovar la pestaña del navegador después de ejecutar la prueba.

Tareas relacionadas:

"Despliegue del patrón Ejemplo del tiempo de ejecución básico de la pasarela de política SOA" en la página 73
Cuando se despliega el patrón Ejemplo del tiempo de ejecución básico de la pasarela de política SOA se crea una instancia de sistema virtual en ejecución del patrón.

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-subje
<!--
************************************************
Starting here, use the MC result as subject.
************************************************
```

sendToPDP.xsl

Esta hoja de estilo invoca el StoreXACMLFW utilizando url-open. La llamada se dirige a otro cortafuegos XML, por lo que no se utiliza ningún perfil proxy SSL. Si se desea mover el punto de decisión de política (PDP) a otro buzón DataPower, se puede 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.xm
xmlns:xacml-context="urn:oasis:names:tc:xacml:2.0:context:schema:os" xmlns:ws="http://docs.oasis-open
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',':',$StoreGWPort,'/rtss/authz/services/AuthzServic
</xsl:variable>
<dp:url-open target="{$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>
```

Si se examina el archivo `sendToPDP.xsl`, se pueden observar los elementos siguientes:

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 crea 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.

El paso siguiente es examinar la redacción de la hoja de estilo de políticas.

StorePrivateDataXACML.xml

```
<PolicySet PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:deny-over
PolicySetId="RPS:StorePrivateData:policy:dc703409-d408-49b3-acc1-16c89c844fce:rolec4a9f664-a0af-45
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:s
/>
</SubjectMatch>
</Subject>
</Subjects>
</Target>
<Policy PolicyId="PPS:StorePrivateData:dc703409-d408-49b3-acc1-16c89c844fce:c4a9f664-a0af-451b-b80
a0af-451b-b80b-1cafdb9fd9f0:pps" RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-a
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-a0a
1cafdb9fd9f0:c4a9f664-a0af-451b-b80b-1cafdb9fd9f0:pps:rules:0">
<Target />
</Rule>
</Policy>
</PolicySet>
</PolicySet>
```

Tenga en cuenta lo siguiente:

- El rol debe ser Manager:

  ```
  <xacml:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string" xmlns:xacml="urn:oasis:na
  ```

- 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

Existen varios puntos en los que puede modificar los scripts `.xsl` utilizados en la aplicación.

Procedimiento

Para modificar las hojas de estilo XSL de ejemplo, puede:

1. Modificar la correlación de credenciales para AZ.

   Abra la hoja de estilo `rgxacml.xsl` y complete las sentencias XSL siguientes:

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

   Las siguientes variables se definen en la hoja de estilo `soavars.xsl`:

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

   El ejemplo contiene una contraseña no cifrada para el servidor LDAP, es posible que desee personalizar la hoja de estilo proporcionada para que se descifre una contraseña cifrada.

   ```
   <!-- Specify base DN to begin search -->
   <xsl:variable name="baseDN">dc=ibm.com</xsl:variable>
   ```

   El `baseDN` está codificado como `dc=ibm.com`. Si ha configurado LDAP con un sufijo diferente, baseDN, cambie esta línea para personalizar el ejemplo.

2. Modifique la hoja de estilo de redacción.

   La hoja de estilo `noPriceInfo.xsl` contiene el código siguiente, que convertirá en cero los valores de precios. 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.

Edición de documentos de política

Utilice la interfaz de usuario de Business Space para editar documentos de política.

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 105.

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” en la página 118.
2. Pulse **Finalizar**. Se abrirá la vista Examinar.

3. 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 120.
   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.

Tareas relacionadas:

“Creación de nuevas políticas” en la página 118
Cuando cree políticas de mediación en la interfaz de usuario de Business Space, especifique las condiciones y acciones para la política.

“Gestión del ciclo de vida de la política” en la página 120
Las políticas se pueden cambiar de un estado de gobierno a otro utilizando la interfaz de usuario de Business Space.

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 plantillas 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 82.
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. Esto incluye las acciones siguientes:
   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 ni algo similar). La regla de proceso de la solicitud:

1. Identifica con la autenticación básica.
2. Autentica con una búsqueda LDAP muy 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 una implementación. Las operaciones findInventory, compra y devolución están todas ellas soportadas. Este servicio se utiliza para mostrar la política de direccionamiento que se aplica.

