IBM SOA
Policy Gateway Pattern

Indice

Capitolo 1. Panoramica della politica SOA

La gestione della politica svolge un ruolo chiave nel governare le politiche in modo strutturato e coerente. Le politiche possono essere utilizzate per consentire una migliore governance in qualsiasi ambiente orientata ai servizi.

La politica è un elemento indipendente che può essere applicata a una o molte risorse, includendo servizi differenti. L'assegnazione della politica e di eventuali metadati associati, soprattutto in un ambiente distribuito, può avvenire in diversi punti di applicazione e di decisione.

Architettura della politica SOA

L'architettura della politica SOA descrive l'interazione di PAP (Policy Administration Point), PEP (Policy Enforcement Point), PDP (Policy Decision Point), PIP (Policy Information Point) e PMP (Policy Monitoring Point). Nel pattern, il PAP è fornito da WSRR, il PEP è fornito da WebSphere DataPower e il PMP tramite il componente di monitoraggio DataPower.

L'organizzazione dell'architettura della politica di base e la definizione di quei punti chiave:

- **Policy Administration Point**. Fornisce le capability per la creazione di una politica, la gestione e la governance della politica e relativa assegnazione alle risorse, nonché l'amministrazione dei risultati della politica durante il runtime. Il PAP include un repository per archiviare le politiche. Il PAP è fornito da WSRR.
- **Policy Enforcement Point**. Il PEP (Policy Enforcement Point) è un punto funzionale che viene eseguito sul middleware. Esso esegue le seguenti funzioni:
  - Applica le politiche.
  - Riceve gli aggiornamenti della politica di applicazione e li rende pronti oppure li converte per l'utilizzo.
  - Fornisce le metriche dell'applicazione al PMP (Policy Monitoring Point).
  - Fornisce le funzioni di analisi ed i risultati della politica di applicazione al PAP (Policy Administration Point) e PMP (Policy Monitoring Point).
  - Modifica le posizioni in cui le politiche vengono applicate ed eseguite in base allo stadio del ciclo di vita:
    - Durante la fase di progettazione, WSRR stesso è il punto di applicazione.
    - Durante il runtime, le politiche vengono generalmente applicate dal sistema intermediario sottostante (middleware) che connette i provider dei servizi ai consumer.

  In questo pattern, il PEP è fornito da WebSphere DataPower.
- **Policy Decision Point**. Un PDP (Policy Decision Point) valuta le richieste del partecipante rispetto alle politiche o ai contratti e attributi rilevanti. Il PDP rappresenta un'autorizzazione, idoneità o decisione di convalida per fornire risultati calcolati.
- **Policy Information Point**. Un PIP (Policy Information Point) fornisce informazioni esterne al PDP (Policy Decision Point), ad esempio, le informazioni sull'attributo LDAP o i risultati di un database, con informazioni che devono essere valutate per prendere una decisione politica.

- **Policy Monitoring Point**. Un componente funzionale che fornisce la funzione di monitoraggio della politica dettagliata per l'architettura globale; ad esempio, la panoramica della politica nell'ambiente distribuito. Esso esegue le seguenti funzioni:
  - Ricezione degli aggiornamenti della politica di monitoraggio e loro immediata disponibilità o conversione per l'utilizzo.
  - Cattura dell'analisi delle statistiche e della raccolta in tempo reale per la visualizzazione.
  - Correlazione, analisi e visualizzazione dei dati alimentati dai vari programmi di raccolta in tempo reale, inclusi i PEP (Policy Enforcement Point).
  - Una console di gestione che fornisce visibilità nella gestione della rete distribuita di PEP (Policy Enforcement Point) e lo stato di tali applicazioni.
  - Registrazione, aggregazione di misurazioni ed evidenziazione di eventi significativi come specificato dalla politica di monitoraggio.
  - Fornitura di funzioni di analisi della politica di monitoraggio al PAP (Policy Administration Point) e ai PEP (Policy Enforcement Point).

  In questo pattern, il PMP è fornito dal componente di monitoraggio DataPower.

Il consumer e il provider interagiscono entrambi con il middleware, che a sua volta interagisce con il repository e qualsiasi software di monitoraggio.

Modalità di utilizzo combinato dell'architettura della politica SOA

Il flusso pattern della politica SOA viene mostrato in Figura 1 a pagina 3.

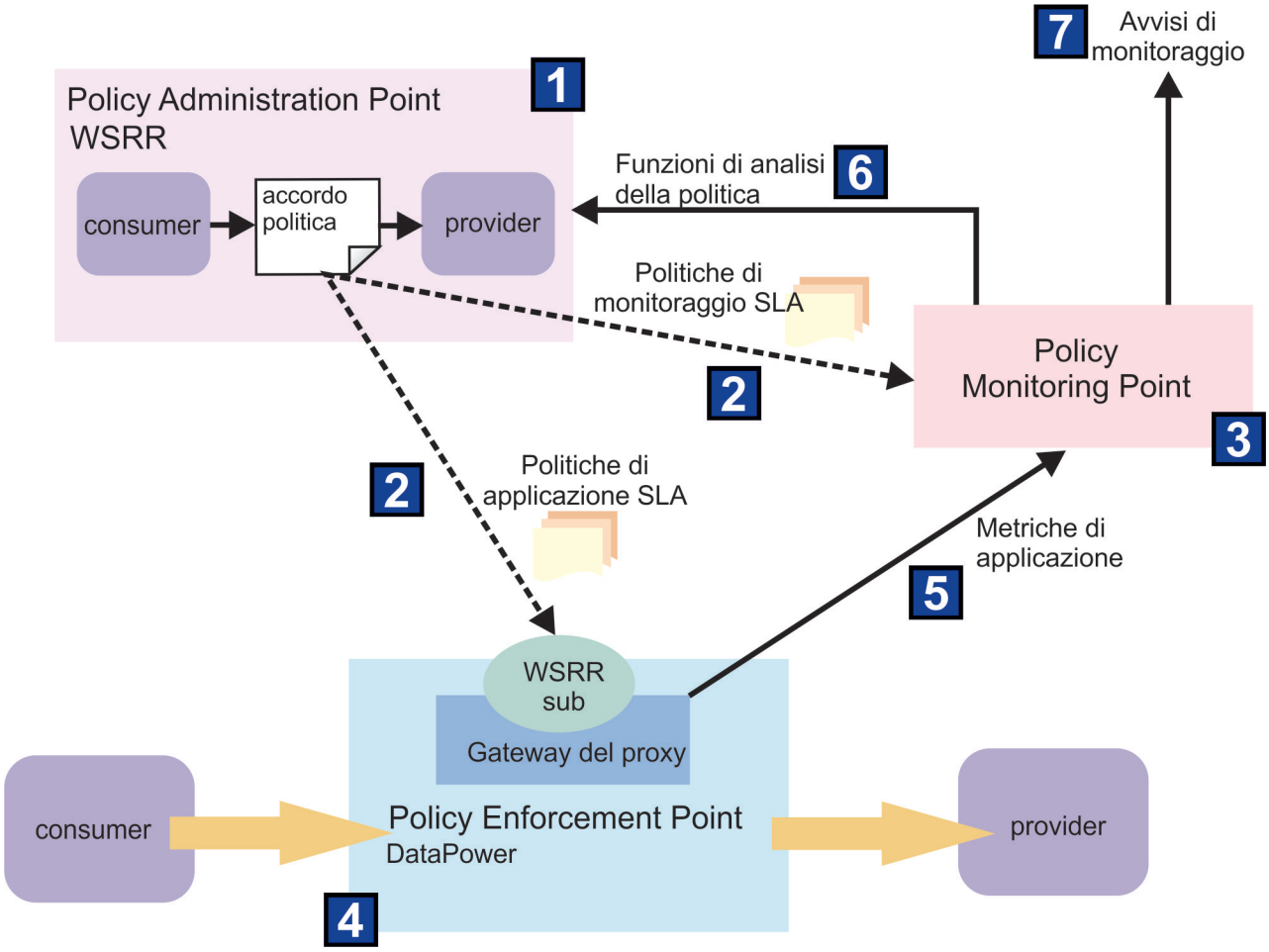


Figura 1. Politica SLA (Service Level Agreement) - Modello di distribuzione SOA

1 Le politiche vengono create e quindi allegate ai servizi che richiedono quella politica. Di solito ha il seguente ordine:

1. L'insieme di servizi vengono caricati o creati nel repository di servizi. Questa azione è una parte del PAP (Policy Administration Point).
2. L'insieme di politiche richieste viene creato nel PAP (Policy Administration Point) utilizzando il ciclo di vita della politica:
   - Le politiche vengono allegate ai servizi che richiedono tali politiche, a livello di servizio, operazione o endpoint come richiesto.

2 Pubblicazione/sottoscrizione automatizzata delle politiche dal PAP (Policy Administration Point) ai PEP (Policy Enforcement Point) e al PMP (Policy Monitoring Point):

1. Come parte della configurazione, il servizio di monitoraggio si sottoscrive alla politica di monitoraggio da WSRR. Questa azione si verifica solo una volta.
2. Come parte della configurazione, i gateway del proxy vengono creati in ogni dispositivo WebSphere DataPower (o dispositivo virtuale) che dispone di transazioni del servizio con applicazione della politica. Questa azione si verifica solo una volta e viene aggiunta o modificata come richiesto.

3. Come parte della configurazione, ogni gateway del proxy nel dispositivo si sottoscrive alle politiche da WSRR per servizi per cui è responsabile. Questa azione si verifica solo una volta e viene aggiunta o modificata come richiesto.
4. Come parte della configurazione, WebSphere DataPower è configurato in modo che le politiche vengano condivise da altri dispositivi in un cluster. Questa azione si verifica solo una volta e viene aggiunta o modificata come richiesto.
5. Il PMP (Policy Monitoring Point) scarica le politiche di monitoraggio quando vengono pubblicate.
6. Il PMP (Policy Monitoring Point) converte le politiche nella rappresentazione interna denominata politiche di situazione.
7. WebSphere DataPower scarica i WSDL per i servizi per cui è responsabile per la transazione.
8. WebSphere DataPower scarica le politiche per i servizi per cui è responsabile quando riceve notifica da WSRR.
9. WebSphere DataPower converte le politiche nella rappresentazione WebSphere DataPower interna nel formato di oggetti SLM.


Monitoraggio delle politiche SOA con l'invio di report e la notifica di operazioni:

1. Le politiche di monitoraggio sono attive nella politica di situazione PMP (Policy Monitoring Point).
2. Il PMP (Policy Monitoring Point) riceve le informazioni di monitoraggio e le colloca negli spazi di lavoro.


Applicazione delle politiche SOA:

1. Le politiche di applicazione sono attive nei diversi dispositivi WebSphere DataPower.
2. WebSphere DataPower riceve le transazioni di servizio e applica le politiche per quel servizio del consumer e del provider.


Il PEP (Policy Enforcement Point) invia le statistiche di applicazione della politica SOA al PMP (Policy Monitoring Point).


Il PMP (Policy Monitoring Point) invia gli eventi di monitoraggio al PAP (Policy Administration Point):

1. Gli eventi vengono configurati nel PAP (Policy Administration Point) che richiede il monitoraggio da parte del PMP (Policy Monitoring Point). Questa azione si verifica solo una volta e viene aggiunta o modificata come richiesto.
2. Poiché le politiche di situazione assumono il valore true, gli eventi vengono inviati al PAP (Policy Authoring Point) dal PMP (Policy Monitoring Point).


Monitoraggio di avvisi:

- Le politiche di situazione vengono eseguite periodicamente e intraprendono un'azione operativa come specificato nella politica. Il valore predefinito è ogni 5 minuti.

Ciclo di vita della politica SOA

Le politiche sono governate dal ciclo di vita della politica SOA. Il ciclo di vita consiste in una identificazione iniziale della politica, in una sua successiva distribuzione in produzione e, infine, quando non più utilizzata, in un suo abbandono.

Per ulteriori informazioni sugli stati e sulle transazioni del ciclo di vita della politica SOA, consultare Centro informazioni di IBM® WebSphere Service Registry and Repository Versione 8.0 - SOA policy lifecycle.

Standard della politica

I gruppi della community tecnica Web, W3C e OASIS, hanno creato degli standard per definire le politiche applicabili ai servizi Web.

- **WS-Policy**: il dominio Web Services Mediation Policy 1.0 definisce un insieme di asserzioni della politica per la descrizione dei requisiti di mediazione per un servizio.
- **Web Services Policy 1.5 - Framework**: definisce un framework e un modello per esprimere le politiche che fanno riferimento alle capability specifiche del dominio, ai requisiti e alle caratteristiche generali delle entità in un sistema basato su servizi Web.

Esempi di specifiche che definiscono le asserzioni di politiche specifiche del dominio:

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

Per ulteriori informazioni su WS-MediationPolicy, consultare ftp://public.dhe.ibm.com/software/solutions/soa/pdfs/WSMediationPolicy1.7-20130506.pdf.

Il modello di dati WS-Policy include le seguenti entità:

- **Politica**: una raccolta non ordinata di “alternative della politica”.
- **Alternativa della politica**: una politica alternativa è una raccolta di “asserzioni di politiche”.
- **Asserzione di politiche**: rappresenta una preferenza individuale; ad esempio, un requisito o una capability.
- **Parametri della politica**: il payload opaco di un'“asserzione di politiche”.
- **Oggetto della politica**: un'entità a cui è possibile collegare un'espressione della politica. Questa entità è utilizzata in un documento WS-PolicyAttachment.

Il seguente esempio, Figura 2 a pagina 6, mostra un'espressione della politica di sicurezza che utilizza le asserzioni definite in WS-Security e 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>
```

Le righe (03-07) rappresentano un'alternativa di politica per la firma di un corpo del messaggio.

Le righe (08-12) rappresentano una seconda alternativa di politica per la codifica di un corpo del messaggio.

Le righe (02-13) mostrano l'operatore della politica `ExactlyOne`. Gli operatori della politica raggruppano le asserzioni di politiche in alternative della politica. Un'interpretazione valida della politica è che il richiamo di un servizio Web firmi o codifichi il corpo del messaggio, ma non entrambe le operazioni.

Figura 2. Utilizzo della politica dei servizi Web con asserzioni della politica di sicurezza.

Figura 3 mostra una definizione delle politiche.

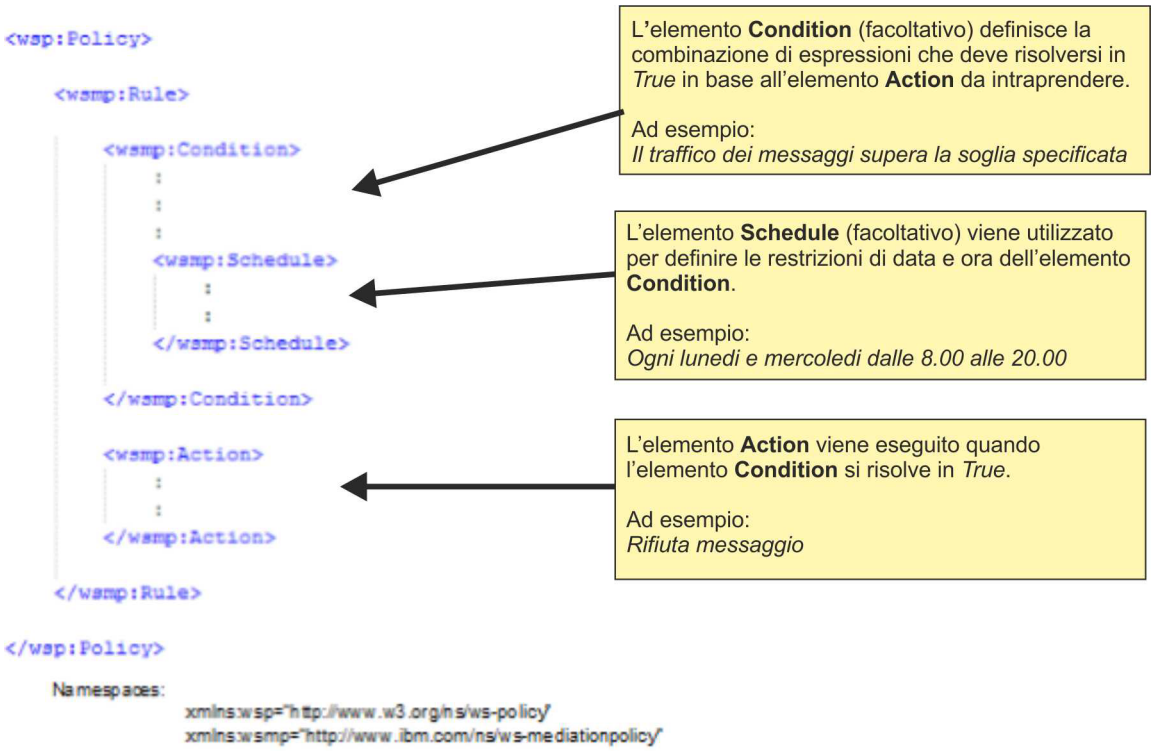


Figura 3. Panoramica sulla struttura della politica

Allegato di politica

Il ruolo del documento allegato di politica consiste nell'associare un insieme di politiche WS-Policy con un punto di allegato specifico del servizio per l'applicazione, ad esempio un punto di allegato dei servizi Web.

Ad esempio, le piattaforme di servizi Web possono supportare i punti di allegati che si basano su:

- Elementi WSDL Element URI 1.1
- Elementi WS-Addressing

La sintassi è definita nella specifica WS-PolicyAttachment:

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


    </wsp:AppliesTo>
    <wsp:Policy>


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

Figura 4. Specifica WS-PolicyAttachment

WSRR espone le interfacce REST per acquisire gli allegati di politica appropriati in un modello SLA. Le informazioni nella coppia Consumer-Provider a cui la politica si applica vengono inoltrate a ESB nel formato WS-PolicyAttachment. La sintassi viene definita nella specifica WS-PolicyAttachment: Message Content Filters.

La politica può essere specificata solo per un servizio del provider, per una coppia consumer-provider specifica o per consumer anonimi. I consumer anonimi forniscono una modalità di definizione di una politica predefinita che si applica solo ai consumer per cui non vengono applicate altre politiche.

In Figura 4, l'oggetto della politica specifica del dominio a cui la politica si applica (il provider) è contenuto nella sezione `<wsp:AppliesTo>`. Esso è seguito dal filtro consumer-context a cui la politica si applica (consumer). Quindi, nella sezione `<wsp:Policy>`, la politica o le politiche vengono dichiarate o riportate come riferimento.

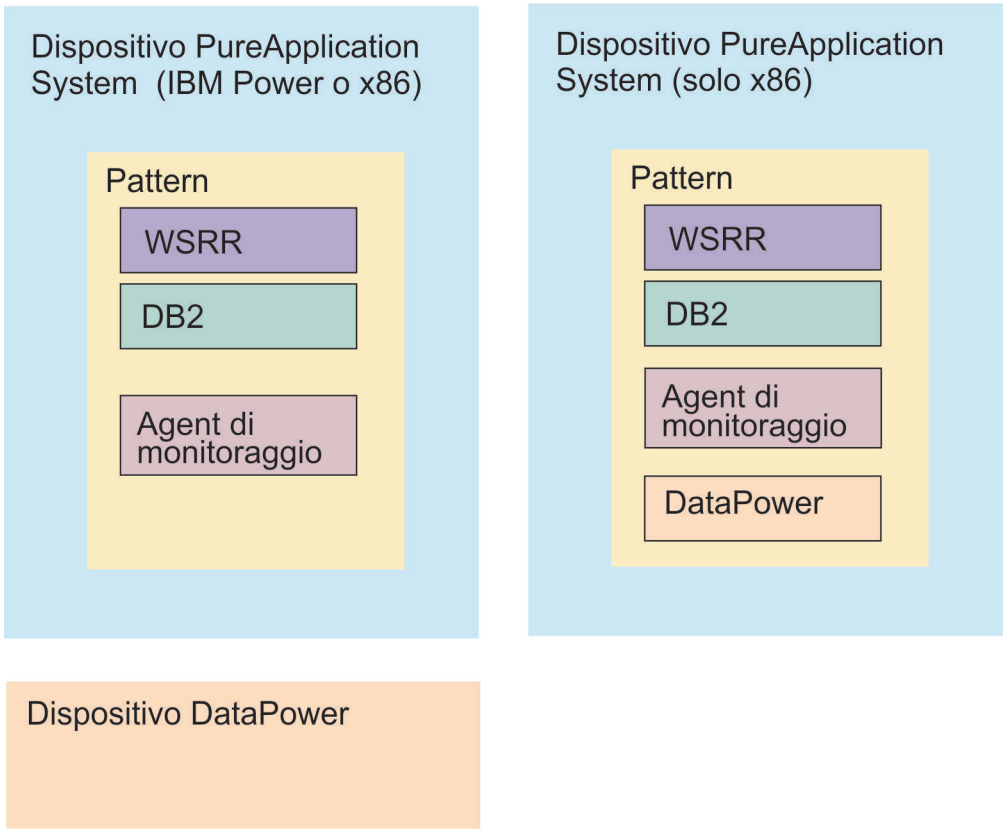
Capitolo 2. Panoramica del pattern

IBM SOA Policy Gateway Pattern è un insieme di pattern del sistema virtuale che forniscono un PEP (policy enforcement point), un PAP (policy administration point) ed un PMP (policy monitoring point).

È possibile installare IBM SOA Policy Gateway Pattern su un dispositivo IBM PureApplication System su architetture IBM Power o x86.

Il PAP (policy administration point) viene fornito dai pattern del sistema virtuale che eseguono il provisioning di WSRR in un'architettura a più livelli, distribuendo un ambiente di produzione e di staging. Il PEP (policy enforcement point) può essere fornito da un dispositivo WebSphere DataPower. In alternativa, su x86, PureApplication System può distribuire un'immagine DataPower virtuale. In entrambi i casi, durante la distribuzione del pattern del sistema virtuale, viene creato un dominio. Il PMP (policy monitoring point) viene fornito da un componente aggiuntivo di monitoraggio al servizio di monitoraggio PureApplication System.

Il diagramma riportato di seguito illustra le capability derivate da IBM SOA Policy Gateway Pattern



Sono presenti esempi di politica in molti, se non in tutti, gli ambienti SOA (Service Oriented Architecture). I produttori ed i consumer del servizio stabiliscono le capability, le prestazioni e le caratteristiche del servizio durante la fase di

progettazione. Per implementare tali accordi, è possibile utilizzare SLD (Service Level Definition) ed SLA (Service Level Agreement). Utilizzare il pattern per definire le politiche per le SLD e gli SLA in modo regolato, definito e gestito in modo efficace. I tipi di politica utilizzati in questo pattern includono le politiche riportate di seguito:

- **Politiche di mediazione** -
  - Rifiuto - Rifiuto o accelerazione delle richieste che arrivano con una frequenza maggiore rispetto a quella definita.
  - Registrazione - Creazione di un messaggio di log con il PEP (policy enforcement point) quando viene richiamato un servizio.
  - Trasformazione.
  - Convalida - Convalida della chiamata di servizio rispetto alla definizione del servizio.
  - Instradamento - In base al messaggio, l'instradamento verso uno specifico endpoint.
- **Politiche di sicurezza**: L'esempio illustra l'applicazione delle politiche di sicurezza del controllo accessi XACML. Tali politiche non sono attualmente gestite all'interno del PAP (policy administration point).
- **Politiche di monitoraggio**: È possibile definire le politiche di monitoraggio in distribuzioni PureApplication System.

IBM SOA Policy Gateway Pattern contiene i pattern del sistema virtuale riportati di seguito:

- SOA Policy Gateway Basic Runtime Sample (solo x86)
- SOA Policy Gateway Governance Master
- SOA Policy Gateway Basic Runtime
- SOA Policy Gateway Basic Runtime External DataPower
- SOA Policy Gateway Advanced Runtime
- SOA Policy Gateway Advanced Runtime External DataPower
- Monitoraggio di sistema per SOA Policy Gateway Pattern 2.5 (un servizio condiviso)

I pattern del sistema virtuale funzionano insieme per fornire un ambiente di governance dei servizi a più fasi. IBM SOA Policy Gateway Pattern, inoltre, consente di eseguire il provisioning di più domini DataPower configurati all'ambiente di governance durante la distribuzione del pattern.

Per ulteriori informazioni relative a SOA Policy, consultare Capitolo 1, “Panoramica della politica SOA”, a pagina 1.

Concetti correlati:

Capitolo 1, “Panoramica della politica SOA”, a pagina 1
La gestione della politica svolge un ruolo chiave nel governare le politiche in modo strutturato e coerente. Le politiche possono essere utilizzate per consentire una migliore governance in qualsiasi ambiente orientata ai servizi.

“SOA Policy Gateway Basic Runtime External DataPower” a pagina 23
Il pattern SOA Policy Gateway Basic Runtime External DataPower è uguale a quello Basic Runtime, ma richiede la specifica del dispositivo DataPower esterno al momento della distribuzione.

“SOA Policy Gateway Basic Runtime Sample (x86)” a pagina 19
SOA Policy Gateway Basic Runtime Sample fornisce un pattern Basic Runtime con un'interfaccia ed un'applicazione di esempio che dimostra le politiche attualmente

supportate in questa release.

"SOA Policy Gateway Governance Master" a pagina 21
Il pattern SOA Policy Gateway Governance Master fornisce un ambiente governance in cluster per l'authoring e la gestione dei servizi e delle politiche. L'ambiente viene fornito con il profilo di abilitazione governance WSRR predefinito configurato. Il profilo di abilitazione governance predefinito supporta due destinazioni della promozione, Staging e Produzione.

"SOA Policy Gateway Advanced Runtime External DataPower" a pagina 27
Il pattern SOA Policy Gateway Advanced Runtime External DataPower è uguale a quello Advanced Runtime, ma richiede la specifica del dispositivo DataPower esterno al momento della distribuzione.

"Monitoraggio di sistema per SOA Policy Gateway" a pagina 29
Il servizio condiviso Monitoraggio di sistema per SOA Policy Gateway fornisce i componenti per il monitoraggio del SOA Policy Gateway.

Capitolo 3. Introduzione a IBM SOA Policy Gateway Pattern

Questo pattern utilizza WebSphere DataPower per controllare i messaggi utilizzando le politiche gestite e le definizioni del servizio in WSRR. Consultare gli argomenti in questa sezione per comprendere come scaricare ed installare il pattern, come verificare il pattern dopo l'installazione, accettare le licenze ed i ruoli utente coinvolti.

Download ed installazione dei pattern

IBM SOA Policy Gateway Pattern da utilizzare con IBM PureApplication System è disponibile per il download da Passport Advantage.

Prima di iniziare

È possibile scaricare IBM SOA Policy Gateway Pattern su un sistema temporaneo, che può essere un sistema Linux o Microsoft Windows. Quindi, è possibile eseguire il programma di installazione sul sistema temporaneo per installare i pattern su IBM PureApplication System.

Verificare che siano disponibili 16 GB di spazio per il file `CIQ1LML.tar.gz` (destinazione Power) o per il file `CIQ1VML.tar.gz` (destinazione x86) ed ulteriori 40 GB per i file estratti. Prima di avviare l'installazione del pattern, è necessario che sia installato anche JRE (Java™ Runtime Environment) Versione 6. È possibile scaricare JRE per Linux dal seguente indirizzo: http://www.ibm.com/developerworks/java/jdk/linux/download.html

Informazioni su questa attività

IBM SOA Policy Gateway Pattern è compresso nel file `CIQ1LML.tar.gz` per un sistema di destinazione Power oppure nel file `CIQ1VML.tar.gz` per un sistema di destinazione x86. Tale archivio contiene i file OVA (open virtual archive), i file del package di script ed i file di definizione del pattern.

Procedura

Per scaricare le immagini di IBM SOA Policy Gateway Pattern da Passport Advantage, effettuare le operazioni riportate di seguito:

1. Accedere al sito Web Passport Advantage: Passport Advantage.
2. Scaricare il file di archivio che contiene le immagini, i package di script ed i pattern da utilizzare. Il file è denominato `CIQ1LML.tar.gz` (destinazione Power) oppure `CIQ1VML.tar.gz` (destinazione x86).
3. Aprire un terminale su Linux oppure un prompt dei comandi su Windows e passare alla directory in cui è stato scaricato il file di archivio.
4. Estrarre il contenuto del file di archivio nel file system locale. In Linux, viene utilizzato il seguente comando di estrazione:

```
tar xvzf archive_file
```

   In Windows, utilizzare un software di estrazione degli archivi per estrarre il contenuto del file di archivio.
5. Passare alla directory `installer`:

```
cd installer
```

6. Per installare IBM SOA Policy Gateway Pattern in IBM PureApplication System, eseguire il programma di installazione. Il nome del comando è `installer.bat` in Microsoft Windows oppure `installer` in Linux. Immettere il comando riportato di seguito: `installer -h <host> -u <username> -p <password>` dove `<host>` è IBM PureApplication System ed username e password sono le credenziali dell'amministratore Cloud. Ad esempio:

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

7. Quando richiesto, accettare la licenza IBM SOA Policy Gateway Pattern.
   a. In Microsoft Windows: una volta accettato l'accordo di licenza, se una nuova riga nel terminale visualizza >>>, immettere `quit()` e premere il tasto Invio. Ripetere il passo 7.
8. I pattern vengono importati. Man mano che ciascun pattern viene installato, viene visualizzato un messaggio nel programma di installazione per indicarne la corretta installazione. Ad esempio:

```
Importazione del pattern "SOA Policy Gateway 2.5.0.0 - Governance Master" ...
Importazione del pattern "SOA Policy Gateway 2.5.0.0 - Governance Master" eseguita correttamente.
```

Risultati

I pattern e gli script vengono caricati e vengono creati i pattern del sistema virtuale.

Nota: Se nel catalogo esiste un pattern del sistema virtuale alla versione corretta utilizzata in IBM SOA Policy Gateway Pattern, non viene sovrascritto.

Operazioni successive

Accettare le licenze in IBM PureApplication System, consultare .

Per convalidare l'installazione, consultare “Verifica del pattern installato”.

Verifica del pattern installato

È possibile verificare che il pattern sia installato correttamente.

Prima di iniziare

Verificare che siano stati completati tutti i passi da “Download ed installazione dei pattern” a pagina 13.

Informazioni su questa attività

Una volta installato il pattern, è possibile verificarne l'installazione per accertarsi che tutte le parti siano installate correttamente.

Procedura

Per verificare l'installazione di IBM SOA Policy Gateway Pattern, effettuare le operazioni riportate di seguito:

1. Aprire Workload Console sul dispositivo su cui è stato installato il pattern.
2. Verificare le immagini virtuali passando a **Catalogo** > **Immagini virtuali** ed individuare i seguenti elementi:
   - DB2 Enterprise 10.1.0.2

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

3. Passare a **Catalogo** > **Package di script** ed individuare:
   - SOA Policy Gateway 2.5.0.0 - DataPower Domain
   - SOA Policy Gateway 2.5.0.0 - DataPower Monitoring (solo x86)
   - SOA Policy Gateway 2.5.0.0 - External DataPower Monitoring
   - SOA Policy Gateway 2.5.0.0 - Promotion
   - SOA Policy Gateway 2.5.0.0 - Sample (solo x86)
   - SOA Policy Gateway 2.5.0.0 - Security
   - SOA Policy Gateway 2.5.0.0 - Add_Named_Queries
   - SOA Policy Gateway 2.5.0.0 - Tear Down

   Questi package di script sono tutti presenti in un'installazione eseguita correttamente.
4. Passare a **Pattern** > **Sistemi virtuali**. Su sistemi x86, individuare:
   - SOA Policy Gateway 2.5.0.0 - Advanced Runtime
   - SOA Policy Gateway 2.5.0.0 - Advanced Runtime External DataPower
   - SOA Policy Gateway 2.5.0.0 - Basic Runtime
   - SOA Policy Gateway 2.5.0.0 - Basic Runtime External DataPower
   - SOA Policy Gateway 2.5.0.0 - Basic Runtime Sample
   - SOA Policy Gateway 2.5.0.0 - Governance Master

   Su Power Systems, individuare:
   - SOA Policy Gateway 2.5.0.0 - Advanced Runtime
   - SOA Policy Gateway 2.5.0.0 - Basic Runtime
   - SOA Policy Gateway 2.5.0.0 - Governance Master

   Questi pattern sono tutti presenti in un'installazione eseguita correttamente.
5. Passare a **Cloud** > **Tipi di pattern** ed individuare il seguente elemento:
   - Monitoraggio di sistema per SOA Policy Gateway Pattern 2.5.0.0

   Questo pattern è presente in un'installazione eseguita correttamente.

Risultati

L'installazione di IBM SOA Policy Gateway Pattern è stata verificata.

Operazioni successive

Se l'installazione è stata eseguita correttamente, è possibile continuare ed accettare le licenze; consultare “Accettazione delle licenze”. Se l'installazione non è stata eseguita correttamente, ripetere la procedura a partire dal passo 7 dell'argomento “Download ed installazione dei pattern” a pagina 13.

Accettazione delle licenze

È necessario accettare le licenze per le parti appena installate prima di poter utilizzare i pattern.

Prima di iniziare

Verificare che siano stati completati tutti i passi da “Download ed installazione dei pattern” a pagina 13.

Informazioni su questa attività

Prima di poter utilizzare qualsiasi immagine virtuale, è necessario accettare la relativa licenza.

Procedura

Per accettare le licenze, effettuare le operazioni riportate di seguito:

1. Aprire Workload Console sul dispositivo su cui è stato installato il pattern.
2. Selezionare **Catalogo** > **Immagini virtuali**.
3. Individuare le seguenti immagini nell'elenco **Immagini virtuali** e confermare che la licenza è stata accettata nel riquadro dei dettagli; in caso contrario, fare clic su 'Accetta' per visualizzare ed accettare la licenza. Per i sistemi x86:
   - WebSphere DataPower XI52 Virtual Edition, Versione 6.0.0.0 - Numero di riferimento immagine: XI52.6.0.0.0231528 (2013/06/16 14:14:19)
   - WebSphere Service Registry and Repository 8.0.0.2 - Numero di riferimento immagine: 201309062038
   - DB2 Enterprise 10.1.0.2 - Numero di riferimento immagine: 39
   - IBM OS Image for Red Hat Linux Systems, versione 2.0.0.3 - Numero di riferimento immagine: 136

   Per sistemi Power:
   - WebSphere Service Registry and Repository 8.0.0.2 - Numero di riferimento immagine: 201309080001
   - DB2 Enterprise 10.1.0.2 - Numero di riferimento immagine: 50
   - IBM OS Image for AIX Systems versione 2.0.0.2 - Numero di riferimento immagine: 126
4. Per accettare una licenza, fare clic sull'immagine per visualizzarne i dettagli. Viene visualizzato lo stato. Fare clic su **Accetta** per l'accordo di licenze, quindi fare clic su tutte le licenze che devono essere accettate prima che sia possibile utilizzare l'immagine virtuale. Una volta completate le operazioni, lo stato viene visualizzato come **Sola lettura** e l'accordo di licenza viene visualizzato come **Accettato**. Se una licenza non è stata accettata, l'icona dell'immagine contiene un riquadro rosso con una croce.

Risultati

Le licenze per IBM SOA Policy Gateway Pattern sono state accettate.

Operazioni successive

Se l'installazione è stata eseguita correttamente e sono state accettate tutte le licenze, è possibile continuare ed utilizzare il pattern; consultare Capitolo 5, “Utilizzo di IBM SOA Policy Gateway Pattern”, a pagina 45. Se l'installazione non è stata eseguita correttamente, ripetere la procedura a partire dal passo 7 dell'argomento “Download ed installazione dei pattern” a pagina 13.

Configurazione dell'accesso utenti

Per consentire agli utenti di accedere alle immagini ed ai pattern sul dispositivo, l'amministratore del dispositivo deve innanzitutto consentire l'accesso utente. È possibile creare prima gli utenti ed aggiungere gli utenti ai gruppi oppure creare prima il gruppo e quindi creare gli utenti ed aggiungerli al gruppo.

Informazioni su questa attività

Gli utenti di gestione, generalmente l'amministratore del dispositivo, possono aggiungere altri utenti che possono accedere e gestire i pattern. Questa operazione viene eseguita utilizzando la console di sistema.

Procedura

Per configurare l'accesso utente, effettuare le operazioni riportate di seguito:

1. Scegliere una delle seguenti opzioni per configurare gli utenti e, come opzione, i gruppi di utente:
   - Aggiungere e configurare un utente dalla finestra Utenti della console.
     a. Dal menu, fare clic su **Sistema** > **Utenti**.
     b. Fare clic sull'icona **Aggiungi**.
     c. Fornire un nome utente breve ed il nome reale dell'utente, l'indirizzo email e le password e fare clic su **OK**.
     d. Selezionare l'utente aggiunto nel pannello Utenti per configurare l'accesso. Configurare l'accesso e le azioni dell'utente selezionato.
     e. Aggiungere l'utente ad uno o più gruppi di utenti nel campo **Gruppi di utenti**.
   - Creare un gruppo di utenti.
     a. Dal menu, fare clic su **Sistema** > **Gruppi di utenti**.
     b. Fare clic sull'icona **Aggiungi**. Fornire un nome ed una descrizione per il gruppo.
     c. Selezionare il gruppo aggiunto nel pannello Gruppi di utenti per configurare l'accesso.
     d. Aggiungere i membri nel campo **Membri del gruppo** e fornire le autorizzazioni da applicare al gruppo.
2. Opzionale: Se sono già state aggiunte le immagini virtuali, fornire l'accesso alle immagini virtuali per gli utenti o il gruppo. Passare a Workload Console e fare clic su **Pattern** > **Sistemi virtuali** per aprire la finestra Pattern del sistema virtuale. Selezionare un'immagine virtuale IBM SOA Policy Gateway Pattern per visualizzarne i dettagli. Aggiungere gli utenti o il gruppo nel campo **Accesso consentito a**.

Operazioni successive

Se le immagini virtuali non sono ancora state aggiunte, aggiungerle e fornire l'accesso agli utenti o al gruppo.

Informazioni correlate:

IBM PureApplication System: Gestione di utenti e gruppi

Capitolo 4. Pattern, parti e package di script

Un pattern fornisce una definizione della topologia per le distribuzioni ripetute che possono essere condivise. Le parti IBM SOA Policy Gateway Pattern sono i componenti funzionali del pattern. Ciascuna parte rappresenta una macchina virtuale singola.

I pattern descrivono la funzione fornita da ciascuna macchina virtuale in un sistema virtuale. Ciascuna funzione è identificata come una parte nel pattern. Pattern acquisiscono le caratteristiche delle relative parti. Ad esempio, quando una parte WSRR viene inserita in un pattern, che viene poi distribuito, il risultato è una macchina virtuale che ha un'istanza WSRR in esecuzione.

Pattern

Quando le immagini virtuali vengono caricate in IBM PureApplication System, e viene assegnato l'accesso agli utenti, questi potranno iniziare ad utilizzare i pattern.

I pattern forniscono una topologia ripetibile che può essere distribuita in un cloud. I pattern distribuiti sono sistemi virtuali eseguiti nel cloud. I pattern, predefiniti o creati, contengono parti. Alcune parti sono necessarie per il funzionamento del pattern al momento della sua distribuzione nel cloud come sistema virtuale.

SOA Policy Gateway Basic Runtime Sample (x86)

SOA Policy Gateway Basic Runtime Sample fornisce un pattern Basic Runtime con un'interfaccia ed un'applicazione di esempio che dimostra le politiche attualmente supportate in questa release.

Il pattern SOA Policy Gateway Basic Runtime Sample è disponibile solo sui sistemi x86.

Il pattern SOA Policy Gateway Basic Runtime Sample è composto delle seguenti parti:

- Server WSRR Standalone
- DB2 Enterprise
- DataPower

Il pattern SOA Policy Gateway Basic Runtime Sample installa le applicazioni di esempio nell'ambiente distribuito. Il pattern installa un dominio di esempio all'interno di DataPower che implementa un servizio di esempio, installa un WSDL di esempio e le politiche allegate in WSRR per il servizio, e fornisce un'applicazione di test per dimostrare le politiche applicate. Per ulteriori informazioni sull'applicazione di esempio, consultare “Applicazione di esempio” a pagina 58. Installa un dominio di esempio all'interno di DataPower, installa un WSDL di esempio e le Politiche in WSRR, e dimostra più politiche rispetto ad un servizio.

Il seguente diagramma mostra il pattern Basic Runtime Sample.

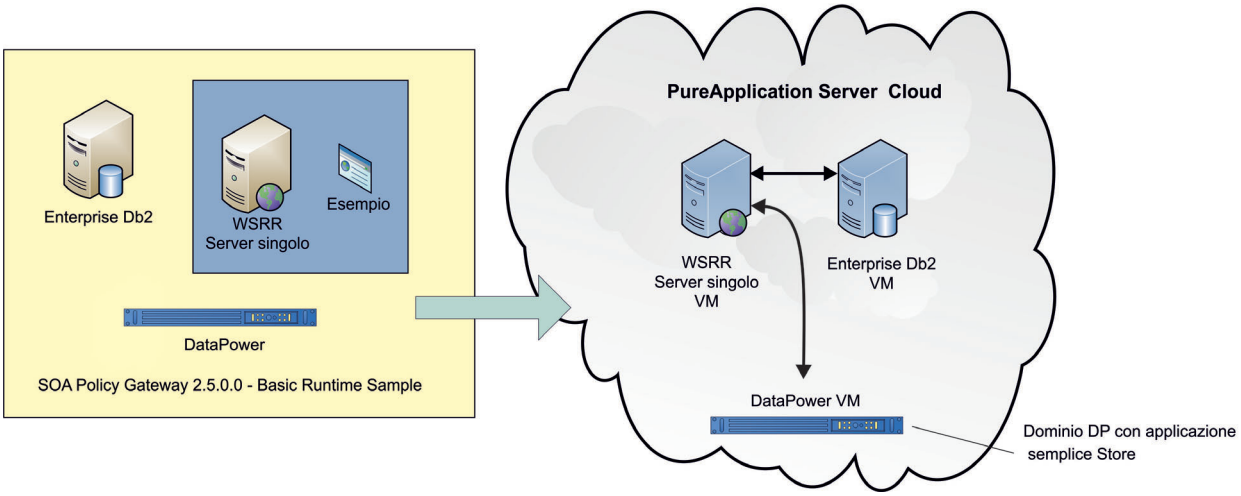


Figura 5. Configurazione del server PureApplication con DataPower VM (solo x86)

Tra le politiche implementate vi sono:

Tabella 1. Politiche incluse nel pattern Basic Runtime Sample

Tipo di politica	Descrizione
Registrazione	Registra la richiesta in DataPower sulla base dell'ID di contesto della richiesta.
Instradamento	Instrada la richiesta verso un endpoint specifico sulla base dell'ID di contesto della richiesta.
Convalida	Convalida la richiesta rispetto al WSDL delle implementazioni del servizio.
Rifiuto	Controlla le richieste indirizzate ad un servizio in base al numero di messaggio con le azioni: reject, queue ed altre.
Sicurezza AAA	Controllo l'accesso al servizio utilizzando l'autorizzazione utente basata su XACML. L'XACML non è memorizzato in WSRR.
Redazione Sicurezza	Redige le parti del messaggio di risposta basato su XACML. L'XACML non è memorizzato in WSRR.

Script ed opzioni avanzate

Il pattern richiede le seguenti parti.

Nella parte del server WSRR Standalone:
- SOA Policy Gateway 2.5.0.0 - Sample

Visualizzare i parametri dello script e della parte:
- “Parte DB2 Enterprise” a pagina 29
- “Parte Server WSRR Standalone” a pagina 35
- “Parte DataPower” a pagina 37
- “Script: SOA Policy Gateway 2.5.0.0 - Sample” a pagina 40

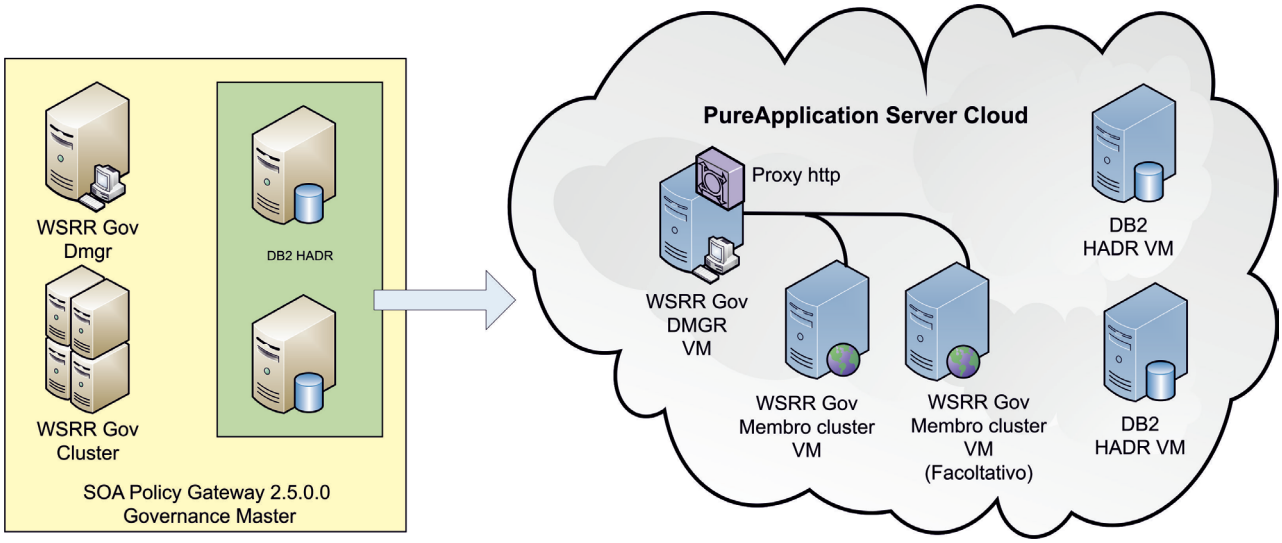
SOA Policy Gateway Governance Master

Il pattern SOA Policy Gateway Governance Master fornisce un ambiente governance in cluster per l'authoring e la gestione dei servizi e delle politiche. L'ambiente viene fornito con il profilo di abilitazione governance WSRR predefinito configurato. Il profilo di abilitazione governance predefinito supporta due destinazioni della promozione, Staging e Produzione.

Il pattern SOA Policy Gateway Governance Master richiede le seguenti parti:

- DB2 HADR Primary
- DB2 HADR Standby
- Gestore distribuzione WSRR
- Nodi personalizzati WSRR

Nota: Il pattern Governance Master deve essere distribuito prima della distribuzione dei di Runtime. I parametri utilizzati per configurare il pattern Governance Master vengono utilizzati dai pattern di runtime per configurare se stessi con il Governance Master.



Parametri della parte

Visualizzare i parametri della parte:

- “Parte DB2 Enterprise HADR Primary” a pagina 31
- “Parte DB2 Enterprise HADR Standby” a pagina 33
- “Parte Gestore distribuzione WSRR” a pagina 36
- “Parte nodi personalizzati WSRR” a pagina 37
- “Script: SOA Policy Gateway 2.5.0.0 - Security” a pagina 42
- “Script: SOA Policy Gateway 2.5.0.0 - Promotion” a pagina 40

Utilizzo del pattern Governance come Governance Master

Il pattern SOA Policy Gateway Governance Master viene distribuito con il profilo WSRR Governance Enablement che contiene due stage di promozione, Staging e Produzione. Per ulteriori informazioni sul profilo Governance Enablement in WSRR, consultare Centro informazioni di IBM WebSphere Service Registry and Repository Versione 8.0 - Governance Enablement Profile. I pattern Basic runtime o

Advanced runtime possono essere distribuiti nell'integrazione come destinazioni della promozione. Per ulteriori informazioni sui destinatari della promozione, consultare “Aggiunta di un ulteriore ambiente di runtime” a pagina 55.

Informazioni correlate:

Centro informazioni di IBM WebSphere Service Registry and Repository Versione 8.0 - Governance Enablement Profile

SOA Policy Gateway Basic Runtime

Il pattern SOA Policy Gateway Basic Runtime rappresenta il modo più semplice di fornire un runtime per SOA Policy Gateway, include due istanze DataPower (solo x86), un'istanza WSRR autonoma, un'istanza autonoma di DB2 ed un'istanza del sistema operativo di base (per ospitare gli agent di monitoraggio di DataPower).

Nota: Questo argomento illustra il pattern disponibile su x86. Per il pattern IBM Power, consultare “SOA Policy Gateway Basic Runtime External DataPower” a pagina 23.

Il pattern SOA Policy Gateway Basic Runtime richiede le seguenti parti:

- Server WSRR Standalone
- DB2 Enterprise
- WebSphere DataPower X152 Virtual Edition
- SOA monitoring for DataPower (in una parte Core OS)

Il seguente diagramma mostra la configurazione del pattern SOA Policy Gateway Basic Runtime.

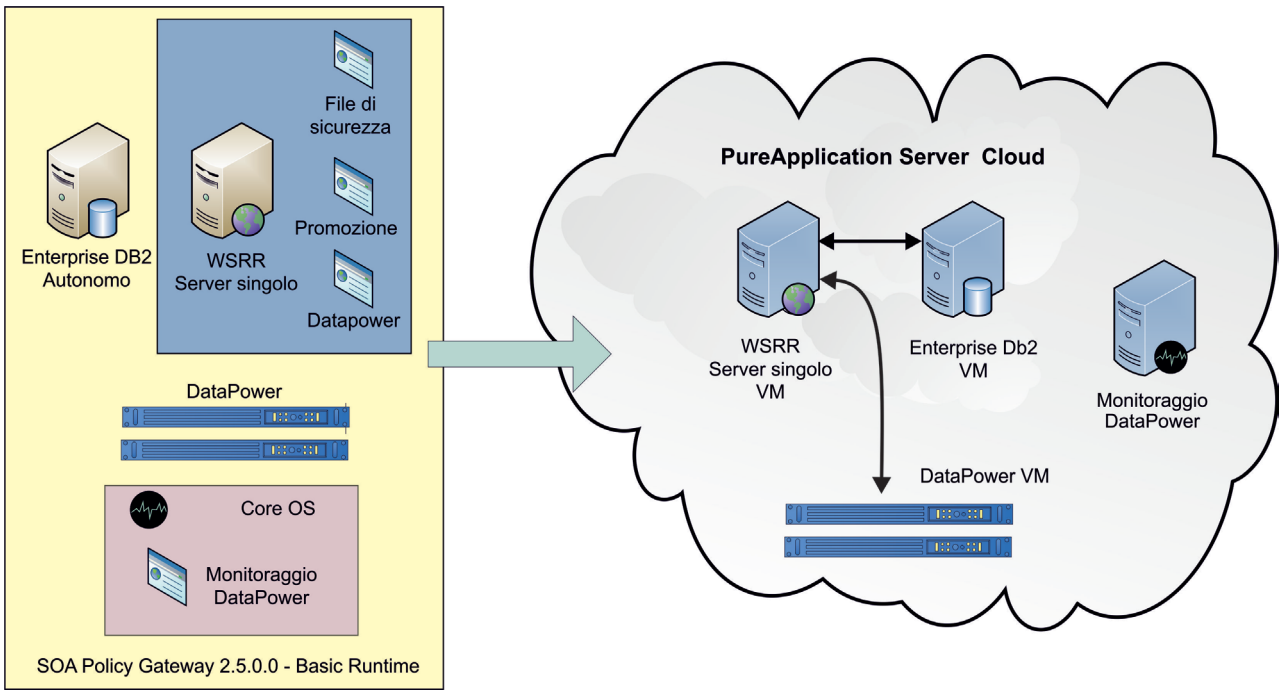


Figura 6. Configurazione di PureApplication Server con DataPower VM

Script ed opzioni avanzate

Il pattern richiede l'input dell'utente per i seguenti script al momento della distribuzione.

Sulla parte del server WSRR Standalone:

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

Nella parte del Core OS:

- SOA Policy Gateway 2.5.0.0 - DataPower Monitoring

Visualizzare i parametri dello script e della parte:

- “Parte Server WSRR Standalone” a pagina 35
- “Parte DB2 Enterprise” a pagina 29
- “Parte DataPower” a pagina 37
- “Script: SOA Policy Gateway 2.5.0.0 - Security” a pagina 42
- “Script: SOA Policy Gateway 2.5.0.0 - Promotion” a pagina 40
- “Script: SOA Policy Gateway 2.5.0.0 - DataPower Domain” a pagina 38
- “Script: SOA Policy Gateway 2.5.0.0 - DataPower Monitoring (solo x86)” a pagina 42

Configurazione di un Basic Runtime con Governance Master

Quando il pattern Basic Runtime viene configurato con un pattern Governance Master si verifica quanto segue:

- La sicurezza tra celle viene configurata
- Il file `promotion.xml` nel Governance Master viene aggiornato con i dati di distribuzione della distribuzione Basic Runtime.

Per configurare la promozione, è necessario scegliere una delle seguenti opzioni stage:

- produzione
- staging

Queste opzioni si allineamento con i livelli forniti dal Profilo di abilitazione governance in WSRR. Per ulteriori informazioni sul profilo di abilitazione governance in WSRR, consultare Centro informazioni di IBM WebSphere Service Registry and Repository Versione 8.0 - Governance Enablement Profile.

Nota: È possibile utilizzare questo pattern per fornire un sistema autonomo, senza un Governance Master. A tale scopo, specificare i parametri Governance Master come “Unset” durante la distribuzione del pattern. Queste impostazioni, determinano la generazione di un errore durante la distribuzione da parte dello script di promozione, e la distribuzione viene visualizzata come **non riuscita**, ma è possibile ignorare questo l'errore.

SOA Policy Gateway Basic Runtime External DataPower

Il pattern SOA Policy Gateway Basic Runtime External DataPower è uguale a quello Basic Runtime, ma richiede la specifica del dispositivo DataPower esterno al momento della distribuzione.

Nota: Questa descrizione si applica al pattern sui sistemi IBM Power.

Il pattern SOA Policy Gateway Basic Runtime External DataPower è composto delle seguenti parti:

- Server WSRR Standalone
- DB2 Enterprise
- SOA monitoring for DataPower (in una parte Core OS)