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 lo siguiente:

1. Realiza la acción AAA utilizando la información SSL para autenticación.
2. Realiza la autorización utilizando un PDP de XACML incluido. La política utilizada por 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 emite una excepción que se maneja mediante la regla de proceso de excepciones y se devuelve una respuesta Denegar al cliente.

Nota: Esta respuesta 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 manualmente. 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 primero es la operación en el servicio web y el segundo 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:denyoverr
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}findInve
cml:AttributeValue>
<ResourceAttributeDesignator AttributeId="urn:ibm:xacml:profiles:web-services:1.0:wsdl:1.1:operati
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}StoreSOA
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</x
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, verá que existen correlaciones similares para Customer y Clerk. Verá 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.

Si examina la hoja de estilo storeCallPDP.xsl, observará lo siguiente:

1. La inclusión de la hoja de estilo storeSendToPDP.xsl. Es la hoja de estilo que 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 es las hojas de estilo allData.xsl o noPriceInfo.xsl.
5. Cuando se examina el XACML para la Reacción, storePrivateDataXACML.xml, vemos que la estructura es casi la misma que la estructura utilizada para 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.c
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-na
        response']/*[local-name()='Envelope']/*[local-name()='Body']/*[local-name()='Response']/*[loc
        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:otherwise>
    </xsl:choose>
  </xsl:template>
</xsl:stylesheet>
```

Artefactos de WSRR creados en el Ejemplo del tiempo de ejecución básico de la pasarela de política SOA

Artefactos de WSRR creados en el patrón Ejemplo del tiempo de ejecución básico de la pasarela de política SOA, cómo el ejemplo los utiliza.

Tabla 33. Artefactos de WSRR creados para el patrón Ejemplo del tiempo de ejecución básico de la pasarela de política SOA

Objeto	Descripción
Organización	Almacén de Bob.
Función empresarial	Warehouse, propiedad de la organización Bob's Warehouse.
Versión de servicio	Store 1.0 utiliza el servicio web Store, la definición de nivel de servicio Store y la función empresarial Warehouse.

Tabla 33. Artefactos de WSRR creados para el patrón Ejemplo del tiempo de ejecución básico de la pasarela de política SOA (continuación)

Objeto	Descripción
WSDL	Store.wsdl
XSD	Company.xsd
Política	• Validate.xml • RouteForGold.xml • LogEveryTime.xml • RejectAfter5MsgIn90Seconds.xml
Archivos adjuntos de políticas	• Anonymous Users_GenericObject_Anonymous Users_LogEveryTime.xml: asocia la política LogEveryTime al Acuerdo de nivel de servicio (SLA) de los usuarios anónimos. • Gold SLA_GenericObject_Gold SLA_RouteForGold.xml: asocia la política RouteForGold al Acuerdo de nivel de servicio Gold. • Store_GenericObject_Store_urn :RejectAfter5MsgIn90Seconds.xml: asocia la política RejectAfter5MsgIn90Seconds a la definición de nivel de servicio Store. • Store_GenericObject_Store_urn :Validate.xml: asocia la política Validate a la definición de nivel de servicio Store.
SLD	Definición de nivel de servicio Store: es utilizada por la versión de servicio Store 1.0.
SLA	Acuerdo de nivel de servicio Gold: direcciona hacia el punto final Gold si ContextId es “Gold”.
Acuerdo de nivel de servicio Anonymous	Usuarios anónimos: utiliza la notificación de política LogEveryTime y se aplica si ContextId no es “Gold”.

Utilización de artefactos de WSRR en la aplicación de ejemplo

StoreWSP utiliza una suscripción WSRR para recuperar artefactos de WSDL y de política. Cuando se procesa una solicitud a través de StoreWSP, se realizan las acciones siguientes:

1. La versión de servicio Store 1.0 se conecta a la definición de nivel de servicio Store, que tiene dos políticas directas asociadas: Validate y RejectAfter5MsgIn90Seconds. El orden en que se ejecutan las políticas es indeterminado.
   a. Si se han producido 5 solicitudes en los últimos 90 segundos se rechaza la solicitud.
   b. La solicitud se valida mediante Store.wsdl con su Company.xsd asociado.
2. El servicio Store 1.0 utiliza la definición de nivel de servicio Store, que tiene dos acuerdos de nivel de servicio: Gold para usuarios Gold, y Anonymous para los demás usuarios. Si el valor del atributo ContextId es “Gold”, la solicitud se direcciona hacia el cortafuegos StoreMockServiceAlternate de XML; si el valor es “Silver” o cualquier otro, se utiliza el acuerdo de nivel de servicio Anonymous y se ejecuta la política LogEveryTime. Esto coloca una notificación en el archivo `default.log` del dominio de ejemplo. Esta notificación solo se puede ver si se ha habilitado la modalidad de depuración en el dominio. A continuación, el mensaje de direcciona hacia el cortafuegos StoreMockService de XML.