Il seguente diagramma mostra la configurazione del patternSOA Policy Gateway Basic Runtime External DataPower.

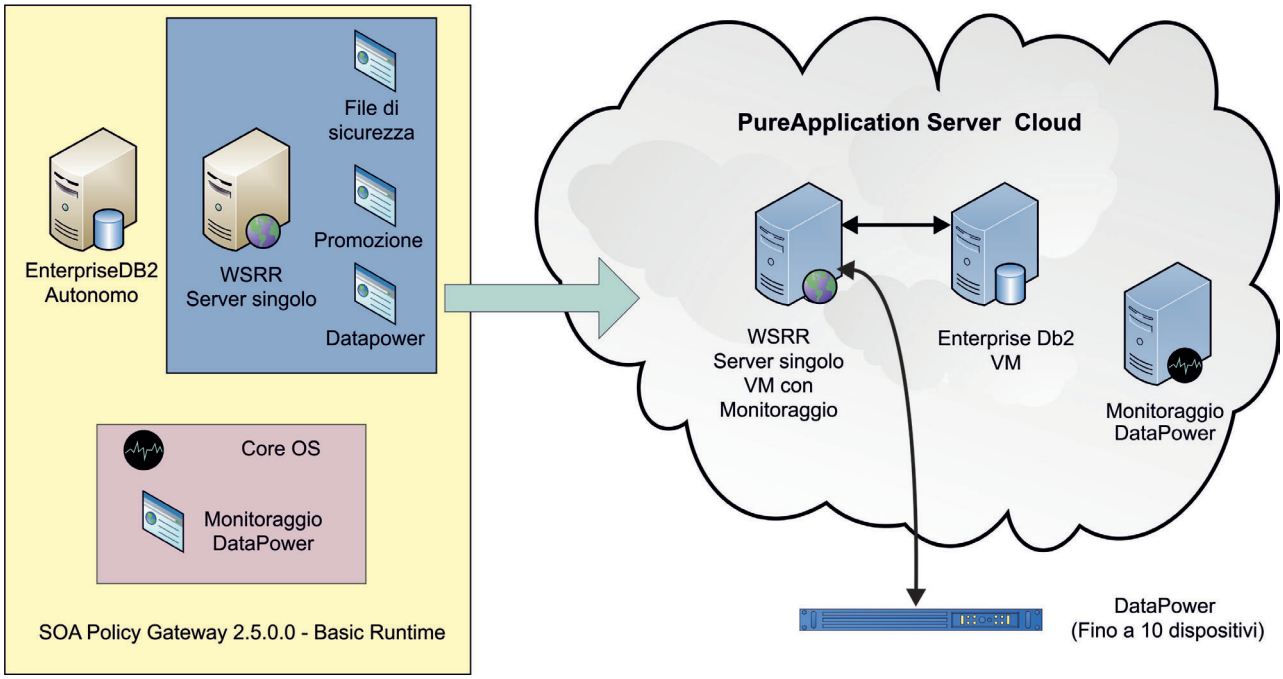


Figura 7. Configurazione di PureApplication Server con il dispositivo DataPower

Script ed opzioni avanzate

Il pattern richiede l'input dell'utente per i seguenti script al momento della distribuzione.

Nella parte del server WSRR Standalone:
- SOA Policy Gateway 2.5.0.0 - Security
- SOA Policy Gateway 2.5.0.0 - Promotion
- SOA Policy Gateway 2.5.0.0 - DataPower Domain

Nella parte del Core OS:
- SOA Policy Gateway 2.5.0.0 - DataPower Monitoring

Visualizzare i parametri dello script e della parte:
- “Parte Server WSRR Standalone” a pagina 35
- “Parte DB2 Enterprise” a pagina 29
- “Script: SOA Policy Gateway 2.5.0.0 - Security” a pagina 42
- “Script: SOA Policy Gateway 2.5.0.0 - Promotion” a pagina 40
- “Script: SOA Policy Gateway 2.5.0.0 - DataPower Domain” a pagina 38
- “Script: SOA Policy Gateway 2.5.0.0 - DataPower Monitoring (solo x86)” a pagina 42

Configurazione di un Basic Runtime con Governance Master

Quando il pattern Basic Runtime viene configurato con un pattern Governance Master si verifica quanto segue:

- La sicurezza tra celle viene configurata
- Il file `promotion.xml` nel Governance Master viene aggiornato con i dati di distribuzione della distribuzione Basic Runtime.

Per configurare la promozione, è necessario scegliere una delle seguenti opzioni stage:

- produzione
- staging

Queste opzioni si allineamento con i livelli forniti dal Profilo di abilitazione governance in WSRR. Se il profilo Governance è diverso, quando viene cambiato il profilo governance di Governance Master, viene scelto "altri". Per ulteriori informazioni sul profilo Governance Enablement in WSRR, consultare Centro informazioni di IBM WebSphere Service Registry and Repository Versione 8.0 - Governance Enablement Profile.

Nota: È possibile utilizzare questo pattern per fornire un sistema autonomo, senza un Governance Master. A tale scopo, specificare i parametri Governance Master come "Unset" durante la distribuzione del pattern. Queste impostazioni, determinano la generazione di un errore durante la distribuzione da parte dello script di promozione, e la distribuzione viene visualizzata come **non riuscita**, ma è possibile ignorare questo l'errore.

SOA Policy Gateway Advanced Runtime

Il pattern SOA Policy Gateway Advanced Runtime comprende due istanze di server DB2 in una configurazione HADR ed un cluster WSRR con un singolo gestore distribuzione e due nodi personalizzati.

Nota: Questo argomento illustra il pattern disponibile su x86. Per il pattern IBM Power, consultare "SOA Policy Gateway Advanced Runtime External DataPower" a pagina 27.

Il pattern richiede le seguenti parti:

- Gestore distribuzione WSRR
- Nodi personalizzati WSRR
- DB2 HADR Primary
- DB2 HADR Standby
- WebSphere DataPower X152 Virtual Edition
- SOA monitoring for DataPower (in una parte Core OS)

Il seguente diagramma mostra la configurazione di un sistema Advanced runtime.

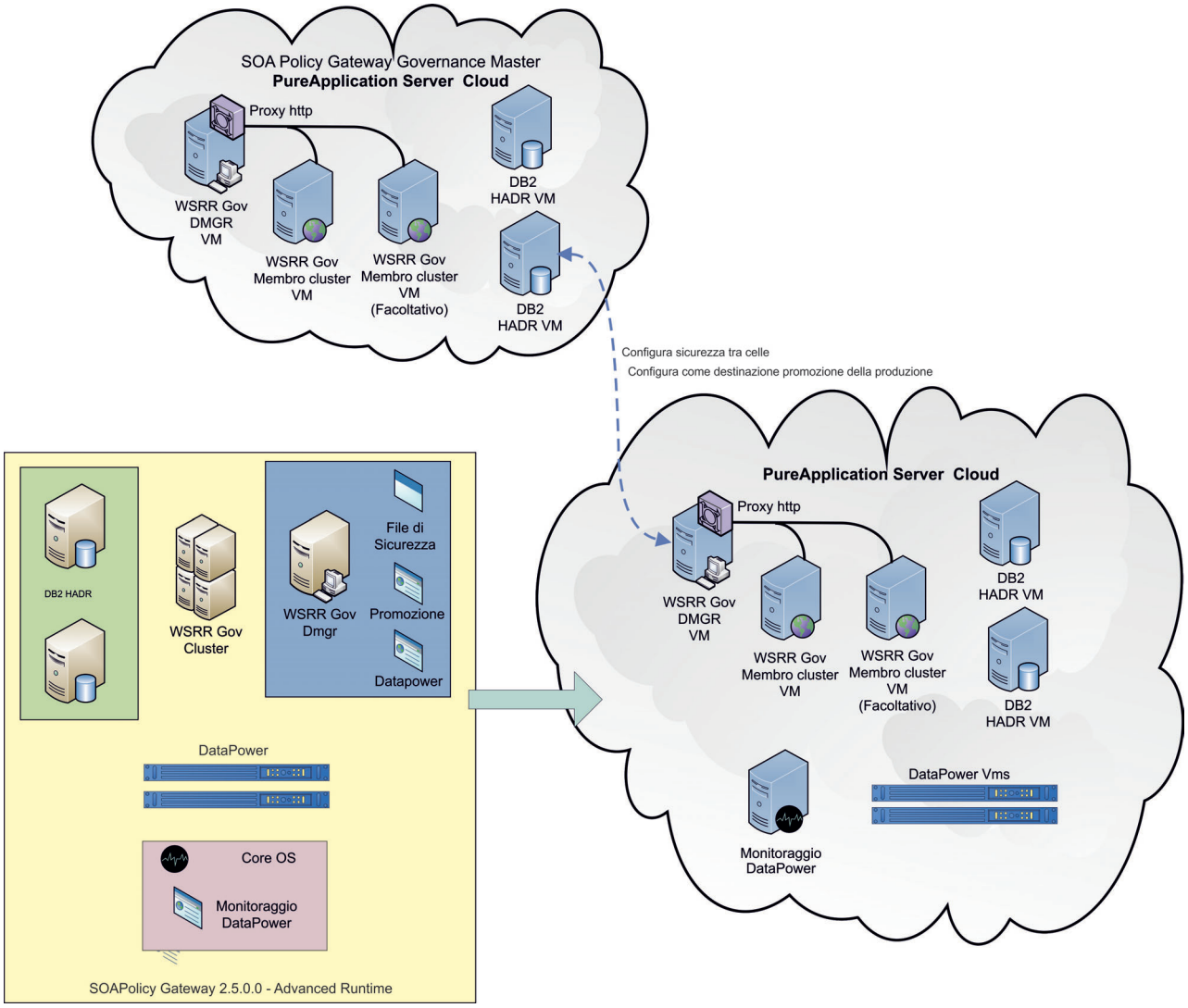


Figura 8. Configurazione di PureApplication Server con DataPower VM

Script ed opzioni avanzate

Il pattern richiede al momento della distribuzione l'input dell'utente nei seguenti script:

Nella parte Gestore distribuzione WSRR:

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

Nella parte del Core OS:

- SOA Policy Gateway 2.5.0.0 - DataPower Monitoring

Visualizzare i parametri dello script e della parte:

- "Parte DB2 Enterprise HADR Primary" a pagina 31
- "Parte DB2 Enterprise HADR Standby" a pagina 33
- "Parte Gestore distribuzione WSRR" a pagina 36

- “Parte nodi personalizzati WSRR” a pagina 37
- “Script: SOA Policy Gateway 2.5.0.0 - Promotion” a pagina 40
- “Script: SOA Policy Gateway 2.5.0.0 - DataPower Domain” a pagina 38
- “Script: SOA Policy Gateway 2.5.0.0 - DataPower Monitoring (solo x86)” a pagina 42

Configurazione di un Advanced Runtime con Governance Master

Quando il pattern Advanced Runtime viene configurato con un pattern Governance Master si verifica quanto segue:

- La sicurezza tra celle viene configurata
- Il file `promotion.xml` nel Governance Master viene aggiornato con i dati della distribuzione Advanced Runtime.

Per configurare la promozione, è necessario scegliere una delle seguenti opzioni stage:

- produzione
- staging

Queste opzioni si allineamento con i livelli forniti dal Profilo di abilitazione governance in WSRR. Per ulteriori informazioni sul profilo Governance Enablement in WSRR, consultare Centro informazioni di IBM WebSphere Service Registry and Repository Versione 8.0 - Governance Enablement Profile.

SOA Policy Gateway Advanced Runtime External DataPower

Il pattern SOA Policy Gateway Advanced Runtime External DataPower è uguale a quello Advanced Runtime, ma richiede la specifica del dispositivo DataPower esterno al momento della distribuzione.

Nota: Questa descrizione si applica al pattern SOA Policy Gateway Advanced Runtime sui sistemi IBM Power.

Il pattern SOA Policy Gateway Advanced Runtime External DataPower richiede le seguenti parti:

- Gestore distribuzione WSRR
- Nodi personalizzati WSRR
- DB2 HADR Primary
- DB2 HADR Standby
- SOA monitoring for DataPower (in una parte Core OS)

Il seguente diagramma mostra la configurazione di un sistema Advanced runtime.

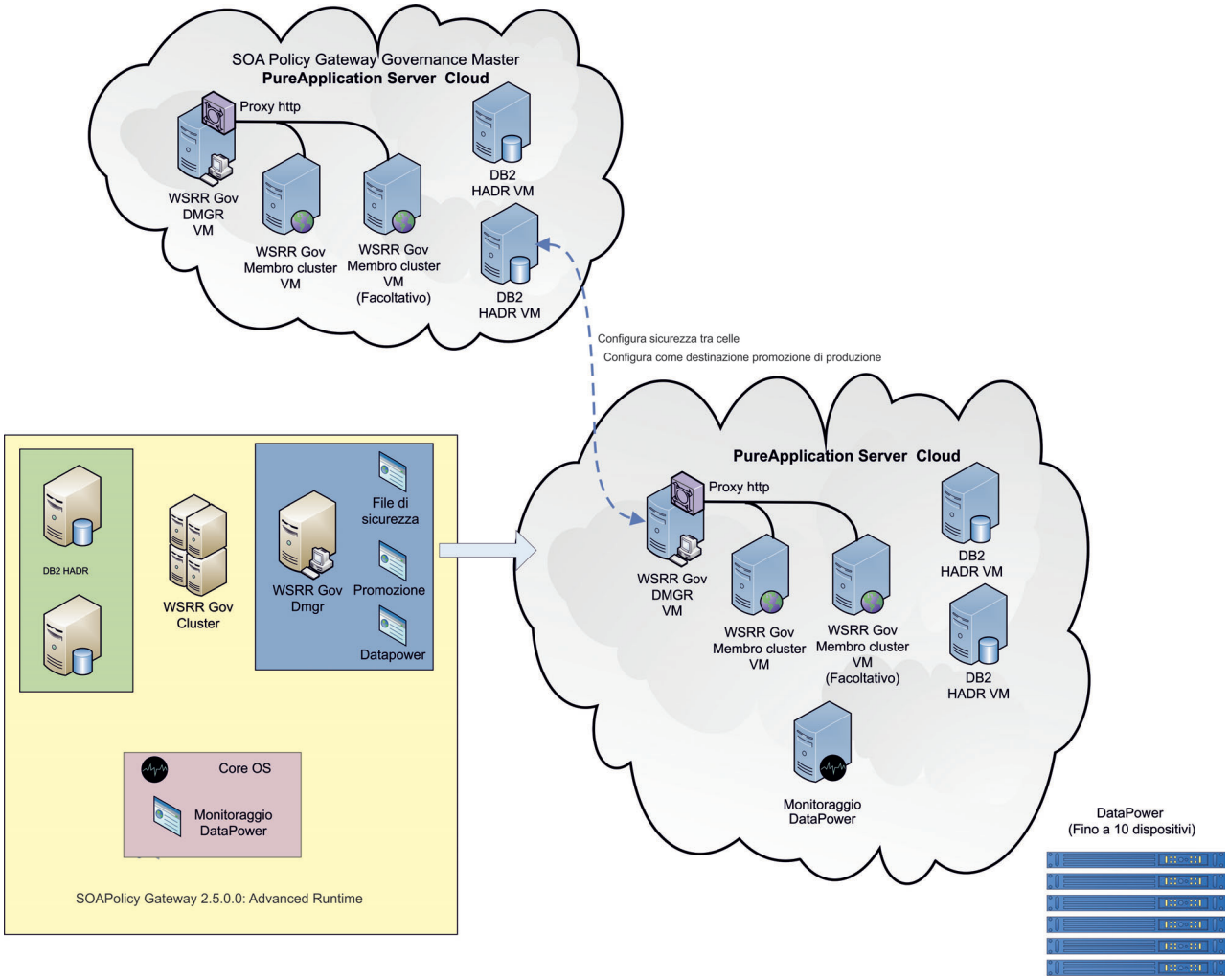


Figura 9. Configurazione di PureApplication Server con dispositivo DataPower

Script ed opzioni avanzate

Il pattern richiede l'input dell'utente per i seguenti script al momento della distribuzione.

Nella parte Gestore distribuzione WSRR:

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

Nella parte del Core OS:

- SOA Policy Gateway 2.5.0.0 - DataPower Monitoring

Visualizzare i parametri dello script e della parte:

- “Parte DB2 Enterprise HADR Primary” a pagina 31
- “Parte DB2 Enterprise HADR Standby” a pagina 33
- “Parte Gestore distribuzione WSRR” a pagina 36
- “Parte nodi personalizzati WSRR” a pagina 37
- “Script: SOA Policy Gateway 2.5.0.0 - Promotion” a pagina 40

- "Script: SOA Policy Gateway 2.5.0.0 - DataPower Domain" a pagina 38
- "Script: SOA Policy Gateway 2.5.0.0 - DataPower Monitoring (solo x86)" a pagina 42

Configurazione di un Advanced Runtime con Governance Master

Quando il pattern Advanced Runtime viene configurato con un Pattern Governance Master si verifica quanto segue:

- La sicurezza tra celle viene configurata
- Il file `promotion.xml` nel Governance Master viene aggiornato con i dati provenienti della distribuzione Advanced Runtime.

Per configurare la promozione, è necessario scegliere una delle seguenti opzioni stage:

- produzione
- staging

Queste opzioni si allineamento con i livelli forniti dal Profilo di abilitazione governance in WSRR. Per ulteriori informazioni sul profilo Governance Enablement in WSRR, consultare Centro informazioni di IBM WebSphere Service Registry and Repository Versione 8.0 - Governance Enablement Profile.

Servizio condiviso

Il pattern include un servizio condiviso utilizzato dai pattern distribuiti per fornire il monitoraggio.

Monitoraggio di sistema per SOA Policy Gateway

Il servizio condiviso Monitoraggio di sistema per SOA Policy Gateway fornisce i componenti per il monitoraggio del SOA Policy Gateway.

Il monitoraggio nei pattern Basic e Advanced è fornito dal servizio di monitoraggio DataPower in esecuzione in una parte Core OS. Il servizio di monitoraggio stesso utilizza i componenti di ITCAM for SOA contenuti nel Monitoraggio di sistema per SOA Policy Gateway Pattern. Monitoraggio delle istanze WSRR richiede inoltre che sia in esecuzione il servizio condiviso Monitoraggio di sistema per WebSphere Application Server.

Seguire il link correlato per la documentazione dettagliata di ITCAM per SOA.

Informazioni correlate:

Documentazione ITCAM for SOA 7.2.1 (in Fix Central)

Parti

Le seguenti parti comprendono IBM SOA Policy Gateway Pattern.

Parte DB2 Enterprise

La parte DB2 Enterprise fornisce alcune opzioni di configurazione.

I parametri configurabili dell'immagine di sistema virtuale DB2 Enterprise 10.1.0.2 sono descritti nella seguente tabella:

Tabella 2. Parametri configurabili

Nome parametro	Valore predefinito	Descrizione
CPU virtuali	1	Il numero di processori virtuali allocati per la macchina virtuale rappresentata da questa parte.
Dimensione di memoria (MB)	2048	La quantità di memoria allocata nella macchina virtuale, in megabyte.
Gruppo proprietario istanza	db2iadm1	Il gruppo a cui appartiene il proprietario dell'istanza DB2.
Proprietario istanza	db2inst1	L'Id del proprietario dell'istanza DB2. Questo ID utente viene utilizzato come proprietario dell'installazione dell'istanza DB2 e come proprietario dei database e degli schemi.
Password (proprietario istanza)	password	La password dell'ID utente db2inst1 del sistema operativo.
Verifica password	password	Verifica la password del proprietario dell'istanza.
Gruppo utenti protetti	db2fadm1	Il gruppo a cui appartiene il proprietario protetto DB2.
Utente protetto	db2fenc1	L'Id dell'utente protetto DB2. L'ID utente protetto viene utilizzato per eseguire funzioni definite dall'utente (UDF) e procedure memorizzate al di fuori dello spazio indirizzi utilizzato dal database DB2. L'utente protetto è un utente con cui le procedure memorizzate "protette" possono essere eseguite con un'autorizzazione di sistema operativo ridotta.
Password (db2fenc1)		La password dell'ID utente protetto
Verifica password		Verifica la password dell'utente protetto.
Gruppo utente DAS	dasadm1	Il gruppo a cui appartiene il proprietario DAS DB2.
Utente DAS	dasusr1	L'ID dell'utente del server delle applicazioni DB2 utilizzato per eseguire il server delle applicazioni DB2 sul sistema. Questo ID utente viene utilizzato anche dagli strumenti della GUI DB2 per l'esecuzione delle attività di amministrazione delle istanze di database e sui database del server locale.
Password (utente DAS)	password	La password dell'utente DAS.
Verifica password	password	Verifica la password dasusr1.
Porta del servizio DB2	50000	La porta è bloccata e non può essere modificata.

Tabella 2. Parametri configurabili (Continua)

Nome parametro	Valore predefinito	Descrizione
Creazione del database	Create-new-database	Il valore è bloccato e non può essere modificato.
Nome del nuovo database	WSRR	Il valore è bloccato e non può essere modificato.
Codeset del nuovo database	UTF-8	
Territorio del nuovo database	US	
Collation del nuovo database	SYSTEM	
Dimensione pagina del nuovo database	32768	Il valore è bloccato e non può essere modificato.
Modalità di compatibilità DB2	Default	Il valore è bloccato e non può essere modificato.
Configurare tutti i dischi raw per essere utilizzati DB2	NO	
Password (root)		La password dell'ID utente root. La password del sistema operativo della macchina virtuale che è rappresentata da questa parte nel pattern.
Verifica password		Verifica la password di root.
Password (virtuser)		La password dell'ID utente virtuser del sistema operativo. Questo ID utente viene utilizzato come un ID utente non root della macchina virtuale.
Verifica password		Verifica la password virtuser.
Abilita VNC	True	Il valore è bloccato e non può essere modificato.

Parte DB2 Enterprise HADR Primary

La parte DB2 Enterprise HADR Primary fornisce alcune opzioni di configurazione.

I parametri configurabili della parte DB2 Enterprise HADR Primary sono descritti nella seguente tabella:

Tabella 3. Parametri configurabili

Nome parametro	Valore predefinito	Descrizione
CPU virtuali	1	Il numero di processori virtuali allocati per la macchina virtuale rappresentata da questa parte.
Dimensione di memoria (MB)	2048	La quantità di memoria allocata nella macchina virtuale, in megabyte.
Gruppo proprietario istanza	db2iadm1	Il gruppo a cui appartiene il proprietario dell'istanza DB2.

Tabella 3. Parametri configurabili (Continua)

Nome parametro	Valore predefinito	Descrizione
Proprietario istanza	db2inst1	L'Id del proprietario dell'istanza DB2. Questo ID utente viene utilizzato come proprietario dell'installazione dell'istanza DB2 e come proprietario dei database e degli schemi.
Password (proprietario istanza)	password	La password dell'ID utente db2inst1 del sistema operativo.
Verifica password	password	Verifica la password del proprietario dell'istanza.
Gruppo utenti protetti	db2fadm1	Il gruppo a cui appartiene il proprietario protetto DB2.
Utente protetto	db2fenc1	L'Id dell'utente protetto DB2. L'ID utente protetto viene utilizzato per eseguire funzioni definite dall'utente (UDF) e procedure memorizzate al di fuori dello spazio indirizzi utilizzato dal database DB2. L'utente protetto è un utente con cui le procedure memorizzate "protette" possono essere eseguite con un'autorizzazione di sistema operativo ridotta.
Password (db2fenc1)		La password dell'ID utente protetto
Verifica password		Verifica la password dell'utente protetto.
Gruppo utente DAS	dasadm1	Il gruppo a cui appartiene il proprietario DAS DB2.
Utente DAS	dasusr1	L'ID dell'utente del server delle applicazioni DB2 utilizzato per eseguire il server delle applicazioni DB2 sul sistema. Questo ID utente viene utilizzato anche dagli strumenti della GUI DB2 per l'esecuzione delle attività di amministrazione delle istanze di database e sui database del server locale.
Password (utente DAS)	password	La password dell'utente DAS.
Verifica password	password	Verifica la password di dasusr1.
Porta del servizio DB2	50000	La porta è bloccata e non può essere modificata.
Creazione del database	Create-new-database	Il valore è bloccato e non può essere modificato.
Nome del nuovo database	WSRR	Il valore è bloccato e non può essere modificato.
Codeset del nuovo database	UTF-8	
Territorio del nuovo database	US	
Collation del nuovo database	SYSTEM	

Tabella 3. Parametri configurabili (Continua)

Nome parametro	Valore predefinito	Descrizione
Dimensione pagina del nuovo database	32768	Il valore è bloccato e non può essere modificato.
Modalità di compatibilità DB2	Default	Il valore è bloccato e non può essere modificato.
Configurare tutti i dischi raw per essere utilizzati DB2	NO	
Password (root)		La password dell'ID utente root. La password del sistema operativo della macchina virtuale che è rappresentata da questa parte nel pattern.
Verifica password		Verifica la password di root.
Password (virtuser)		La password dell'ID utente virtuser del sistema operativo. Questo ID utente viene utilizzato come un ID utente non root della macchina virtuale.
Verifica password		Verifica la password virtuser.
Abilita VNC	True	Il valore è bloccato e non può essere modificato.

Altri parametri sono ereditate dal pattern di sistema virtuale di base e sono bloccati.

Parte DB2 Enterprise HADR Standby

La parte DB2 Enterprise HADR Standby fornisce alcune opzioni di configurazione.

Tabella 4. Parametri configurabili

Nome parametro	Valore predefinito	Descrizione
CPU virtuali	1	Il numero di processori virtuali allocati per la macchina virtuale rappresentata da questa parte.
Dimensione di memoria (MB)	2048	La quantità di memoria allocata nella macchina virtuale, in megabyte.
Gruppo proprietario istanza	db2iadm1	Il gruppo a cui appartiene il proprietario dell'istanza DB2.
Proprietario istanza	db2inst1	L'Id del proprietario dell'istanza DB2. Questo ID utente viene utilizzato come proprietario dell'installazione dell'istanza DB2 e come proprietario dei database e degli schemi.
Password (proprietario istanza)	password	La password dell'ID utente db2inst1 del sistema operativo.
Verifica password	password	Verifica la password del proprietario dell'istanza.
Gruppo utenti protetti	db2fadm1	Il gruppo a cui appartiene il proprietario protetto DB2.

Tabella 4. Parametri configurabili (Continua)

Nome parametro	Valore predefinito	Descrizione
Utente protetto	db2fenc1	L'Id dell'utente protetto DB2. L'ID utente protetto viene utilizzato per eseguire funzioni definite dall'utente (UDF) e procedure memorizzate al di fuori dello spazio indirizzi utilizzato dal database DB2. L'utente protetto è un utente con cui le procedure memorizzate "protette" possono essere eseguite con un'autorizzazione di sistema operativo ridotta.
Password (db2fenc1)		La password dell'ID utente protetto
Verifica password		Verifica la password dell'utente protetto.
Gruppo utente DAS	dasadm1	Il gruppo a cui appartiene il proprietario DAS DB2.
Utente DAS	dasusr1	L'ID dell'utente del server delle applicazioni DB2 utilizzato per eseguire il server delle applicazioni DB2 sul sistema. Questo ID utente viene utilizzato anche dagli strumenti della GUI DB2 per l'esecuzione delle attività di amministrazione delle istanze di database e sui database del server locale.
Password (utente DAS)	password	La password dell'utente DAS.
Verifica password	password	Verifica la password dasusr1.
Porta del servizio DB2	50000	La porta è bloccata e non può essere modificata.
Creazione del database	Create-new-database	Il valore è bloccato e non può essere modificato.
Nome del nuovo database	WSRR	Il valore è bloccato e non può essere modificato.
Codeset del nuovo database	UTF-8	
Territorio del nuovo database	US	
Collation del nuovo database	SYSTEM	
Dimensione pagina del nuovo database	32768	Il valore è bloccato e non può essere modificato.
Modalità di compatibilità DB2	Default	Il valore è bloccato e non può essere modificato.
Configurare tutti i dischi raw per essere utilizzati DB2	NO	
Password (root)		La password dell'ID utente root. La password del sistema operativo della macchina virtuale che è rappresentata da questa parte nel pattern.
Verifica password		Verifica la password di root.

Tabella 4. Parametri configurabili (Continua)

Nome parametro	Valore predefinito	Descrizione
Password (virtuser)		La password dell'ID utente virtuser del sistema operativo. Questo ID utente viene utilizzato come un ID utente non root della macchina virtuale.
Verifica password		Verifica la password virtuser.
Abilita VNC	True	Il valore è bloccato e non può essere modificato.

Altri parametri sono ereditate dal pattern di sistema virtuale di base e sono bloccati.

Parte Server WSRR Standalone

La parte Server WSRR Standalone fornisce alcune opzioni di configurazione.

I parametri configurabili della parte Server WSRR Standalone sono descritti nella seguente tabella:

Tabella 5. Parametri configurati

Nome parametro	Valore predefinito	Descrizione
CPU virtuali	1	Il numero di processori virtuali allocati per la macchina virtuale rappresentata da questa parte.
Dimensione di memoria (MB)	4096	La quantità di memoria allocata nella macchina virtuale, in megabyte.