Artefactos de DataPower creados en el Ejemplo del tiempo de ejecución básico de la pasarela de política SOA

Artefactos de DataPower creados en el patrón Ejemplo del tiempo de ejecución básico de la pasarela de política SOA

Tabla 34. Artefactos de DataPower creados para el patrón Ejemplo del tiempo de ejecución básico de la pasarela de política SOA

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 de 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, es el certificado predeterminado para un servidor individual, o es el certificado predeterminado de CMSKeyStore en el caso de un entorno ND donde 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. Esto 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` y se encuentran en el directorio local del dominio instalado.

Tabla 35. 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 35. 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 36. 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

Una vez desplegada la imagen del patrón de pasarela de política SOA de IBM, puede registrar sus propias definiciones de servicio y adjuntar sus propias políticas a las definiciones. También puede ver y gestionar los sistemas desplegados. Para ver la lista de instancias desplegadas, pulse **Instancias** > **Sistema virtual**.

Visualización de los detalles de la instancia

Los detalles de una instancia desplegada pueden verse seleccionando una instancia en la lista de instancias de la ventana Instancias del sistema virtual. Los detalles de la instancia de sistema virtual se visualizan a la derecha. Los detalles incluyen una lista de máquinas virtuales suministradas en la infraestructura de nube para este despliegue, la dirección IP, el estado de máquina virtual y el estado de rol. Rol es una unidad de función que el middleware de aplicación virtual ejecuta en una máquina virtual. También puede ver la información del estado de salud del rol de la máquina virtual. Por ejemplo, aparece una marca de selección roja en la flecha de estado de color verde cuando la CPU esté en estado crítico en la 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**. Expanda una máquina virtual en ejecución para ver los registros de scripts en la sección **Paquetes de script** y los enlaces para acceder a la máquina virtual utilizando la sección **Consolas**.

Administración de instancias desplegadas

Después de desplegar un patrón de sistema virtual, puede ver y administrar la instancia de sistema virtual que se ha creado para ver su entorno del patrón de pasarela de política SOA de IBM.

Antes de empezar

Para ver una instancia de sistema virtual, primero debe haber desplegado 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 de pasarela de política SOA de IBM recién suministrado. Cuando el despliegue se completa, se ejecuta la instancia de sistema virtual.

Procedimiento

Para administrar las instancias de sistema virtual del patrón de pasarela de política SOA de IBM, realice los siguientes pasos:

1. Pulse **Instancias** > **Sistemas virtuales** para acceder a la ventana Instancias del sistema virtual.
2. En la lista de instancias de la ventana Instancias del sistema virtual, seleccione el patrón que se ha de desplegar.
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 estén disponibles dependerán del patrón que haya creado. Por ejemplo, puede:
   - Lanzar e iniciar la sesión en la consola administrativa para el gestor de despliegue y, a continuación, ver los clústeres creados.
   - Iniciar el centro de procesos y, a continuación, descargar el diseñador de procesos para crear las aplicaciones de proceso.
   - Configurar IBM Integration Designer y conectar con el centro de procesos para la creación de procesos.

Conexión a WSRR - Business Space

Utilice la interfaz de usuario de Business Space para administrar políticas.

Acerca de esta tarea

Acceder a la interfaz de usuario de Business Space utilizando la dirección de host del sistema WSRR.

Procedimiento

1. Pulse **Instancias** > **Sistemas virtuales** para acceder a la ventana Instancias del sistema virtual.
2. En la lista de instancias de la ventana Instancias del sistema virtual, seleccione el patrón que se ha de desplegar. Se muestran los detalles de la instancia.
3. Acceda al sistema WSRR utilizando la interfaz de usuario de Business Space:
   - En la sección **Consolas**, pulse **WSRR Business Space** para conectar con el Business Space que se ejecuta en el sistema WSRR.
   - Como alternativa, en un navegador Web externo:
     a. Busque el nombre de host y los números de puertos para WSRR. Expanda la sección **Máquinas virtuales** y seleccione la máquina virtual para el servidor autónomo de 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**.
     b. Escriba el URL de Business Space:
        – Para el servidor WSRR autónomo con la seguridad habilitada: `https://<nombrehost>:9443/BusinessSpace`.
        – Para el clúster: `http://<nombrehost>/BusinessSpace`

        donde *<nombrehost>* y *puerto* son el nombre de host y el puerto del servidor WSRR.

Resultados

Se abrirá Business Space, que se puede utilizar para añadir, editar o eliminar políticas.

Qué hacer a continuación

Si utiliza 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 Operaciones.

Información relacionada:

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

Conexión a WSRR - Consola del registro de servicios

Utilice la consola del registro de servicios para clasificar las versiones de servicio.

Acerca de esta tarea

Acceder a la interfaz de usuario de la consola del registro de servicios utilizando la dirección de host del sistema WSRR.

Procedimiento

1. Pulse **Instancias** > **Sistemas virtuales** para acceder a la ventana Instancias del sistema virtual.
2. En la lista de instancias de la ventana Instancias del sistema virtual, seleccione el patrón que se ha de desplegar. Se muestran los detalles de la instancia.
3. Acceda al sistema WSRR :
   - En la sección **Consolas**, pulse **WSRR_Web_UI** para conectar con el Business Space que se ejecuta en el sistema WSRR.
   - Como alternativa, en un navegador Web externo:
     a. Busque el nombre de host y los números de puertos para WSRR. Expanda la sección **Máquinas virtuales** y seleccione la máquina virtual para el servidor autónomo de 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**.
     b. Escriba el URL de la consola del registro de servicios: *nombrehost*/ServiceRegistry

        donde *nombrehost* es el nombre de host del servidor WSRR.

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 104.

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 se ha creado un espacio de gobierno 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 dependerá de lo que se especificó al crear el espacio.

Qué hacer a continuación

Puede añadir acciones adicionales 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**.

Configuración de patrones después del despliegue

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

Cambios de los valores de LDAP para la aplicación de ejemplo

Si está utilizando el Ejemplo del tiempo de ejecución básico de la pasarela de política SOA y necesita cambiar los valores de seguridad para el servidor LDAP; por ejemplo, la contraseña o el nombre de usuario, debe cambiar esos valores en dos lugares.

Los lugares donde realizar los cambios son:

- La sección Autenticación de políticas AAA correspondiente a la política StoreAddLTPA - Para encontrar esta política, utilice la ventana de búsqueda de la interfaz de usuario web de administración de DataPower y busque `AAA`. Seleccione la política AAA correcta y cambie el valor en la pestaña Autenticación.
- El archivo `soavars.xsl` - Utilice la sección Gestión de archivos en la interfaz de usuario web de administración de DataPower. Abra el dominio creado por el patrón de Ejemplo del tiempo de ejecución básico de la pasarela de política SOA en el dispositivo DataPower y busque el archivo `soavars.xsl` en el directorio local. Cambie las variables LDAPHost, LDAPPort, LDAPCN y LDAPPassword según sea necesario.

  Nota: Puede ser necesario reiniciar el dominio para que estos cambios entren en vigor.

Valores de DN de certificado para certificados de DataPower

Cuando SSL se utiliza con el patrón de pasarela de política SOA de IBM proporcionado, la verificación de host de DN es más estricta que la seguridad predeterminada de WebSphere Application Server.

La verificación de host de DN no está habilitada en WebSphere Application Server de forma predeterminada. Pero en los paquetes script utilizados por el patrón de pasarela de política SOA de IBM, la verificación de host de DN está habilitada y no se puede inhabilitar. Un certificado muy específico que funciona entre el WebSphere Application Server predeterminado y DataPower podría no funcionar para el paquete script “SOA Policy Gateway 2.0.0.0 - Seguridad” o el paquete script “ SOA Policy Gateway 2.0.0.0 - Ejemplo” utilizado con el patrón de pasarela de política SOA de IBM; por ejemplo, el nombre distinguido `myserver.yourcompany.com` podría ser aceptado por el WebSphere Application Server predeterminado, pero no por los paquetes script. Para añadir o eliminar los certificados de DataPower utilizados con el despliegue, consulte “Añadir o eliminar certificados DataPower para el almacén de WSRR” en la página 108.

Modificación de las claves LTPA

Este procedimiento describe cómo cambiar la clave LTPA. La clave LTPA se comparte entre todas las células en Básico. No se utiliza en el patrón Ejemplo del tiempo de ejecución básico de la pasarela de política SOA. La clave LTPA se exporta desde el maestro de gobierno y se importa a entornos de ejecución, tales como los de transición, producción o sin definir.

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 es un entorno ND avanzado, complete los pasos siguientes de forma ordenada:
   a. Sincronice todos los nodos.
   b. Detenga el clúster WSRR.
   c. Detenga los agentes de nodo.
   d. Detenga el Dmgr.
4. Si el entorno es Avanzado, se debe reiniciar 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, se debe detener y reiniciar para que el cambio de la clave LTPA entre en vigor.