Nome cella	Impostato con uno dei seguenti valori: • SOAPolicySampleCell (Pattern basic runtime sample) • SOAPolicyBasicCell (Pattern basic runtime) • SOAPolicyBasicCell (Pattern basic runtime external DataPower)	
Nome nodo	Impostato con uno dei seguenti valori: • SOAPolicySampleNode (Pattern basic runtime sample) • SOAPolicyBasicNode (Pattern basic runtime) • SOAPolicyBasicNode (Pattern basic runtime external DataPower)	
Password (root)		La password dell'ID utente root. La password del sistema operativo della macchina virtuale che è rappresentata da questa parte nel pattern.
Verifica password		Verifica l'input dell'utente per Password (root).

Tabella 5. Parametri configurati (Continua)

Nome parametro	Valore predefinito	Descrizione
Nome utente di gestione WebSphere	virtuser	Il nome utente di gestione di WebSphere Application Server. Non modificare questo valore.
Password di gestione WebSphere		La password dell'utente di gestione di WebSphere Application Server.
Verifica password		Verifica l'input utente per la password di gestione WebSphere Application Server.
Abilita VNC	True	Il valore è bloccato e non può essere modificato.

Parte Gestore distribuzione WSRR

La parte Gestore distribuzione WSRR fornisce alcune opzioni di configurazione.

I parametri configurabili della parte Gestore distribuzione WSRR Deployment sono descritti nella seguente tabella:

Tabella 6. Parametri configurabili

Nome parametro	Valore predefinito	Descrizione
CPU virtuali	1	Il numero di processori virtuali allocati per la macchina virtuale rappresentata da questa parte.
Dimensione di memoria (MB)	2048	La quantità di memoria allocata nella macchina virtuale, in megabyte.
Nome cella	SOAPolicyAdvancedCell	Il nome cella del pattern Advanced Runtime.
Nome nodo	SOAPolicyAdvancedNode	Il nome del nodo che risiede sulla macchina virtuale del Gestore distribuzione nel pattern Advanced Runtime.
Password (root)		La password dell'ID utente root. La password del sistema operativo della macchina virtuale che è rappresentata da questa parte nel pattern.
Verifica password		Verifica l'input dell'utente per Password (root).
Nome utente di gestione di WebSphere	virtuser	Il nome utente di gestione di WebSphere Application Server. Non modificare questo valore.
Password di gestione WebSphere		La password dell'utente di gestione di WebSphere Application Server.
Verifica password		Verifica l'input utente per la password di gestione WebSphere Application Server.
Abilita VNC	True	Il valore è bloccato e non può essere modificato.

Parte nodi personalizzati WSRR

La parte nodi personalizzati WSRR fornisce alcune opzioni di configurazione.

I parametri configurabili della parte nodi personalizzati WSRR sono descritti nella seguente tabella:

Tabella 7. Parametri configurabili

Nome parametro		**Descrizione**
CPU virtuali	2	Il numero di processori virtuali allocati per la macchina virtuale rappresentata da questa parte.
Dimensione di memoria (MB)	4096	La quantità di memoria allocata nella macchina virtuale, in megabyte.
Nome cella	CloudBurstCell	Il valore nome cella nella configurazione della parte del nodo personalizzato viene ignorato.
Nome nodo	SOAPolicyAdvancedNode	Il nome del nodo che risiede sulla macchina virtuale del Nodo personalizzato nel pattern Advanced Runtime.
Password (root)		La password dell'ID utente root. La password del sistema operativo della macchina virtuale che è rappresentata da questa parte nel pattern.
Verifica password		Verifica l'input dell'utente per Password (root).
Nome utente di gestione WebSphere	virtuser	Il nome utente di gestione dell'ambiente di WebSphere Application Server. Non modificare questo valore.
Password di gestione WebSphere		La password dell'utente di gestione dell'ambiente di WebSphere Application Server.
Verifica password		Verifica l'input utente per la password di gestione WebSphere Application Server.
Abilita VNC	True	Il valore è bloccato e non può essere modificato.

Parte DataPower

La parte DataPower presenta alcune opzioni di configurazione.

I parametri configurabili dell'immagine di sistema virtuale DataPower sono descritti nella seguente tabella:

Tabella 8. Parametri configurati

Nome parametro	**Valore predefinito**	**Descrizione**
CPU virtuali	4	Il numero di processori virtuali allocati per la macchina virtuale rappresentata da questa parte.
Dimensione di memoria (MB)	4096	La quantità di memoria allocata nella macchina virtuale, in megabyte.

Tabella 8. Parametri configurati (Continua)

Nome parametro	Valore predefinito	Descrizione
Password di admin		La password dell'amministratore DataPower.
Verifica password		Verifica l'input dell'utente per la password di admin.
Abilita SSH	True	Abilita SSH (per l'utilizzo dell'interfaccia di riga comandi DataPower).
Porta SSH	22	La porta per SSH.
Abilita l'interfaccia di gestione XML	True	Abilita l'interfaccia di gestione XML. Se abilitata, questa interfaccia consente agli amministratori di inviare richieste di stato e configurazione al dispositivo DataPower attraverso l'interfaccia SOAP standard.
Porta interfaccia di gestione XML	5550	La porta dell'interfaccia di gestione XML.
Abilita Servizio gestione Web	True	Abilita la WebGUI per l'interazione con il dispositivo DataPower.
Porta del servizio di gestione Web	9090	La porta della WebGUI.
Directory RAID	raid0	La directory in cui accedere ai file nell'archivio dati ausiliare di DataPower.

Package di script

Vi sono sette package di script forniti con IBM SOA Policy Gateway Pattern.

I seguenti package di script sono inclusi con questo pattern:

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

Gli script Add Named Queries e Tear Down non contengono parametri configurabili dall'utente.

Script: SOA Policy Gateway 2.5.0.0 - DataPower Domain

Lo script DataPower Domain fornisce il dominio DataPower durante la distribuzione. Lo script configura il collegamento tra il runtime WSRR ed un massimo di 10 dispositivi DataPower (virtuali).

Parametri

Tabella 9. Parametri configurabili

Nome parametro	Valore predefinito	Descrizione
DataPower_hostname	*Il valore è bloccato e non può essere modificato.*	Il nome host dell'istanza o del dispositivo DataPower da monitorare.
DataPower_admin_id	*Il valore è bloccato e non può essere modificato.*	L'ID utente dell'amministratore di tale istanza o dispositivo.
DataPower_XML_mgmt_port	*Il valore è bloccato e non può essere modificato.*	La porta per la comunicazione con l'interfaccia di gestione XML nell'istanza o nell'applicazione di DataPower.
DataPower_admin_password	*Il valore è bloccato e non può essere modificato.*	La password dell'ID utente amministratore.
Verifica password	*Il valore è bloccato e non può essere modificato.*	Ripetere la password dell'ID utente amministratore.
DataPower2_hostname	*Il valore è bloccato e non può essere modificato.*	
DataPower2_admin_id	*Il valore è bloccato e non può essere modificato.*	
DataPower2_XML_mgmt_port	*Il valore è bloccato e non può essere modificato.*	
DataPower2_admin_password	*Il valore è bloccato e non può essere modificato.*	
Verifica password	*Il valore è bloccato e non può essere modificato.*	
...		...
DataPower10_hostname	*Il valore è bloccato e non può essere modificato.*	
DataPower10_admin_id	*Il valore è bloccato e non può essere modificato.*	
DataPower10_XML_mgmt_port	*Il valore è bloccato e non può essere modificato.*	
DataPower10_admin_password	*Il valore è bloccato e non può essere modificato.*	
Verifica password	*Il valore è bloccato e non può essere modificato.*	
New_DataPower_domain	Il valore predefinito dipende dal tipo di pattern: • SOAPolicyAdvancedRuntime • SOAPolicyBasicRuntime	Il nuovo nome dominio da creare su ogni applicazione o istanza DataPower. Tale nome non deve corrispondere ad alcun dominio esistente altrimenti si verifica un errore del package di script oppure lo stesso viene interrotto. Il valore non può contenere spazi.
Remove_security_files	True	Per l'utilizzo del supporto, è possibile ignorare questa impostazione.

Script: SOA Policy Gateway 2.5.0.0 - Promotion

Lo script Promotion consente l'integrazione di un pattern Basic Runtime o Advanced Runtime con il pattarn SOA Policy Gateway Governance Master pre distribuito. Stabilisce la sicurezza tra celle tra il pattern Runtime e Governance, mentre può facoltativamente configurare la promozione WSRR nel Governance Master.

Parametri

Tabella 10. Parametri configurabili

Nome parametro	Valore predefinito	Descrizione
WSRR_GOV_DMGR_hostname		Il nome host del Dmgr del cluster WSRR.
WSRR_GOV_DMGR_cellname	SOAPolicyGMCell	Il nome cella del cluster WSRR.
WSRR_GOV_admin_user	virtuser	L'ID admin della cella Governance WSRR.
WSRR_GOV_admin_password		La password dell'ID Admin della cella Governance WSRR.
Verifica password		Verifica l'input dell'utente di WSRR_admin_password.
Promotion_environment		Deve essere uno tra staging, produzione, o non impostato. Questi valori sono sensibili al maiuscolo/minuscolo e devono corrispondere esattamente.
LTPA_key_password		Viene esportata una chiave LTPA ed utilizzata durante la creazione del package dello script. La chiave proviene dal Governance Master e viene utilizzata in tutte le celle nell'ambiente di promozione. Questa è la password utilizzata durante l'esportazione di tale chiave LTPA.
Verifica password		Verifica l'input dell'utente di LTPA_key_password.

Script: SOA Policy Gateway 2.5.0.0 - Sample

Lo script Sample configura i parametri di esempio dell'applicazione da utilizzare con il patternSOA Policy Gateway Basic Runtime Sample.

Parametri

Nessuno di questi parametri può essere impostato dall'utente.

Tabella 11. Parametri configurabili

Nome parametro		Descrizione
SCP_host	*Il valore è bloccato e non può essere modificato.*	
SCP_user	*Il valore è bloccato e non può essere modificato.*	
SCP_password	*Il valore è bloccato e non può essere modificato.*	

Tabella 11. Parametri configurabili (Continua)

Nome parametro		**Descrizione**
Verifica password	*Il valore è bloccato e non può essere modificato.*	
SCP_zip_location	*Il valore è bloccato e non può essere modificato.*	
CLIENT_PUBLIC_KEY_file	*Il valore è bloccato e non può essere modificato.*	
CLIENT_PUBLIC _KEY_password	*Il valore è bloccato e non può essere modificato.*	
Verifica password		
CLIENT_PRIVATE_KEY_file	*Il valore è bloccato e non può essere modificato.*	
CLIENT_PRIVATE_KEY_password	*Il valore è bloccato e non può essere modificato.*	
Verifica password		
CLI_FILE_file	*Il valore è bloccato e non può essere modificato.*	
Verifica password	*Il valore è bloccato e non può essere modificato.*	
DataPower_hostname	*Il valore è bloccato e non può essere modificato.*	Il nome host dell'istanza DataPower.
DataPower_XML_mgmt_port	*Il valore è bloccato e non può essere modificato.*	La porta utilizzata per l'interfaccia di gestione XML di DataPower XML.
DataPower_admin_id	*Il valore è bloccato e non può essere modificato.*	L'ID utente amministratore con autorizzazioni adeguate per utilizzare l'interfaccia di gestione XML.
DataPower_admin_password	*Il valore è bloccato e non può essere modificato.*	La password di DataPower_admin_id.
Verifica password	*Il valore è bloccato e non può essere modificato.*	Verifica l'input dell'utente di DataPower_admin_password.
SOAPolicySample_DataPower_domain	*Il valore è bloccato e non può essere modificato.*	Il nome del dominio di esempio. Tale nome non deve corrispondere ad alcun nome di dominio esistente sull'istanza DataPower.
SamplePolicySample_starting_port	*Il valore è bloccato e non può essere modificato.*	L'applicazione richiede 5 porte libere, che vengono utilizzate in modo sequenziale da questo valore. Ad esempio, se il valore è 62000, vengono utilizzate le porte 62000-62004. Lo script non verifica se le porte sono libere.
LDAP_hostname	*Il valore è bloccato e non può essere modificato.*	Il nome host della parte WSRR autonoma, dove è ospitato anche un server LDAP.
LDAP_port	*Il valore è bloccato e non può essere modificato.*	La porta del server LDAP.
LDAP_password	*Il valore è bloccato e non può essere modificato.*	La password utilizzata durante il bind con LDAP_DN.

Tabella 11. Parametri configurabili (Continua)

Nome parametro		Descrizione
Verifica password	*Il valore è bloccato e non può essere modificato.*	Verifica l'input utente per LDAP_password.
LDAP_DN	*Il valore è bloccato e non può essere modificato.*	Il DN (Distinguished Name) che viene utilizzato per il bind all'LDAP.

Script: SOA Policy Gateway 2.5.0.0 - Security

Lo script Security copia le informazioni sulla sicurezza (certificati ed altro) tra i sistemi DataPower e WSRR nel pattern.

I parametri di configurazione dei file di script di sicurezza sono per uso di supporto. Lasciarli impostati con i valori predefiniti.

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

Lo script DataPower Monitoring specifica i parametri di connessione del servizio condiviso DataPower Monitoring. L'agent ed i programmi di raccolta dati ITCAM DataPower sono eseguiti nella parte Core OS.

Parametri

Il servizio di monitoraggio può controllare fino a 10 dispositivi virtuali DataPower.

Tabella 12. Parametri configurabili

Nome parametro	Valore predefinito	Descrizione
DataPower1_hostname		Il nome host del dispositivo virtuale DataPower da monitorare.
DataPower1_admin_id	admin	L'ID utente amministratore di tale dispositivo virtuale.
DataPower1_XML_mgmt_port	5550	La porta per la comunicazione con l'interfaccia di gestione XML nell'applicazione virtuale di DataPower.
DataPower1_admin_password		La password dell'ID utente amministratore.
Verifica password		Ripetere la password dell'ID utente amministratore.
DataPower2_hostname		
DataPower2_admin_id	admin	
DataPower2_XML_mgmt_port	5550	
DataPower2_admin_password		
Verifica password		
...		...
DataPower10_hostname		
DataPower10_admin_id	admin	
DataPower10_XML_mgmt_port	5550	
DataPower10_admin_password		

Tabella 12. Parametri configurabili (Continua)

Nome parametro	Valore predefinito	Descrizione
Verifica password		

Script: SOA Policy Gateway 2.5.0.0 - External DataPower Monitoring

Lo script DataPower Monitoring specifica i parametri di connessione del servizio condiviso DataPower Monitoring. L'agent ed i programmi di raccolta dati ITCAM DataPower sono eseguiti nella parte Core OS.

Parametri

Il servizio di monitoraggio può controllare fino a 10 dispositivi DataPower.

Tabella 13. Parametri configurabili

Nome parametro	Valore predefinito	Descrizione
DataPower1_hostname		Il nome host del dispositivo DataPower da monitorare.
DataPower1_admin_id	admin	L'ID utente amministratore di tale dispositivo.
DataPower1_XML_mgmt_port	5550	La porta per la comunicazione con l'interfaccia di gestione XML nell'applicazione di DataPower.
DataPower1_admin_password		La password dell'ID utente amministratore.
Verifica password		Ripetere la password dell'ID utente amministratore.
DataPower2_hostname		
DataPower2_admin_id	admin	
DataPower2_XML_mgmt_port	5550	
DataPower2_admin_password		
Verifica password		
...		...
DataPower10_hostname		
DataPower10_admin_id	admin	
DataPower10_XML_mgmt_port	5550	
DataPower10_admin_password		
Verifica password		

Capitolo 5. Utilizzo di IBM SOA Policy Gateway Pattern

IBM SOA Policy Gateway Pattern fornisce le definizioni del pattern per la distribuzione ripetibile. Questi argomenti descrivono come distribuire i pattern.

Come parte del processo di distribuzione, configurare i parametri della parte. Per ulteriori informazioni, consltare “Distribuzione di pattern” a pagina 47. I pattern sono descritti in Capitolo 4, “Pattern, parti e package di script”, a pagina 19.

Attività correlate:

Capitolo 3, “Introduzione a IBM SOA Policy Gateway Pattern”, a pagina 13
Questo pattern utilizza WebSphere DataPower per controllare i messaggi utilizzando le politiche gestite e le definizioni del servizio in WSRR. Consultare gli argomenti in questa sezione per comprendere come scaricare ed installare il pattern, come verificare il pattern dopo l'installazione, accettare le licenze ed i ruoli utente coinvolti.

Pianificazione della configurazione e dei prerequisiti del pattern

IBM SOA Policy Gateway Pattern fornisce in modo veloce ed affidabile un ambiente per la gestione delle definizioni dei servizi e delle politiche, e per la loro applicazione. La distribuzione del pattern inizia con il pattern Governance Master, seguito da quello Runtime.

Preparazione e distribuzione di IBM SOA Policy Gateway Pattern

- Se si utilizza un dispositivo DataPower esterno, prepararlo per la gestione remota. Per ulteriori informazioni, consultare “Configurazione di un dispositivo DataPower per IBM SOA Policy Gateway Pattern” a pagina 46.

Distribuire il pattern Governance Master:

1. Distribuire un pattern SOA Policy Gateway Governance Master. Attendere il completamento della distribuzione dei pattern di Runtime. Per ulteriori informazioni, consultare “Distribuzione del pattern Governance Master” a pagina 50.

Distribuire i pattern Runtime:

1. Verificare se si necessita di un pattern Basic runtime con ambiente autonomo o di un pattern Advanced runtime con ambiente cluster.
2. Determinare quante istanze o dispositivi richiedono i pattern runtime.

   I pattern con comprendono DataPower hanno per impostazione predefinita due istanze DataPower. È possibile configurare fino a 10 istanze di DataPower. Per ulteriori informazioni, consultare “Aggiunta di istanze DataPower ad un pattern” a pagina 56.

   I pattern con DataPower esterno possono essere configurati per gestire fino a 10 dispositivi DataPower. Consultare “Distribuzione dei pattern DataPower esterni di base e avanzati” a pagina 57.

   Nota: Non è possibile aggiungere ulteriori istanze o dispositivi DataPower dopo il completamento della configurazione.
3. Configurare il pattern Runtime con le informazioni del pattern Governance Master. Per ulteriori informazioni, consultare “Informazioni sulla distribuzione di SOA Policy Gateway Governance Master” a pagina 51. Se necessario, è

possibile omettere le informazioni del pattern Governance Master per effettuare la distribuzione di un sistema autonomo (anche se ciò determinerà la visualizzazione di un errore sulla distribuzione che però potrà essere ignorato).

4. Specificare se il sistema di runtime è staging o produzione.
5. Distribuire il pattern. Per ulteriori informazioni, consultare "Distribuzione di un pattern di runtime avanzato" a pagina 53 o "Distribuzione di un pattern di runtime di base" a pagina 51.
6. Prima di avviare la distribuzione di un altro runtime, attendere il completamento della distribuzione in corso.