Añadir o eliminar certificados DataPower para el almacén de WSRR

Esta tarea describe cómo añadir o eliminar certificados de DataPower. Una ventaja de realizar esta tarea es que simplifica la configuración futura de la función de actualización sincronizada entre WSRR y DataPower para las actualizaciones de políticas.

Acerca de esta tarea

Los certificados DataPower como parte de los patrones utilizados por la herramienta curl. Las llamadas a DataPower se cargan en el almacén de confianza predeterminado del nodo o célula. Esto simplifica la configuración futura de la función de actualización sincronizada entre WSRR y DataPower para las actualizaciones de políticas. Si esta posibilidad no es necesaria, este procedimiento describe cómo eliminar los certificados DataPower. Este procedimiento también describe cómo se añaden nuevos certificados DataPower, si se deben cambiar los certificados.

Procedimiento

1. Inicie la sesión en el gestor de despliegue de WSRR o en el WSRR autónomo en `http://nombrehost:9060/admin`. Especifique el usuario y la contraseña.
2. Vaya a **Seguridad, certificados SSL y gestión de claves**.
3. Pulse **Almacenes de claves y certificados**.
4. Pulse **NodeDefaultTrustStore** si selecciona un patrón básico o **CellDefaultTruststore** si selecciona un patrón avanzado.
5. Pulse **Certificados de firmante**.
6. Marque los recuadros de selección de cualquier certificado que desee eliminar.
7. Pulse **Suprimir**.
8. Pulse **Guardar**.
9. Opcional: si necesita añadir nuevos certificados de DataPower, pulse **Añadir** para añadir el nuevo certificado.

Configuración del punto de aplicación de políticas

El dispositivo DataPower es el punto de aplicación de políticas del patrón de pasarela de política SOA de IBM. Una vez desplegado el dominio de aplicación, se puede crear el contenido de dicho dominio.

Procedimiento

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 está en el proceso de creación de la acción de política AAA, o es posible que ya la haya creado antes utilizando el editor de AAA.

   - La identificación es el paso en el que se identifica al usuario. En este ejemplo, se utilizan dos formas de identificación. En el cortafuegos XML StoreAddLTPA, la identificación se realiza con 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 93.
     - 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.

Qué hacer a continuación

Además de crear un dominio y definir la configuración del servidor WSRR en los patrones Tiempo de ejecución avanzado de pasarela de política SOA y Tiempo de ejecución básico de la pasarela de política SOA , se puede el dominio ejecutando un script de CLI personalizado. El script CLI debe estar en la raíz de la estructura del archivo `DomainZipFile.zip`, por ejemplo, `/cli.cli`. El script CLI puede ejecutar cualquier mandato CLI estándar pero todos los artefactos a los que hace referencia CLI deben existir o debe estar accesibles mediante el dominio de DataPower creado por el patrón. Cuando despliegue una instancia de los patrones Tiempo de ejecución avanzado de pasarela de política SOA o Tiempo de ejecución básico de la pasarela de política SOA , se le solicitará el nombre del archivo CLI en los parámetros del paquete de seguridad.

Utilización del patrón Tiempo de ejecución básico de la pasarela de política SOA

El patrón Tiempo de ejecución básico de la pasarela de política SOA consta de tres funciones principales: se obtienen los archivos necesarios para la seguridad entre los scripts de patrón de DataPower y WSRR, se configura un dominio en DataPower, y finalmente se configura la promoción.

Una vez completados esos pasos, se habrán producido las acciones siguientes:

1. Existe un nuevo dominio en el dispositivo DataPower especificado.
2. Existe una definición de servidor WSRR en el dominio.
3. Se ejecuta el script CLI personalizado para el dominio de DataPower.
4. Se configura un servidor WSRR.
5. Los certificados de firmante de DataPower proporcionados por el cliente se cargan en el NodeDefaultTruststore (almacén de claves de confianza) de la célula WSRR.
6. Se configura la promoción entre la célula WSRR del patrón Tiempo de ejecución básico de la pasarela de política SOA y la célula del Maestro de gobierno de pasarela de política SOA.
7. Se intercambian certificados de firmante. El certificado de firmante del gestor de despliegue de gobierno se coloca en el NodeDefaultTrustStore de la célula Básica, y el certificado de firmante del gestor de despliegue de la célula Básica se coloca en el CellDefaultTrustStore de la célula de gobierno.
8. Se intercambian claves de LPTA. La clave de LTPA de la célula de gobierno se importa a la célula Básica.
9. Cada host del clúster WSRR del maestro de gobierno se añade a los dominios de confianza de la célula Básica. Cada host del clúster WSRR de la célula Básica se añade a los dominios de confianza del maestro de gobierno.
10. Se configura el archivo de propiedades de promoción si la célula se ha designado como entorno de transición o de producción en las entradas de datos proporcionadas.

Aunque tendrá que realizar otros pasos para completar un entorno de producción totalmente seguro, la configuración realizada hasta este momento le permite hacer lo siguiente:

1. Crear servicios y políticas y gobernarlos mediante el ciclo de vida de política SOA en WSRR (cuando se han proporcionado entornos de transición y de producción), utilizando el GEP predeterminado.
2. Crear proxies de servicio web que pueden utilizar la definición de servidor WSRR creada previamente para crear suscripciones.

Utilización del patrón Tiempo de ejecución avanzado de pasarela de política SOA

El patrón Tiempo de ejecución avanzado de pasarela de política SOA consta de tres funciones principales: se obtienen los archivos necesarios para la seguridad entre los scripts de patrón de DataPower y WSRR, se configura un dominio en DataPower, y finalmente se configura la promoción.

Una vez completados esos pasos, se habrán producido las acciones siguientes:

1. Existe un nuevo dominio en el dispositivo DataPower especificado.
2. Existe una definición de servidor WSRR en el dominio.
3. Se ejecuta el script CLI personalizado para el dominio de DataPower.
4. Se habrá creado y configurado un entorno en clúster de WSRR con 'n' nodos.
5. Los certificados de firmante de DataPower proporcionados por el cliente se cargan en el CellDefaultTruststore (almacén de claves de confianza) de la célula WSRR.
6. Se configura la promoción entre la célula WSRR del patrón Tiempo de ejecución avanzado de pasarela de política SOA y la célula del Maestro de gobierno de pasarela de política SOA:
   a. Se intercambian certificados de firmante. El certificado de firmante del gestor de despliegue de gobierno se coloca en el CellDefaultTrustStore de la célula Avanzada y el certificado de firmante del gestor de despliegue de la célula Avanzada se coloca en el CellDefaultTrustStore de la célula de gobierno.
   b. Se intercambian claves de LTPA. La clave de LTPA de la célula de gobierno se importa a la célula Avanzada.
   c. Cada host del clúster WSRR del Maestro de gobierno se añade a los dominios de confianza de la célula Avanzada. Cada host del clúster WSRR de la célula Avanzada se añade a los dominios de confianza del Maestro de gobierno.
   d. Se configura el archivo de propiedades de promoción si la célula se ha designado como entorno de transición o de producción en las entradas de datos proporcionadas.

La configuración actual le permite hacer lo siguiente:

1. Crear servicios y políticas y gobernarlos mediante el ciclo de vida de política SOA en WSRR (cuando se han proporcionado entornos de transición y de producción), utilizando el GEP (perfil de habilitación de gobierno) predeterminado.
2. Crear proxies de servicio web que pueden utilizar la definición de servidor WSRR creada previamente para crear suscripciones.

A continuación, debe emprender pasos adicionales para completar un entorno de producción totalmente seguro. Para obtener más información, consulte “Seguridad para los patrones patrón de pasarela de política SOA de IBM” en la página 63.

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

Visión general de los objetos DataPower creados en los patrones Tiempo de ejecución básico de la pasarela de política SOA y Tiempo de ejecución avanzado de pasarela de política SOA, y de su función.

Tabla 37. 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 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.

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 se ha creado el espacio de gobierno SOA, consulte “Configuración de Business Space para utilizarlo por primera vez” en la página 105 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 104
Utilice la interfaz de usuario de Business Space para administrar políticas.

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

WSRR se puede utilizar para crear todas las políticas SOA, incluidas las políticas SLA (Acuerdo de nivel de servicio), las políticas de mediación, las políticas de supervisión, las políticas personalizadas y otros dominios de políticas que estarán soportados en el futuro. 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" en la página 118.

Aserciones de políticas de mediación

Los Acuerdos de nivel de servicio (SLA) deben estar basados en la necesidad que tienen las empresas de que la calidad de un servicio proporcionado cumpla un estándar especificado. 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 deben especificar 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.