Una volta completata la distribuzione dei pattern Runtime:

1. La sicurezza WSRR e WebSphere può essere aggiornata dalla configurazione della sicurezza predefinita. Per ulteriori informazioni, consultare "Sicurezza per i pattern IBM SOA Policy Gateway Pattern".
2. Il dominio DataPower è pronto per la configurazione del gateway. Se si utilizza un dispositivo virtuale DataPower, è necessario applicare il fix pack più recente, consultare "Aggiornamento di DataPower nell'istanza distribuita" a pagina 54.

Configurazione di un dispositivo DataPower per IBM SOA Policy Gateway Pattern

Effettuare le operazioni di configurazione di DataPower riportate di seguito prima di eseguire gli script SOAPolicy.

Procedura

1. Accedere alla WebGUI del dispositivo DataPower come Administrator.
2. Ricercare `Interfaccia di gestione XML`.
3. Verificare che lo stato sia abilitato.
4. Verificare che quanto riportato di seguito sia attivo e protetto:
   - SOAP Management URI
   - SOAP Configuration Management
   - SOAP Configuration Management (v2004)
   - Endpoint AMP
   - Endpoint SLM
   - Endpoint WS-Management
   - Endpoint WSDM
   - Sottoscrizione UDDI
   - Sottoscrizione WSRR

Sicurezza per i pattern IBM SOA Policy Gateway Pattern

Si verifica un'autenticazione reciproca tra le applicazioni DataPower e gli script nei pattern Basic e Advanced. Gli script eseguono lo scambio di certificati necessario. Tenere presente che i certificati SSL predefiniti forniti con il pattern sono attribuiti all'host che è stato utilizzato per creare il pattern.

Aumento della sicurezza

Le immagini WSRR e WebSphere Application Server utilizzate nei pattern hanno solo la sicurezza predefinita impostata. Per creare un ambiente più sicuro, è possibile utilizzare le tecniche di sicurezza WebSphere Application Server standard.

Consultare il centro informazioni di WebSphere Network Deployment Versione 8.0 presso i seguenti link:

- WebSphere Application Server, Network Deployment (piattaforme distribuite e Windows), Versione 8.0: Centro informazioni di IBM WebSphere Application Server, Network Deployment (Distributed platforms and Windows), Versione 8.0
- Sicurezza applicazione: Centro informazioni di IBM WebSphere Application Server, Network Deployment (Distributed platforms and Windows), Versione 8.0 - Securing applications and their environment
- Percorsi end-to-end per la sicurezza: Centro informazioni di IBM WebSphere Application Server, Network Deployment (Distributed platforms and Windows), Versione 8.0 - Securing applications and their environment

Distribuzione di pattern

La distribuzione di pattern con IBM PureApplication System nel cloud fornisce un ambiente SOA Policy Gateway in esecuzione. È possibile distribuire i pattern predefiniti disponibili con le immagini IBM SOA Policy Gateway Pattern oppure distribuire pattern creati dall'utente.

Prima di iniziare

Per distribuire un pattern, è necessario prima disporre di un pattern predefinito o di un nuovo pattern completo, con tutte le parti richieste configurate. I dettagli relativi all'ambiente, al gruppo cloud ed al gruppo IP in cui eseguire la distribuzione vengono richiesti all'amministratore del sistema PureAS.

Informazioni su questa attività

Il pattern viene distribuito utilizzando Workload Console.

Procedura

Per distribuire IBM SOA Policy Gateway Pattern per l'esecuzione nel proprio cloud privato, effettuare le operazioni riportate di seguito:

1. Dall'elenco dei pattern nella finestra Pattern del sistema virtuale, selezionare il pattern da distribuire.
2. Fare clic sull'icona **Distribuisci**.
3. Completare i campi richiesti per distribuire il pattern. Nella finestra, immettere un nome per il sistema virtuale ed immettere le altre informazioni richieste. Un segno di spunta visualizzato a ciascun elemento indica che non è necessaria ulteriore configurazione. È possibile modificare i parametri per le parti configurate, prima di distribuire il pattern, facendo clic sul nome della parte per aprire il relativo editor. Le macchine virtuali vengono create, nell'ordine richiesto, e quindi avviate.

Risultati

Il processo di distribuzione crea ed avvia le macchine virtuali per le parti definite e fornisce i link alle console richieste. Il tempo per la distribuzione dipende dalla complessità del pattern distribuito. Un pattern distribuito è un sistema virtuale oppure un ambiente runtime IBM SOA Policy Gateway Pattern di cui è appena stato eseguito il provisioning.

Operazioni successive

È possibile visualizzare lo stato della propria istanza, per verificare quando la distribuzione è completa ed iniziare a gestirla, dalla finestra Istanze del sistema virtuale.

Informazioni correlate:

IBM PureApplication System: Gestione dei pattern del sistema virtuale

Distribuzione del servizio condiviso Monitoraggio di sistema

La distribuzione del servizio condiviso Monitoraggio di sistema per SOA Policy Gateway fornisce i componenti di monitoraggio per il proprio sistema virtuale.

Prima di iniziare

L'amministratore del sistema PureAS deve avviare il servizio condiviso Monitoraggio di sistema ed indicare all'utente il gruppo cloud e l'ambiente in cui è stato avviato. È necessario utilizzare lo stesso gruppo cloud e lo stesso ambiente per distribuire il servizio condiviso di monitoraggio del sistema di SOA Policy Gateway ed i pattern di governance e runtime.

Il monitoraggio delle istanze WSRR richiede che sia avviato il servizio condiviso Monitoraggio di sistema per WebSphere Application Server, per cui è necessario verificare che tale servizio sia presente sul sistema PureAS.

Procedura

Completare i passi riportati di seguito in Workload Console:

1. Fare clic su **Istanze** > **Servizi condivisi**.
2. Verificare che il servizio Monitoraggio di sistema sia in esecuzione nel gruppo cloud in cui verranno distribuiti i pattern. In caso contrario, rivolgersi all'amministratore PureAS per avviarlo.
3. Per abilitare il servizio condiviso di monitoraggio DataPower:
   a. Fare clic su **Cloud** > **Tipi di pattern**.
   b. Selezionare la voce **Monitoraggio di sistema per SOA Policy Gateway Pattern 2.5.0.0** nel riquadro Tipi di pattern.
   c. Fare clic su **Abilita** nel campo **Stato** ed attendere che il campo relativo allo stato venga modificato in **Disabilita**.
4. Per avviare il servizio condiviso di monitoraggio di WebSphere Application Server:
   a. Fare clic su **Istanze** > **Servizi condivisi**.
   b. Fare clic sul simbolo di addizione nel riquadro Istanze del servizio condiviso per visualizzare la finestra Distribuisci servizio condiviso.
   c. Selezionare **Monitoraggio di sistema per WebSphere Application Server** e fare clic su **OK**.
   d. Nella finestra Configura e distribuisci un servizio condiviso, specificare se si desidera che il servizio venga avviato su pattern precedentemente distribuiti selezionando le due caselle di spunta in basso. Fare clic su **OK**.
   e. Nella finestra Distribuisci applicazione virtuale, specificare il **Gruppo cloud di destinazione**, il **Gruppo IP** ed il **Profilo** come indicato dall'amministratore del sistema PureAS. Tali valori devono essere uguali a quelli distribuiti dai propri sistemi virtuali.

5. Per avviare il servizio condiviso di monitoraggio di WebSphere DataPower:
   a. Fare clic su **Instanze** > **Servizi condivisi** nella barra dei menu.
   b. Fare clic sul simbolo di addizione nel riquadro Istanze del servizio condiviso per visualizzare la finestra Distribuisci servizio condiviso.
   c. Selezionare **Monitoraggio di sistema per WebSphere DataPower** dall'elenco e fare clic su **OK**.
   d. Nella finestra Configura e distribuisci un servizio condiviso, specificare se si desidera che il monitoraggio venga avviato su pattern precedentemente distribuiti selezionando le due caselle di spunta in basso. Fare clic su **OK**.
   e. Nella finestra Distribuisci applicazione virtuale, specificare il **Gruppo cloud di destinazione**, il **Gruppo IP** ed il **Profilo** come indicato dall'amministratore del sistema PureAS. Tali valori devono essere uguali a quelli distribuiti dai propri sistemi virtuali.
   f. Generare e salvare una chiave SSH se è richiesto l'accesso di debug al servizio condiviso di monitoraggio.
   g. Fare clic su **OK**.

Risultati

Il servizio condiviso Monitoraggio di sistema per WebSphere DataPower è visualizzato come in esecuzione. Il servizio condiviso Monitoraggio di sistema per WebSphere Application Server è visualizzato come in esecuzione.

Operazioni successive

Per verificare la distribuzione, consultare “Verifica della distribuzione” a pagina 55.

Distribuzione del pattern Basic Runtime Sample

La distribuzione del pattern SOA Policy Gateway Basic Runtime Sample crea un'istanza del sistema virtuale in esecuzione del pattern. Questo pattern è disponibile solo su sistemi x86.

Informazioni su questa attività

La distribuzione di un pattern crea un'istanza del sistema virtuale in esecuzione nel cloud.

Procedura

Per distribuire un pattern SOA Policy Gateway Basic Runtime Sample, effettuare le operazioni riportate di seguito:

1. In Workload Console, fare clic su **Pattern** > **Sistemi virtuali**.
2. Dall'elenco Pattern del sistema virtuale, selezionare **SOA Policy Gateway 2.5.0.0 - Basic Runtime Sample**.
3. Fare clic sull'icona **Distribuisci**.
4. Completare i campi richiesti per distribuire il pattern. Un segno di spunta visualizzato a ciascun elemento indica che non è necessaria ulteriore configurazione.
   a. Nella casella **Nome sistema virtuale**, immettere un nome univoco per l'istanza.
   b. Espandere la sezione **Scegli ambiente** e specificare il **Profilo** indicato dall'amministratore del sistema PureAS.

c. Configurare i pattern virtuali. Fare clic su **Configura parti virtuali**, quindi fare clic sul nome della parte per aprire l'editor per le parti e gli script. Specificare il **Gruppo cloud** ed il **Gruppo IP** come indicato dall'amministratore del sistema PureAS. Per i dettagli relativi ai parametri di configurazione specifici degli script e specifici dei pattern, consultare gli argomenti riportati di seguito.

   Nota: Per impostazione predefinita, tutte le password per questo pattern sono impostate su `password`.

   - "Parte DataPower" a pagina 37
   - "Parte DB2 Enterprise" a pagina 29.
   - "Parte Server WSRR Standalone" a pagina 35
   - "Script: SOA Policy Gateway 2.5.0.0 - Sample" a pagina 40

5. Fare clic su **OK** per distribuire il pattern.

Operazioni successive

Per verificare la distribuzione, consultare "Verifica della distribuzione" a pagina 55.

Distribuzione del pattern Governance Master

La distribuzione del pattern SOA Policy Gateway Governance Master crea un'istanza del sistema virtuale in esecuzione del pattern.

Procedura

Per distribuire il pattern SOA Policy Gateway Governance Master, effettuare le operazioni riportate di seguito:

1. In Workload Console, fare clic su **Pattern** > **Sistemi virtuali**.
2. Dall'elenco Pattern del sistema virtuale, selezionare **SOA Policy Gateway 2.5.0.0 - Governance Master**.
3. Fare clic sull'icona **Distribuisci**.
4. Completare i campi per distribuire il pattern. Un segno di spunta visualizzato a ciascun elemento indica che non è necessaria ulteriore configurazione.
   a. Nella casella **Nome sistema virtuale**, immettere un nome univoco per l'istanza.
   b. Espandere la sezione **Scegli ambiente** e specificare il **Profilo** come indicato dall'amministratore del sistema PureAS.
   c. Configurare i pattern virtuali. Fare clic su **Configura parti virtuali** quindi fare clic sul nome della parte per aprire l'editor per le parti e gli script. Specificare il **Gruppo cloud** ed il **Gruppo IP** come indicato dall'amministratore del sistema PureAS. Per i dettagli relativi ai parametri di configurazione specifici degli script e specifici dei pattern, consultare gli argomenti riportati di seguito.
      - "Parte DB2 Enterprise HADR Primary" a pagina 31
      - "Parte Gestore distribuzione WSRR" a pagina 36
      - "Parte nodi personalizzati WSRR" a pagina 37
      - "Parte DB2 Enterprise HADR Standby" a pagina 33
5. Fare clic su **OK** per distribuire il pattern.

Operazioni successive

Per verificare la distribuzione, consultare “Verifica della distribuzione” a pagina 55.

Informazioni sulla distribuzione di SOA Policy Gateway Governance Master

È necessario distribuire Governance Master prima che siano distribuiti i pattern di runtime.

Informazioni su questa attività

Le informazioni sulla distribuzione dall'istanza di Governance Master sono necessarie come input per i valori di distribuzione per i pattern di runtime.

Procedura

Per individuare i valori richiesti dall'istanza di Governance Master:

1. Passare a **Istanze** > **Sistemi virtuali**.
2. Selezionare l'istanza Governance Master di distribuzione.
3. Espandere **Macchine virtuali**.
4. Espandere la macchina virtuale denominata ***WSRRDMGR***.
5. Prendere nota dei punti riportati di seguito:
   - Nella sezione **Hardware e rete**, prendere nota del nome host e dell'indirizzo IP. Il nome host è il valore **Interfaccia di rete 0**.
   - Nella sezione **Configurazione WebSphere**, prendere nota del nome della cella.

   Il nome host o l'indirizzo IP, il nome della cella ed il nome utente di gestione e la password di WebSphere utilizzati durante la distribuzione dell'istanza di Governance Master sono input richiesti per i seguenti parametri nei pattern di runtime:
   - WSRR_GOV_DMGR_hostname
   - WSRR_GOV_DMGR_cellname
   - WSRR_GOV_admin_user
   - WSRR_GOV_admin_password

   Se si desidera distribuire un pattern di runtime come sistema autonomo, è possibile impostare tali parametri su “Non impostato”. Con questa impostazione, la distribuzione viene visualizzata come **non riuscita** in **Sistema virtuale** > **Istanze** perché il package di script della promozione ha esito negativo. Tuttavia, la distribuzione è ancora utilizzabile.

Distribuzione di un pattern di runtime di base

La distribuzione di un pattern di runtime di base crea un'istanza del sistema virtuale in esecuzione del pattern.

Prima di iniziare

Prima di distribuire un pattern di runtime di base, effettuare le operazioni riportate di seguito:

- Se si sta distribuendo un pattern di runtime di base con DataPower esterno, configurare i propri dispositivi DataPower per IBM SOA Policy Gateway Pattern;

consultare “Configurazione di un dispositivo DataPower per IBM SOA Policy Gateway Pattern” a pagina 46. Su sistemi Power, è supportato solo DataPower esterno.

- Ottenere le informazioni relative alla distribuzione di Governance Master; consultare “Informazioni sulla distribuzione di SOA Policy Gateway Governance Master” a pagina 51.

Informazioni su questa attività

La distribuzione di un pattern crea un'istanza del sistema virtuale in esecuzione nel cloud.

Nota: Se si utilizza il profilo GEP (Governance Enablement Profile), non è possibile distribuire un ambiente di staging e di produzione contemporaneamente nei pattern di runtime. Questa limitazione è presente perché ciò potrebbe causare conflitti durante il processo di configurazione delle proprietà di promozione. Distribuire prima l'ambiente di staging e poi l'ambiente di produzione.

Procedura

Per distribuire un pattern di runtime di base, effettuare le operazioni riportate di seguito:

1. Fare clic su **Pattern** > **Sistemi virtuali**.
2. Dall'elenco Pattern del sistema virtuale, selezionare **SOA Policy Gateway 2.5.0.0 - Basic Runtime External DataPower** oppure **SOA Policy Gateway 2.5.0.0 - Basic Runtime**.
3. Fare clic sull'icona **Distribuisci**.
4. Completare i campi richiesti per distribuire il pattern. Un segno di spunta visualizzato a ciascun elemento indica che non è necessaria ulteriore configurazione.
   a. Nella casella **Nome sistema virtuale**, immettere un nome univoco per l'istanza.
   b. Espandere la sezione **Scegli ambiente** e specificare il **Profilo** indicato dall'amministratore del sistema PureAS.
   c. Configurare i pattern virtuali. Fare clic su **Configura parti virtuali**, quindi fare clic sul nome della parte per aprire l'editor per le parti e gli script. Specificare il **Gruppo cloud** ed il **Gruppo IP** come indicato dall'amministratore del sistema PureAS. Per i dettagli relativi ai parametri di configurazione specifici degli script e specifici dei pattern, consultare gli argomenti riportati di seguito.

      Nota: Se si desidera distribuire il pattern senza Governance Master, immettere 'Non impostato' come parametro del nome host di Governance Master. Tenere presente che in questo modo il package dello script di promozione viene riportato come non funzionante nella distribuzione.
      - “Parte DataPower” a pagina 37
      - “Parte DB2 Enterprise” a pagina 29
      - “Parte Server WSRR Standalone” a pagina 35
      - “Script: SOA Policy Gateway 2.5.0.0 - Security” a pagina 42
      - “Script: SOA Policy Gateway 2.5.0.0 - Promotion” a pagina 40
      - “Script: SOA Policy Gateway 2.5.0.0 - DataPower Domain” a pagina 38

- "Script: SOA Policy Gateway 2.5.0.0 - DataPower Monitoring (solo x86)" a pagina 42

5. Fare clic su **OK** per distribuire il pattern.

Operazioni successive

Per verificare la distribuzione, consultare "Verifica della distribuzione" a pagina 55.

Distribuzione di un pattern di runtime avanzato

La distribuzione di un pattern di runtime avanzato crea un'istanza del sistema virtuale in esecuzione del pattern.

Prima di iniziare

Prima di distribuire il pattern di runtime avanzato, effettuare le attività riportate di seguito:

- Se si sta distribuendo un pattern di runtime avanzato con DataPower esterno, configurare i propri dispositivi DataPower per la connessione al pattern. Consultare "Configurazione di un dispositivo DataPower per IBM SOA Policy Gateway Pattern" a pagina 46. Su sistemi Power, è supportato solo DataPower esterno.
- Ottenere le informazioni relative alla distribuzione di Governance Master; consultare "Informazioni sulla distribuzione di SOA Policy Gateway Governance Master" a pagina 51.

Informazioni su questa attività

La distribuzione di un pattern crea un'istanza del sistema virtuale in esecuzione nel cloud.

Nota: Se si utilizza il profilo GEP (Governance Enablement Profile), non è possibile distribuire un ambiente di staging e di produzione contemporaneamente nei pattern di runtime. Questa limitazione è presente perché ciò potrebbe causare conflitti durante il processo di configurazione delle proprietà di promozione. Distribuire prima l'ambiente di staging e poi l'ambiente di produzione.

Procedura