Podemos escribir una política que aplique controles de tiempo en la ejecución del servicio y emprenda una acción cuando no se cumpla el acuerdo de nivel de servicio para asegurar su cumplimiento. Por ejemplo, podemos tener un punto final de servicio primario que normalmente puede proporcionar una respuesta de servicio (el 95% de las veces) en 2 segundos. El arquitecto SOA ha creado un punto final secundario en otro servidor que normalmente se utiliza 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. Podemos 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, podemos 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 ha tomado esta decisión 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, podemos tener una situación en la que un servicio hará todo cuanto sea posible, pero cuando determine que está sometido a una carga de trabajo, pondrá en cola o incluso rechazará los mensajes procedentes de servicios de consumidor de prioridad baja. Un ejemplo de una situación de este tipo es cuando una rutina de proceso por lotes inunda el sistema con solicitudes de consumidores en un momento inesperado. Para proteger la calidad del servicio, podemos crear una política 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. No especificar ninguna condición es equivalente a que el resultado de evaluar la condición lógica sea 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 especificadas 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.

  Nota: pulse el hiperenlace xs:date para conocer este estándar.
- **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. (Nota: pulse en el hiperenlace xs:time para comprender 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 el 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 finalizará 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 necesarios, Atributo, Operador y Valor, y 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 38. 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 39. 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.
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.

  Nota: pulse el hiperenlace xs:duration para conocer este estándar
- **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, esto 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 será 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 volverá 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 rechazarán 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 WebSphere DataPower, se grabará 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 seguirán 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 validarán utilizando las gramáticas especificadas. Los mensajes se rechazarán

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 validará. En la tabla siguiente se muestran los valores posibles y su significado:

Tabla 40. 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 el estilo especificado y los parámetros. 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 utilizará 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

Cuando cree políticas de mediación en la interfaz de usuario de Business Space, especifique las condiciones y 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 104.

Se debe crear el espacio de gobierno SOA para poder crear políticas. Si no se ha creado el espacio de gobierno SOA, consulte “Configuración de Business Space para utilizarlo por primera vez” en la página 105 y siga los pasos para crear el espacio.

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 la pestaña 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 113 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 política de la política que acaba de crear, 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.

Conceptos relacionados:

"Políticas" en la página 113
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

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 105.

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.

Acerca de esta tarea

Para obtener más información sobre gobiernos, consulte "Ciclo de vida de política SOA" en la página 4.

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 Navegador de registro de servicio, 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. 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 4
Las políticas de mediación se gobiernan utilizando el ciclo de vida de política SOA. Inicialmente se define 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 durante el despliegue de los patrones en el patrón de pasarela de política SOA de IBM.

Error de conexión con DataPower durante el despliegue

Pruebe las siguientes soluciones:

- Consulte al administrador de DataPower si el usuario y la contraseña son válidos:
  - En DataPower, compruebe si existe el usuario mediante **Panel de control** > **Gestionar cuentas de usuarios**.
  - 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.
- Revise los pasos para las anomalías de conexión SSL, a continuación, para validar que los certificados se han instalado correctamente tanto en el `DomainZipFile.zip` como en el dispositivo DataPower.

Resolución de errores de autenticación de clientes de autenticación mutua

Pruebe las siguientes soluciones:

- Compruebe que el archivo `DomainZipFile.zip` contenía los certificados correctos.
- Compruebe que el perfil criptográfico del puerto de la interfaz de gestión XML tiene credenciales de validación con todos los certificados de la cadena.
- Compruebe que las contraseñas para la clave pública del cliente y el certificado de cliente público sean correctos.

Resolución de errores de autenticación del servidor

Pruebe las siguientes soluciones:

- Compruebe que todos los certificados de la cadena están presentes en el directorio *`yourDataPowerHostName`* del archivo `DominZipFile.zip` que está utilizando.