Per distribuire un pattern di runtime avanzato, effettuare le operazioni riportate di seguito:

1. Fare clic su **Pattern** > **Sistemi virtuali**.
2. Dall'elenco Pattern del sistema virtuale, selezionare **SOA Policy Gateway 2.5.0.0 - Advanced Runtime External DataPower** o **SOA Policy Gateway 2.5.0.0 - Advanced Runtime**.
3. Fare clic sull'icona **Distribuisci**.
4. Completare i campi richiesti per distribuire il pattern. Un segno di spunta visualizzato a ciascun elemento indica che non è necessaria ulteriore configurazione.
   a. Nella casella **Nome sistema virtuale**, immettere un nome univoco per l'istanza.
   b. Espandere la sezione **Scegli ambiente** e specificare il **Profilo** indicato dall'amministratore del sistema PureAS.

c. Configurare i pattern virtuali. Fare clic su **Configura parti virtuali**, quindi fare clic sul nome della parte per aprire l'editor per le parti e gli script. Specificare il **Gruppo cloud** ed il **Gruppo IP** come indicato dall'amministratore del sistema PureAS. Per i dettagli relativi ai parametri di configurazione specifici degli script e specifici dei pattern, consultare gli argomenti riportati di seguito.

   Nota: Se si desidera distribuire il pattern senza Governance Master, immettere 'Non impostato' come parametro del nome host di Governance Master. Tenere presente che in questo modo il package dello script di promozione viene riportato come non funzionante nella distribuzione.
   - "Parte DataPower" a pagina 37
   - "Parte DB2 Enterprise HADR Primary" a pagina 31
   - "Parte Gestore distribuzione WSRR" a pagina 36
   - "Script: SOA Policy Gateway 2.5.0.0 - Promotion" a pagina 40
   - "Script: SOA Policy Gateway 2.5.0.0 - DataPower Domain" a pagina 38
   - "Parte nodi personalizzati WSRR" a pagina 37
   - "Parte DB2 Enterprise HADR Standby" a pagina 33
   - "Script: SOA Policy Gateway 2.5.0.0 - DataPower Monitoring (solo x86)" a pagina 42

5. Fare clic su **OK** per distribuire.

Operazioni successive

Per verificare la distribuzione, consultare "Verifica della distribuzione" a pagina 55.

Aggiornamento di DataPower nell'istanza distribuita

Una volta distribuito un pattern che include un componente WebSphere DataPower, è necessario aggiornare DataPower al fix pack più recente.

Informazioni su questa attività

È possibile aggiornare DataPower scaricando il fix pack da Fix Central ed applicandolo nella WebGUI DataPower.

Procedura

1. Scaricare il package di aggiornamento da Fix Central:
   a. In Fix Central, ricercare WebSphere DataPower SOA Appliances.
   b. Selezionare e scaricare il package XI52-virtual-6.0.0.1-Firmware.
2. Effettuare la connessione alla WebGUI per la macchina virtuale DataPower nel proprio pattern distribuito, consultare "Connessione alla console di un DataPower virtuale" a pagina 85.
3. Dal pannello di controllo, selezionare **Controllo sistema**.
4. Individuare la sezione **Immagine di avvio**.
5. Caricare sul dispositivo DataPower il file `xi6001.scrypt4` dal fixpack scaricato. Utilizzare File Manager sulla WebGUI DataPower.
6. Selezionare lo script caricato dall'elenco **File firmware**.
7. Accettare i termini della licenza e fare clic su **Immagine di avvio**.
8. Seguire i prompt per installare il fix pack.

Verifica della distribuzione

Una volta distribuito il pattern, verificare che la distribuzione sia stata eseguita correttamente.

Procedura

1. Ricercare nei log di distribuzione eventuali errori nella cronologia della distribuzione del sistema virtuale. Per ulteriori informazioni, consultare “Risoluzione dei problemi con la distribuzione” a pagina 101.
2. Opzionale: Se è stato distribuito SOA Policy Gateway Basic Runtime Sample, verificare l'istanza distribuita seguendo il supporto didattico per inviare alcuni messaggi di esempio utilizzando le applicazioni di esempio fornite. Consultare “Esecuzione di scenari di test di esempio” a pagina 61.

Aggiunta di un ulteriore ambiente di runtime

Il profilo di abilitazione governance è dotato di un sistema di classificazione degli ambienti predefinito che contiene quattro ambienti distinti: sviluppo, test, staging e produzione.

Informazioni su questa attività

Gli ambienti di staging e di produzione sono anche codificati nel ciclo di vita SOA che definisce il ciclo di vita delle versioni di capability, come, ad esempio, le versioni del servizio. Esistono stati e transizioni specifici degli ambienti di staging e di produzione, che consentono la promozione controllata in tali ambienti di runtime mediante la definizione dei sistemi di destinazione nel file di configurazione della promozione. Questa procedura è appropriata se la propria organizzazione definisce gli ambienti nello stesso modo, con l'ambiente di staging impostato come un ambiente di pre-produzione che consente l'esecuzione di test prima che la versione di capability sia aperta per l'utilizzo generale. Tuttavia, molte organizzazioni richiedono ulteriori ambienti, per cui è necessario apportare modifiche nel profilo in modo da colmare tali differenze. Questa sezione descrive un modo per aggiungere un nuovo ambiente di runtime nel profilo di abilitazione governance WSRR.

Per ulteriori informazioni relative alla pianificazione di un ambiente di distribuzione, consultare “Pianificazione della configurazione e dei prerequisiti del pattern” a pagina 45.

Procedura

1. Distribuire il SOA Policy Gateway Governance Master predefinito. Per ulteriori informazioni, consultare “Distribuzione del pattern Governance Master” a pagina 50.
2. Opzionale: Modificare il profilo di abilitazione governance WSRR. Per ulteriori informazioni, consultare Centro informazioni di IBM WebSphere Service Registry and Repository Versione 8.0 - Tutorial: Customizing runtime environments.
3. Configurare i pattern di runtime di base o avanzati con i dettagli di Governance Master. Per ulteriori informazioni, consultare “Informazioni sulla distribuzione di SOA Policy Gateway Governance Master” a pagina 51.

   Nota: Il valore dell'ambiente di promozione deve essere impostato su “Non impostato”.

4. Distribuire i pattern di runtime di base o avanzati. Per ulteriori informazioni, consultare “Distribuzione di un pattern di runtime di base” a pagina 51 e “Distribuzione di un pattern di runtime avanzato” a pagina 53.

Aggiunta di istanze DataPower ad un pattern

Per impostazione predefinita, i pattern di base ed avanzati con istanze DataPower interne dispongono di due istanze. Ciascun pattern può avere fino a 10 istanze DataPower in totale.

Informazioni su questa attività

Non è possibile modificare i pattern. È possibile aggiungere ulteriori istanze DataPower ai pattern di runtime di base o avanzati effettuando una copia del pattern e modificando tale copia.

Procedura

1. Aprire il pattern in Workload Console.
2. Fare clic su **Clona** e specificare un nome per la copia del pattern.
3. Fare clic su **Modifica**.
4. Trascinare ulteriori parti DataPower dall'elenco delle parti per aggiungerle al pattern.
5. Fare clic su **Modifica terminata**.

Eliminazione delle istanze DataPower da un pattern

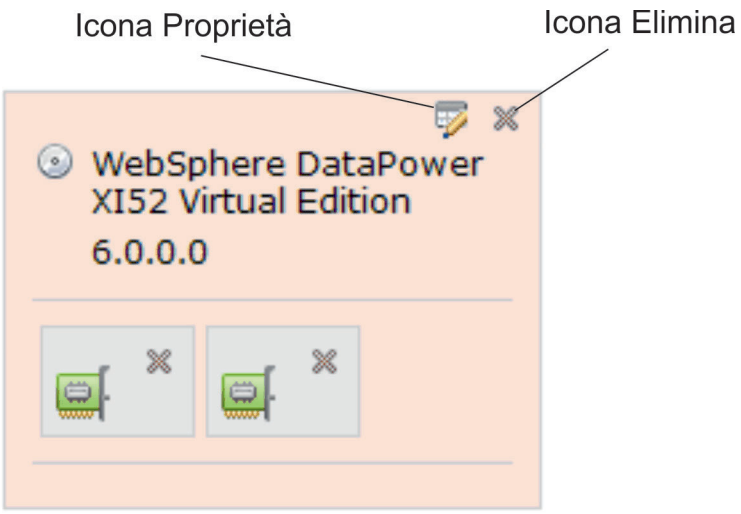
È possibile eliminare le istanze DataPower interne da un pattern, se richiesto.

Informazioni su questa attività

I pattern non possono essere modificati. È possibile eliminare le istanze DataPower dai pattern di runtime di base o avanzati effettuando una copia del pattern e modificando tale copia.

Procedura

1. Aprire il pattern in Workload Console.
2. Fare clic su **Clona** e specificare un nome per la copia del pattern.
3. Fare clic su **Modifica**.
4. Eliminare un'istanza DataPower facendo clic sull'icona Elimina.



Nota: Le istanze DataPower devono essere eliminate in ordine numerico inverso. Ciascuna istanza DataPower nell'area dispone di un numero nel proprio campo relativo al nome, visibile facendo clic sull'icona delle proprietà. Il nome è in formato: 'DataPower_XI52*x*' dove *x* è il numero (la prima istanza DataPower non dispone di alcun numero, il relativo nome è: 'DataPower_XI52'). Le istanze DataPower con numeri più alti si trovano generalmente in alto a sinistra nell'area.

5. Fare clic su **Modifica terminata**.

Distribuzione dei pattern DataPower esterni di base e avanzati

È possibile distribuire i pattern SOA Policy Gateway Basic Runtime External DataPower e SOA Policy Gateway Advanced Runtime External DataPower con un massimo di 10 dispositivi DataPower.

Informazioni su questa attività

Per ulteriori informazioni relative alla distribuzione dei pattern, consultare “Distribuzione di un pattern di runtime di base” a pagina 51 oppure “Distribuzione di un pattern di runtime avanzato” a pagina 53. Per ulteriori informazioni relative ai parametri di configurazione per cui è necessario impostare i valori, consultare “Parte Server WSRR Standalone” a pagina 35, “Parte Gestore distribuzione WSRR” a pagina 36 e “Script: SOA Policy Gateway 2.5.0.0 - DataPower Monitoring (solo x86)” a pagina 42.

Procedura

1. Distribuire il pattern e fare clic su **Configura parti virtuali**.
2. Per la parte WSRR standalone o gestore distribuzione WSRR, immettere le seguenti informazioni per ciascun dispositivo:
   - DataPower_hostname
   - DataPower_XML_mgmt_port
   - DataPower_admin_id
   - DataPower_admin_password
   - Verifica password
   - New_DataPower_domain

Applicazione di esempio

L'applicazione di esempio è costituita da un servizio Web e da un'API RESTful, entrambi descritti e governati in WSRR. Un dominio DataPower è configurato in modo che WSRR agisca da gateway, mentre il client Web di esempio viene fornito per prendere dimestichezza con i servizi.

Lo scenario di base nell'applicazione di esempio riporta un'applicazione di inventario per un archivio (Warehouse) e un servizio RESTful che duplica una delle operazioni per dispositivo mobile. Il servizio Web Store dispone di tre operazioni:

- purchase
- findInventory
- returnProduct

L'ultima operazione, findInventory, è disponibile anche come servizio RESTful.

Servizio Web di esempio

La SLD (Service Level Definition) di base ha due politiche di mediazione allegate:

- Convalida su Store.wsdl. L'esempio presuppone che la convalida DataPower sia disattivata.
- Rifiutare se vi sono più di 5 messaggi in 90 secondi. Questa soglia è bassa per facilità di dimostrazione.

Il consumer del servizio Store è l'applicazione StoreConsumer, che dispone dell'ID consumer “CEO”. Questo consumer ha due SLA (Service Level Agreement), Gold e Silver. Se in DataPower viene ricevuta una richiesta con ID consumer “CEO” e un ID contesto “Silver”, la richiesta viene accettata perché l'accordo SLA è presente. Se l'ID consumer ID è “CEO” e l'ID contesto è “Gold”, l'accordo SLA Gold risulta corrispondente. L'accordo SLA in questione ha una politica di reinstradamento allegata ad esso, pertanto la richiesta viene reinstradata all'endpoint alternativo indicato nella politica.

Se una richiesta viene ricevuta con un ID consumer diverso da “CEO”, non vi è alcuna versione dell'applicazione con questo ID consumer. There are therefore also no SLAs that could match, so this is a request from an anonymous consumer. Di conseguenza, vengono applicate tutte le politiche allegate allo SLA anonimo. In questo caso, viene visualizzata una notifica nei file di log. Tenere presente che l'esempio non include un modo per inviare una richiesta con un ID consumer che non sia “CEO”.

Lo scenario inoltre esegue l'autorizzazione per l'operazione findInventory, che si basa sull'appartenenza del gruppo utenti. Un server LDAP viene fornito con l'esempio per l'associazione delle credenziali utente al gruppo corretto.

Il diagramma di flusso dell'applicazione di esempio mostra il flusso dell'applicazione con ciascuna casella che rappresenta un gateway DataPower differente.

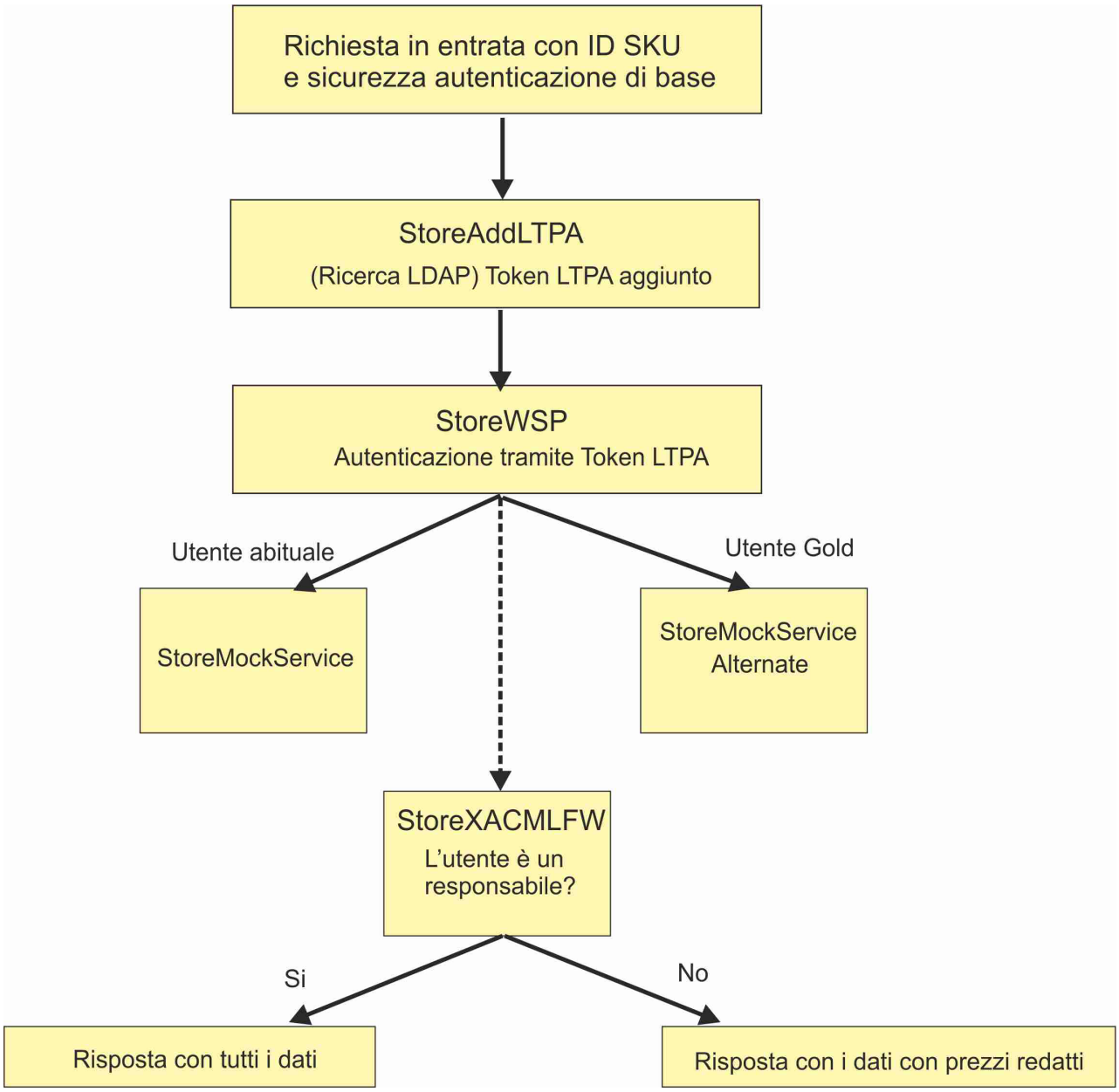


Figura 10. Diagramma di flusso dell'applicazione di esempio

Servizio RESTful di esempio

Il servizio RESTful è governato in modo analogo al servizio web, tranne per il modo in cui le politiche vengono utilizzate. Come con il servizio Web, vi sono due SLA: uno per clienti Silver e l'altro per clienti Gold. Tuttavia, per il servizio REST, non vi sono politiche allegate al livello SLD (applicato a tutte le richieste). Al contrario, vi è un'unica politica allegata a ciascuno SLA. Lo SLA Gold ha una politica che rifiuta i messaggi dopo più di 5 richieste effettuate in 9 secondi, mentre quello Silver consente 2 richieste in 90 secondi prima che i messaggi vengano rifiutati.

Panoramica sulle risorse WSRR presenti nell'esempio

In questa sezione vengono illustrate le risorse WSRR che descrivono il servizio Store. Le risorse del servizio REST seguono un pattern simile.

Bob's Warehouse è l'organizzazione che possiede sia il servizio Store che l'applicazione StoreConsumer.

Warehouse Business Service è l'oggetto in cui risiedono tutte le versioni del servizio Store. La versione del servizio Store rappresenta una determinata vesione del servizio Store. Questa versione è il servizio pornito per il riutilizzo. L'SLD (service level definition) Store ha allegate due politiche; la prima rifiuta i messaggi dopo 5 messaggi in 90 secondi e la seconda effettua la convalida rispetto allo schema Store.wsdl. Con queste politiche si determina la convalida delle richieste effettuate al servizio Store, e l'autorizzazione del passaggio di un massimo di 5 richieste attraverso il servizio, in un intervallo di tempo di 90 secondi, indipendentemente dal mittente della richiesta. SLD ha anche uno SLA anonimo. Tutte le politiche collegate a questo SLA vengono applicate quando si ricevono richieste per cui non vi sono SLA corrispondenti. Una corrispondenza SLA si concretizza nelle seguenti condizioni:

- Vi sia una Versione dell'applicazione utente che corrisponde all'ID consumer presente nella richiesta.
- Vi sia un SLA tra tale versione dell'applicazione utente e l'SLD del servizio utilizzato, che corrisponde all'ID contesto nella richiesta.

L'applicazione business StoreConsumer rappresenta l'applicazione StoreConsumer, mentre la versione dell'applicazione StoreConsumer è una particolare versione di tale applicazione. Questa applicazione è la consumer: essa riutilizza il servizio Store. Ha un ID consumer “CEO”. Per questa applicazione sono disponibili due SLA, che costituiscono un accordo per consentire a questa applicazione di utilizzare il servizio Store. Una ha l'ID contesto “Gold”, il che significa che corrisponde alla richiesta proveniente dall'applicazione StoreConsumer con ID contesto “Gold” nella richiesta, ed una che corrisponde a Silver. Lo SLA Gold ha allegata una politica per instradare nuovamente le richieste, in modo tale che qualsiasi richiesta, proveniente dall'applicazione StoreConsumer, che abbia l'ID contesto impostato su Gold venga instradata all'endpoint specificato nella politica. Lo SLA Silver non ha politiche allegate, il che significa che è consentito il passaggio alle richieste provenienti dall'applicazione StoreConsumer con ID contesto Silver, e non viene applicata alcuna politica.

In questo esempio vi è una politica di notifica allegata allo SLA anonimo.

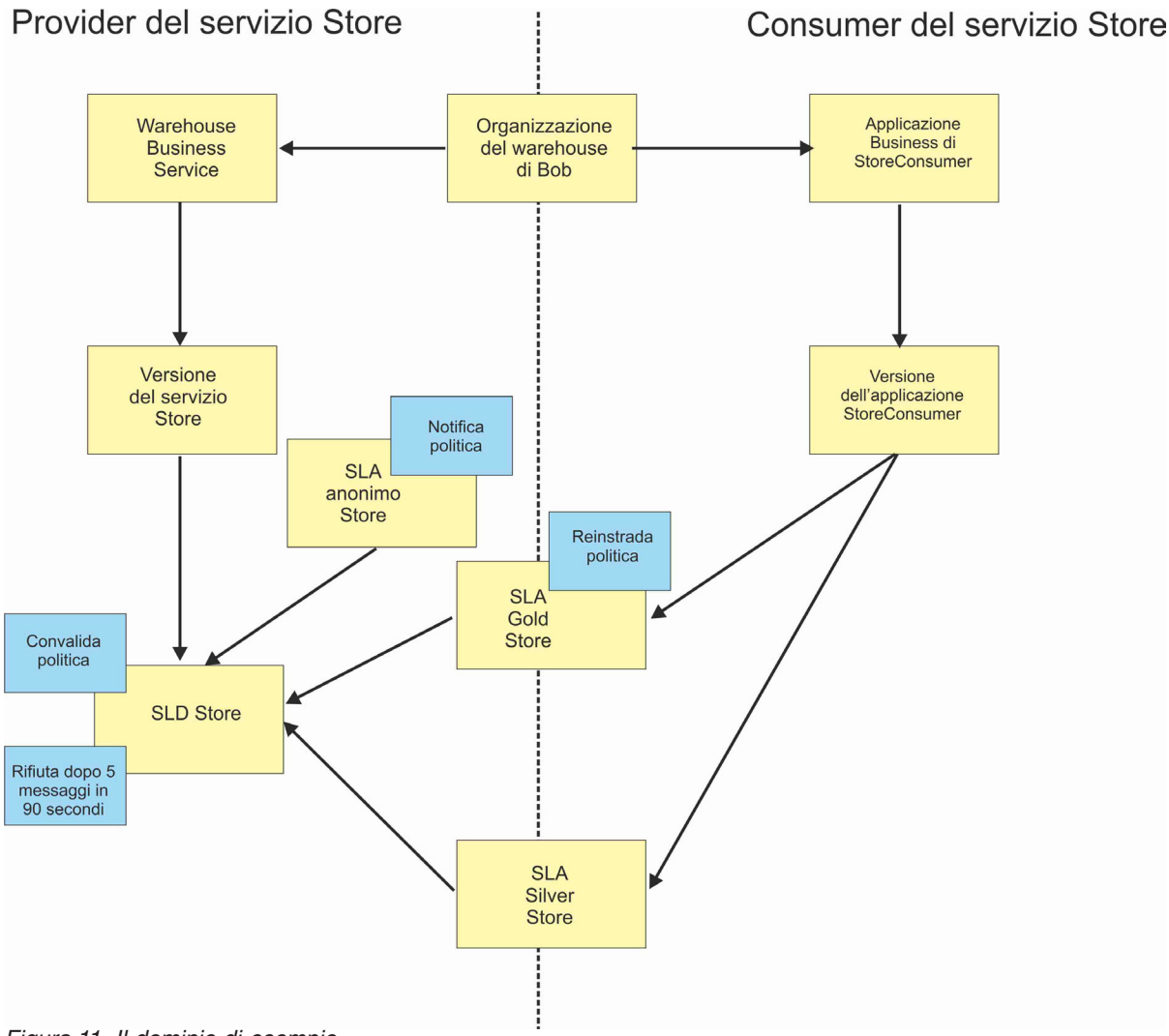


Figura 11. Il dominio di esempio

Esecuzione di scenari di test di esempio

È possibile utilizzare l'applicazione Web di esempio o la riga comandi per eseguire il test dell'applicazione di esempio su SOA Policy Gateway Basic Runtime Sample distribuito. Possono essere eseguite sei variazioni test da riga comandi sull'applicazione di esempio.

Per distribuire il Basic Runtime Sample, consultare "Distribuzione del pattern Basic Runtime Sample" a pagina 49.

Esecuzione dello scenario di test dell'applicazione Web di esempio

Per eseguire lo scenario di test dell'applicazione Web:

1. Individuare il nome host dell'ambiente WSRR distribuito aprendo l'istanza del sistema virtuale distribuito. Per individuare il nome host, espandere la sezione **Macchine virtuali** e selezionare la macchina virtuale del server autonomo WSRR per visualizzarne i dettagli. Nella sezione **Hardware e rete**, il nome host è il valoree **Interfaccia di rete 0**.

2. Aprire l'URL in un browser Web: `http://<wssrHostName>:9080/SoaPolicyTester`
3. Le seguenti opzioni sono disponibili:
   - **Richiesta standard** - Invia una richiesta findInventory al servizio di archivio. L'ID contesto è Silver. L'ID consumer è CEO. Un risultato corretto visualizza il testo "Part: SKU10 Price: 401.73".
   - **Testo politica di instradamento** - Uguale a Richiesta standard, ma con ID contesto di tipo Gold. La richiesta è instradata a un endpoint alternativo eseguendo il servizio. Un risultato corretto restituisce "Part: GOLDSKU10 Price: 401.73".
   - **Test politica di convalida** - Invia una richiesta a un payload non valido. La politica di convalida necessita che DataPower convalidi la richiesta e rifiuti quei messaggi che non sono validi. Un risultato corretto è un messaggio di risposta da DataPower `"Internal Error (from client)"`.
   - **REST Gold** - Invia la richiesta al servizio RESTful SKU con ID consumer CEO e ID contesto Gold. Le richieste Gold sono subordinate a una politica che consente solo 5 messaggi in 90 secondi. Una richiesta corretta visualizza il risultato "Part: SKU33 Price: 136.43".
   - **REST Silver** - Uguale a Rest GOLD, ma con ID contesto Silver. Le richieste Silver sono subordinate a una politica che consente 3 richieste separate in 90 secondi. Una richiesta corretta visualizza il risultato "Part: SKU33 Price: 136.43".
   - **ID utente** - L'opzione ID utente ha due valori possibili; Contenuto completo o Contenuto redatto. Ogni opzione comporta delle richieste provenienti da utenti diversi. L'esempio utilizza una politica XACML, che consente solo ai responsabili la consultazione del prezzo. Il valore di Prezzo nel messaggio di risposta è redatto a meno che Contenuto completo sia selezionato. Un risultato corretto per le richieste quando Contenuto redatto è selezionato contiene "Price: 0.0". Il servizio RESTful non supporta la funzione di redazione. L'utente selezionato non ha alcun effetto.
4. Aprire la console WSRR ed esplorare il servizio e le politiche. Per ulteriori informazioni, consultare "Connessione a WSRR - Business Space" a pagina 82.

L'esempio può essere verificato utilizzando la riga comandi. Questo è l'unico modo per inviare il traffico che utilizza lo SLA anonimo

Descrizione del meccanismo Consenti/Nega XACML con lo scenario di redazione utilizzando la riga comandi

La seguente codifica XML della richiesta può essere inviata a DataPower StoreAddLTPA Service:

```
<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>
```

Supponendo che la codifica XML della richiesta di esempio sia contenuta in un file denominato `silver.xml`, immettere il seguente comando curl:

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

In questo esempio, ConsumerX è un gestore, pertanto le informazioni relative al prezzo pieno sono visibili nella risposta:

```
<?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>
```

Esecuzione dello scenario di redazione utilizzando la riga comandi

ConsumerA non è un responsabile, pertanto visualizza una risposta differente. Immettere il comando curl:

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

Tenere presente che la risposta ha il prezzo redatto. Il prezzo è visualizzato come 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>
```

Verifica della politica di instradamento utilizzando la riga comandi

Affinché la politica di instradamento allegata allo SLA Gold venga applicata, l'ID contesto e l'ID consumer devono corrispondere. In questo caso, lo SLA per i client Gold ha l'ID contesto di tipo Gold, mentre la versione di servizio consumer ha l'ID consumer di tipo CEO. Di seguito è riportato il contenuto di una richiesta di esempio (è possibile visualizzare la corrispondenza dell'ID contesto e dell'ID consumer come richiesto):

```
<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>
```

Supponendo che la codifica XML della richiesta di esempio sia contenuta in un file denominato `gold.xml`, immettere il seguente comando curl:

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

La risposta è riportata di seguito:

```
<?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>
```

Tenere presente che la risposta di ritorno presenta il valore `GOLDSKU` per SKU, per indicare che è stato utilizzato l'endpoint gold.

Verifica della convalida dello schema utilizzando la riga comandi

La politica di convalida controlla lo schema della richiesta sul file Store.wsdl e sul relativo file Company.xsd associato.