- Compruebe que el perfil de Proxy SSL tenga un perfil de cifrado inverso que contiene las credenciales de identificación con la cadena de certificados.

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 del error de falta de conexión con un SCP

Pruebe las siguientes soluciones:

- Compruebe que el nombre de host SCP sea correcto.
- Compruebe que el usuario SCP sea correcto.
- Compruebe que la contraseña SCP sea correcta.
- Pruebe manualmente el SCP desde un nodo en el entorno IBM Workload Deployer o IBM PureApplication System con la información suministrada.

Resolución del error de recuperación del archivo `DomainZipFile.zip` desde SCP o de artefactos de depuración no encontrados

Pruebe las siguientes soluciones:

- Compruebe que el archivo `DomainZipFile.zip` exista en el URI.
- Compruebe que el archivo mencionado en el error de registro exista en la ubicación correcta en el archivo `DomainZipFile.zip`. En particular, asegúrese de que los certificados necesarios se encuentran en el directorio correcto.

Resolución de un error de promoción

Hay muchos problemas que pueden surgir en una promoción, incluido el error de conexión con el maestro de gobierno durante el despliegue.

Pruebe las soluciones siguientes:

- 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, y que existan el Tiempo de ejecución básico de la pasarela de política SOA o el Tiempo de ejecución avanzado de pasarela de política SOA.
  - Vaya a cada entorno de ejecución, el Tiempo de ejecución básico de la pasarela de política SOA o el Tiempo de ejecución avanzado de pasarela de política SOA, examine el almacén CellDefaultTrust (para el entorno ND) o el almacén 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 puede encontrarse en la consola ServiceRegistry para el maestro de gobierno :
  - 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 errores de SSL debidos a que faltan certificados de DataPower

Si el nombre de host correcto para su directorio de certificados de DataPower no se ha proporcionado en el archivo `DomainZipFile.zip`, los paquetes script no se podrán conectar al servidor WSRR si está habilitada la autenticación mutua o de servidor en el host DataPower.

Resolución de problemas de conexión de WSRR/DataPower

Si observa que el estado del WSDL en un proxy de servicio web es Inactivo o Sincronizando y nunca cambia a Correcto, compruebe lo siguiente:

1. Compruebe que el certificado de cifrado es válido para el servidor WSRR (WSRRSVR).

2. Compruebe que DataPower tiene el DNS correcto configurado para reconocer el nombre de host del servidor WSRR o Dmgr.
3. Si el DNS es incorrecto, una solución temporal es cambiar el URL en la definición del servidor WSRR para que apunte directamente a la dirección IP. Para ello sustituya el nombre de host del URL por la dirección IP.
4. Vaya a la suscripción de WSRR y realice una sincronización manual:
   a. Examine el archivo `default.log` para ver si hay errores relacionados con la conectividad del servidor WSRR.
5. Asegúrese de que los certificados necesarios coinciden con los de las credenciales de identificación para el perfil de cifrado del perfil de proxy SSL de la interfaz de gestión XML para dispositivos DataPower.

Resolución de problemas en la instancia desplegada

Puede resolver problemas comunes en la instancia desplegada.

No se ha podido conectar con LDAP

Para diagnosticar errores LDAP en el ejemplo, intente las siguientes soluciones:

- En Resolución de problemas del Panel de control de DataPower, asegúrese de que el rastreo esté en la modalidad de depuración.
- Vaya a StoreAddLTPA, abra los detalles de sondeo y habilite el sondeo.
- Ejecute una prueba de cliente.
- Vea los archivos de registro del sondeo. Busque mensajes de error del enlace LDAP.
- Compruebe el nombre de host LDAP.
- Compruebe el DN de LDAP; por ejemplo, cn=root,dc=ibm.com.
- Compruebe la contraseña de LDAP; por ejemplo, passw0rd.
- Compruebe que el puerto LDAP sea 389 y no seguro.
- Compruebe que las contraseñas de entrada para ConsumerX, ConsumerA, ConsumerB sean todas passw0rd. Asegúrese de que la importación de archivos LDIF haya transcrito las contraseñas correctas.

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 la pestaña 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.

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 de script**. Si cualquiera de los paquetes de 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.

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. El arreglo se muestra en el panel izquierdo de la ventana Arreglos de emergencia y la información del arreglo se muestra en el panel derecho.
6. Vaya a la ubicación donde ha almacenado el arreglo y pulse **Cargar**. Para mayor seguridad, sólo se pueden transferir los 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 nuevo, se definen 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.

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 en la ventana Instancias del sistema virtual.

Capítulo 9. Appendices

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.