Il seguente XML, `badvalid.xml`, mostra una richiesta non valida poiché il corpo contiene un elemento denominato `<skubad>` quando dovrebbe essere `<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>
```

Se si immette la seguente richiesta curl:

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

Viene visualizzato il seguente errore:

```
<?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>
```

Verifica del rifiuto nella politica di mediazione utilizzando la riga comandi

Una delle politiche di mediazione incluse nell'esempio verifica il rifiuto dopo che i messaggi vengono eseguiti 5 volte in 90 secondi. Eseguire il comando riportato di seguito 6 volte:

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

La richiesta di esempio è riportata di seguito:

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
<soapenv:Header>
<KD4NS:KD4SoapHeaderV2
xmlns:KD4NS="http://www.ibm.com/KD4Soap">AFIAAgAkZmExODgzNTQtY2Q1ZC0z
YjU0LWEyMzItZGM3MmEzNWY0MTAzACRmYWVjYjA1Mi1jMWUxLTMyODEtOWY3Ni0wY2IxN
mRhMDc4MjkAAw==</KD4NS:KD4SoapHeaderV2>
</soapenv:Header>
<soapenv:Body>
<b:findInventoryResponse xmlns:a="http://company.ibm.com/"
xmlns:b="http://company.ibm.com/store">
<findInventoryRes>
```

In questo caso, ConsumerX è un Responsabile, pertanto le informazioni relative al prezzo pieno vengono visualizzate come per le prime cinque esecuzioni:

```
<?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>
```

Alla sesta esecuzione si verifica il seguente errore:

```
<?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: Questo errore potrebbe essere visualizzato prima se si eseguono altri test entro l'intervallo di 90 secondi.

Verifica della notifica nella politica di mediazione utilizzando la riga comandi

La politica di notifica viene allegata allo SLA anonimo. Ciò viene applicato quando si riceve una richiesta da un consumer che non dispone di un accordo SLA. In questo esempio, l'unico consumer che dispone di SLA appropriati è CEO, quindi una richiesta contenente l'ID consumer impostato su altro comporta l'applicazione della politica sullo SLA anonimo. In questo caso ConsumerX è un responsabile, quindi vengono visualizzate le informazioni relative al prezzo pieno:

Per verificare questa funzionalità utilizzando la riga comandi, creare un file denominato `anon.xml` contenente il seguente xml:

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

Quindi, immettere il seguente comando:

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

Il seguente messaggio viene emesso nel log predefinito del dominio:

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

Nota: La registrazione deve essere impostata su “notice” per visualizzare questo messaggio. In caso contrario, fare clic sull'icona **Risoluzione dei problemi** nella

console Web DataPower. Nella sezione Registrazione, modificare il valore Livello di registrazione in “notice” e fare clic su **Imposta livello di log**. Per individuare il file di log, ritornare al pannello di controllo e fare clic sull'icona **Visualizza log**.

Verifica del servizio RESTful utilizzando la riga comandi

È possibile inoltre accedere all'interfaccia RESTful dalla riga comandi utilizzando curl. Come con il client Web, un ID contesto di tipo Gold consente 5 messaggi per 90 secondi, mentre Silver solo 2 messaggi.

Per verificare questa funzionalità utilizzando la riga comandi, creare un file denominato restRequest.xml che contiene il seguente xml:

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

Quindi, immettere il seguente comando per eseguire la verifica con ID contesto Gold:

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

Per eseguire la verifica con l'ID contesto Silver, utilizzare lo stesso comando, ma sostituire Gold con Silver.

Una risposta corretta è:

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

Dopo che la soglia è stata raggiunta, viene ricevuto il seguente messaggio:

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

Per acquisire dimestichezza con lo SLA anonimo per il servizio RESTful, che ha semplicemente una politica di notifica allegata, utilizzare un qualsiasi ContextID o ConsumerID diverso da quelli registrati. La notifica appare nel log DataPower come descritto in precedenza per l'esempio dei servizi Web.

Attività correlate:

“Distribuzione del pattern Basic Runtime Sample” a pagina 49
La distribuzione del pattern SOA Policy Gateway Basic Runtime Sample crea un'istanza del sistema virtuale in esecuzione del pattern. Questo pattern è disponibile solo su sistemi x86.

Estensione dell'applicazione di esempio

L'applicazione di esempio può essere modificata modificando il foglio di stile Bindings ed i fogli di stile XSL.

Modifiche al foglio di stile dei bind

Al foglio di stile `apil-xacml-binding-new.xsl` è stata aggiunta la variabile. Comprende la creazione della sezione subjects della richiesta. Questa variabile viene successivamente acceduta in `sendToPDP.xsl`.

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

sendToPDP.xsl

Questo foglio di stile richiama StoreXACMLFW utilizzando url-open. La chiamata è inclusa in un altro firewall XML, quindi non viene utilizzato alcun profilo del proxy SSL. Per rimuovere il PDP (Policy Decision Point) da un altro DataPower, è possibile creare un profilo del proxy SSL con una chiamata url-open.

```
<xsl:param name="resource" />
<!--
<xsl:variable name="incoming_resource">
<xsl:value-of select="$resource" />
</xsl:variable>
<xsl:message dp:priority="debug">
********** ABOUT TO CALL PDP for RESOURCE equal *************
<xsl:value-of select="$incoming_resource" />
</xsl:message>
-->
- <!--
building the XACML request for masking
-->
<xsl:variable name="customized-request">
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
<soapenv:Header />
<soapenv:Body>
<xacml-context:Request xmlns:wsa="http://www.w3.org/2005/08/addressing"
  xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xacml-context="urn:oasis:names:tc:xacml:2.0:context:schema:os"
xmlns:ws="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
wss-wssecurity-secext-1.0.xsd">
- <!--
copy in the subjects saved from AAA request processing
-->
<xsl:copy-of select="dp:variable('var://context/snip/xacml/xacmlSubjects')/*" />
<xacml-context:Resource>
<xacml-context:ResourceContent>
<xsl:copy-of select="./soap:Envelope/soap:Body" />
</xacml-context:ResourceContent>
<xacml-context:Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#string">
<xacml-context:AttributeValue>PriceInfo</xacml-context:AttributeValue>
</xacml-context:Attribute>
</xacml-context:Resource>
<xacml-context:Action>
<xacml-context:Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
DataType="http://www.w3.org/2001/XMLSchema#string">
<xacml-context:AttributeValue>View</xacml-context:AttributeValue>
</xacml-context:Attribute>
</xacml-context:Action>
```

```
<xacml-context:Environment>
<xacml-context:Attribute AttributeId="ContextId" DataType="http://www.w3.org/2001/XMLSchema#string"
Issuer="http://security.tivoli.ibm.com/policy/distribution">
<xacml-context:AttributeValue>StorePriceData</xacml-context:AttributeValue>
</xacml-context:Attribute>
</xacml-context:Environment>
</xacml-context:Request>
</soapenv:Body>
</soapenv:Envelope>
</xsl:variable>
- <!--
Use set-variable so that it is visible in Probe, which is convenient
-->
<dp:set-variable name="'var://context/snip/xacml/BacksideXacmlRequest'" value="$customized-request" />
- <!--
Report the XACML-REQUEST to the debug log
-->
<xsl:message dp:priority="debug">
<XACML-REQUEST>
<xsl:copy-of select="$customized-request" />
</XACML-REQUEST>
</xsl:message>
<xsl:variable name="headers">
<header name="SOAPAction">xacml:authorization</header>
</xsl:variable>
- <!--
Call the XACML PDP for decision
-->
<xsl:variable name="rtss-response">
<xsl:variable name="StoreGWURL">
<xsl:value-of select="concat('http://','127.0.0.1',':',$StoreGWPort,'/rtss/authz/services/AuthzService')" />
</xsl:variable>
<dp:url-open target="{$StoreGWURL}" http-headers="$headers" response="responsecode">
<xsl:copy-of select="$customized-request" />
</dp:url-open>
</xsl:variable>
- <!--
Use set-variable so that it is visible in Probe, which is convenient
-->
<dp:set-variable name="'var://context/snip/xacml/BacksideXacmlResponse'" value="$rtss-response" />
- <!--
Report the XACML-RESPONSE to the debug log
-->
<xsl:message dp:priority="debug">
<XACML-RESPONSE>
<xsl:value-of select="$rtss-response" />
</XACML-RESPONSE>
</xsl:message>
</xsl:template>
</xsl:stylesheet>
```

Tenere presente quanto segue in relazione al file `sendToPDP.xsl`:

1. Il foglio di stile ottiene la porta di XACMLFW da `soavars.xsl`.
2. La variabile rtssResponse deve essere esattamente nel formato utilizzato dai Servizi di sicurezza runtime e nel formato che il PDP incluso in DataPower può elaborare.
3. Il foglio di stile genera una richiesta SOAP. Le informazioni relative all'oggetto sono generate dal foglio di stile `apil-binding.xsl` e ricavate dalla seguente copia della richiesta select:

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

4. L'azione serve semplicemente a visualizzare l'azione: `<xacml-context:AttributeValue>View</xacml-context:AttributeValue>`

5. L'ambiente è StorePriceData, noto come Oggetto applicazione nella terminologia di IBM Tivoli Security Policy Manager o dei Servizi di sicurezza runtime.

StorePrivateDataXACML.xml

Il codice seguente mostra il foglio di stile della politica utilizzato per la redazione.

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

Tenere presente quanto segue:

- Il ruolo deve essere Manager:

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

- La risorsa deve essere PriceInfo:

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

- L'azione deve essere 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>
```

Modifica dei fogli di stile XSL di esempio

È possibile modificare il foglio di stile di revisione, `noPriceInfo.xsl`

Procedura

Modificare il foglio di stile di revisione.
Il foglio di stile `noPriceInfo.xsl` contiene il codice riportato di seguito, che sostituisce i valori del prezzo con degli zeri. È possibile aggiungere altri campi alla logica di revisione oppure aggiungere ulteriori trasformazioni complesse che implicano il calcolo per determinare i valori dei campi.

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

Successivamente, il foglio di stile esegue una trasformazione di identità su tutti gli altri elementi.

Ulteriore esplorazione dell'esempio

Per ulteriori informazioni sull'esempio, è possibile configurare il PDP (Policy Decision Point) XACML su DataPower e modificare i documenti della politica.

Modifica del PDP XACML PDP in DataPower

È possibile modificare l'XACML utilizzato per il PDP (Policy Decision Point) della sicurezza in DataPower per ulteriori informazioni relative al controllo accessi con XACML.

Procedura

Per modificare o aggiungere un PDP:

1. Dal pannello di controllo DataPower, ricercare `PDP XACML`.
2. Fare clic su un PDP esistente oppure fare clic su **Aggiungi**.
3. Immettere un URL, ad esempio `local:///storePrivateDataXACML.xml`.
4. Aggiungere eventuali file di directory o dipendenti necessari per supportare la politica.

   Nota: Se un file della politica XACML viene modificato direttamente sul file system, è necessario tornare alla definizione di PDP ed immettere nuovamente l'URL o eventuali altre informazioni modificate oppure riavviare il dominio per rendere effettive le modifiche.

Aggiunta o modifica di documenti della politica nuovi o esistenti

Utilizzare l'interfaccia utente Business Space per aggiungere nuovi documenti della politica o modificare documenti esistenti.

Prima di iniziare

Configurare lo spazio SOA Governance. Per ulteriori informazioni, consultare “Configurazione di Business Space per il primo utilizzo” a pagina 83.

Procedura

1. Creare una politica di mediazione con le condizioni e le azioni richieste; ad esempio, una condizione Conteggio messaggi > 5 messaggi in 5 minuti ed un'azione di rifiuto. Per ulteriori informazioni relative alla creazione di una politica di mediazione, consultare “Authoring di nuove politiche di mediazione” a pagina 97.
2. Gestire la politica di mediazione. Per ulteriori informazioni relative alla gestione di un documento della politica, consultare “Gestione del ciclo di vita della politica” a pagina 100.
   a. Fare clic sul documento della politica in Navigator del registro del servizio oppure ricercarlo nel widget di ricerca. Le azioni sono visualizzate nell'editor dei documenti delle politiche.
   b. Fare clic su **Proponi specifica**.
   c. Fare clic su **Approva specifica**.

   La politica viene approvata. È possibile ridefinire, sostituire o rendere obsoleta la politica per gestire il ciclo di vita oppure modificare una definizione esistente.
3. Allegare la politica. In Business Space, individuare la SLD o lo SLA a cui si desidera allegare la politica. In questo esempio, è possibile effettuare questa operazione in quattro punti:
   - SLD Store - allegare la politica in questo punto se si desidera che venga applicata a qualsiasi utilizzo del servizio Store.
   - SLA Gold - allegare la politica in questo punto se si desidera che venga applicata solo alle richieste Gold dal consumer CEO.
   - SLA Silver - allegare la politica in questo punto se si desidera che venga applicata solo alle richieste Silver dal consumer CEO.
   - SLA anonimo - allegare la politica in questo punto se si desidera che venga applicata a qualsiasi richiesta proveniente da consumer diversi da CEO.

Attività correlate:

“Authoring di nuove politiche di mediazione” a pagina 97
È possibile creare nuove politiche di mediazione utilizzando l'interfaccia utente Business Space. Quando vengono create le politiche di mediazione, vengono specificate le condizioni e le azioni per la politica.

“Gestione del ciclo di vita della politica” a pagina 100
Le politiche possono essere trasferite da uno stato di governance all'altro utilizzando l'interfaccia utente Business Space. Per essere applicate da DataPower, le politiche devono trovarsi nello stato Approvato.

Informazioni correlate:

Centro informazioni di IBM WebSphere Service Registry and Repository Versione 8.0 - Using the Business Space user interface

Il dominio di esempio DataPower

Il pattern fornisce un dominio DataPower di esempio, che consente all'utente di iniziare ad utilizzare il pattern. In qualità di sviluppatore DataPower, è possibile utilizzare i gateway esistenti come template per le proprie applicazioni. L'ambiente di esempio contiene cinque gateway. Vi è un gateway primario per il servizio

Store, e quattro gateway di supporto che forniscono backend di esempio del gateway Store da chiamare, il supporto XACML per uno scenario di redazione ed un front end per la fornitura delle funzionalità di sicurezza supplementari.

Web Service Proxy Store

Il WSP (Web Service Proxy) Store è il gateway primario del dominio dell'applicazione. Riceve una richiesta con allegato un token LTPA.

Su richiesta, la regola di elaborazione della richiesta porta a termine le seguenti azioni:

1. Convalida la richiesta, come definito nella politica di convalida. Per ulteriori informazioni, consultare "Panoramica sulle risorse WSRR presenti nell'esempio" a pagina 59.
2. Instrada la richiesta all'endpoint alternativo se lo SLA (service level agreement) è "Gold".
3. Effettua l'autenticazione, porta a termine l'autorizzazione e l'accounting (AAA) della richiesta. L'autenticazione prevede quanto segue:
   a. Autentica l'utente con un token LTPA.
   b. Associa le credenziali sul server LDAP che fornisce informazioni quali il gruppo a cui il cliente appartiene. Questi gruppi includono Manager, Commesso e Cliente.
   c. Trasforma l'input fornito in un oggetto richiesta che il PDP (policy decision point) di XACML possa comprendere.
   d. Completa l'autorizzazione mediante un PDP XACML nella casella DataPower, con un documento della politica XACML che può essere creato in IBM Tivoli Security Policy Manager. Il criterio della politica è che l'utente debba essere un Manager, Cliente, Commesso. Per l'operazione findInventory, le restituzioni richiedono un Manager o un Commesso, e gli acquisti possono essere effettuati dai clienti.
4. Imposta il valore ConsumerID mediante script XSL.
5. Rimuove completamente l'intestazione di sicurezza HTTP dalla richiesta.
6. Chiama il back end del servizio Store.

Una volta elaborata la richiesta, la regola di elaborazione della risposta completa le seguenti azioni:

1. Chiama il gateway StoreXACMLFW ed agisce come PDP nello scenario.
2. A seconda della risposta, viene redatto il campo relativo alle informazioni sul prezzo (azzerato) a seconda che l'utente abbia o meno il ruolo Manager.

I firewall XML nell'esempio

Nell'esempio vengono definiti i seguenti filewall XML.

Firewall XML StoreAddLTPA

La funzione del firewall XML StoreAdd LTPA è quella di fornire un front end con una porta che gli utenti possono chiamare utilizzando semplicemente l'autenticazione di base (ad es., senza LTPA). La regola di elaborazione della richiesta:

1. Si identifica con l'autenticazione di base.
2. Si autentica con una ricerca LDAP semplice.
3. Aggiunge un token LTPA come parte della post-elaborazione.
4. Inoltra la richiesta alla politica di sicurezza StoreWSP con le informazioni LTPA ora allegate.

Firewall XML StoreMockService

StoreMockService è un servizio di esempio che utilizza un firewall XML come implementazione. Sono supportate le operazioni findInventory, purchase e return. I valori di risposta sono statici. Questo servizio di esempio viene creato quando non è possibile includere un WebSphere Application Server nel pattern. Le tre regole di richiesta della politica utilizzano un'azione corrispondente per determinare l'operazione request ed, in base ad una corrispondenza, rispondono con una risposta SOAP statica. Le risposte SOAP statiche vengono fornite in base all'operazione request invece che in base ad un'implementazione del servizio completo.

Firewall XML StoreMockServiceAlternate

StoreMockServiceAlternate è un servizio di esempio che utilizza un firewall XML come implementazione. Sono supportate le operazioni findInventory, purchase e return. Questo servizio viene utilizzato per dimostrare l'applicazione della politica di instradamento.

Firewall StoreXACMLFW

Questo scenario esegue la redazione in base al risultato di un meccanismo consenti/nega basato su XACML. In DataPower, non è possibile richiamare un'azione AAA singola nel flusso di risposta. Per contenere un PDP (Policy Decision Point) XACML viene creato un gateway separato. Questo PDP viene incapsulato in un'azione AAA nella regola di richiesta del firewall StoreXACMLFW.

StoreXACMLFW è un gateway del firewall XML in DataPower. Questa implementazione viene utilizzata perché rappresenta un modo semplice per fornire la funzionalità. Il firewall StoreXML utilizza la stessa interfaccia WSDL dei Servizi di sicurezza runtime del server Tivoli. Il gateway StoreWSP crea l'oggetto richiesta e lo invia, protetto da SSL, al gateway StoreXMLFW.

La regola di richiesta del firewall StoreXML esegue le seguenti attività:

1. Esegue AAA utilizzando le informazioni SSL per l'autenticazione.
2. Esegue l'autorizzazione utilizzando un PDP XACML incluso. La politica che viene utilizzata dal PDP viene originariamente creata in IBM Tivoli Security Policy Manager ma può essere ricreati utilizzando un editor standard, e lo schema è definito nella specifica XACML.
3. In questo processo di autorizzazione non è necessaria alcuna trasformazione della richiesta.
4. Se la richiesta XACML è valida, la regola di elaborazione della richiesta recupera una risposta di autorizzazione e ritorna al client. In caso contrario, si verifica un'eccezione che viene gestita dalla regola di elaborazione delle eccezioni e restituisce una risposta Nega al client.

Nota: Consenti/Nega/Indeterminato è solo un esempio di risposta. Nel flusso specifico del cliente è possibile aggiungere ulteriori informazioni sugli errori.

Politica di sicurezza XACML

Questo argomento descrive il modo in cui i documenti XACML vengono creati.

I documenti XACML utilizzati nell'esempio sono stati creati dall'editor di politiche IBM Tivoli Security Policy Manager, ma è possibile utilizzare un qualsiasi editor di

testo o XML per creare documenti di questo tipo. Per creare o modificare le politiche XACML esistenti, consultare le specifiche OASIS: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml.

La politica di sicurezza XACML utilizzata nell'esempio è contenuta in `storeSWPXACML.xml` e `storePrivateDataXACML.xml`. Tali politiche vengono utilizzate per valutare la richiesta in entrata al PDP (Policy Decision Point). La richiesta è costituita da quattro elementi chiave:

1. Sezione Subjects - Contiene i dettagli del DN (Distinguished Name) del chiamante della richiesta, nonché i gruppi a cui il chiamante appartiene.
2. Sezione Resource - Contiene i documenti a cui il chiamante desidera avere accesso. Nell'esempio vengono utilizzati due tipi di risorsa. Il primo tipo è l'operazione sul servizio Web, mentre il secondo tipo è l'autorizzazione ai dati nella risposta, in questo caso la risorsa priceInfo.
3. Sezione Environment - Contiene informazioni sull'ambiente della richiesta.
4. Azione - Finalità di utilizzo del materiale autorizzato da parte dell'utente. Nello scenario di redazione, l'azione consiste semplicemente nel visualizzare i dati priceInfo.

Politica di sicurezza StoreWSP

La politica di sicurezza nel file `storeSWPXACML.xml` associa i gruppi a operazioni del servizio Web.

Una politica di sicurezza di esempio è riportata di seguito:

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

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

Nota: Nella sezione subjects, una corrispondenza si verifica sul nome x500 o sul ruolo oggetto di Manager. Se si esamina l'intera politica del file `.xml`, è possibile osservare che vi sono associazioni analoghe per Customer e Clerk. È possibile osservare che l'operazione findInventory è autorizzata per utilizzare tutti i tre gruppi, mentre le operazioni returnProduce e purchase sono limitate solo a determinati gruppi.

Il Gateway Redazione

Dettagli relativi al foglio di stile storeCallPDP.xsl.

Esaminare il foglio di stile storeCallPDP.xsl e considerare i seguenti punti:

1. L'inclusione del foglio di stile storeSendToPDP.xsl. Questo foglio di stile contiene la logica per richiamare storeXAMLFW.
2. Per richiamare il template call_PDP in storeSendToPDP.
3. L'estrazione della decisione dalla risposta alla chiamata, ad esempio “Consenti”.
4. L'impostazione del valore `var:/context/response/displayfilter` con i fogli di stile allData.xsl o noPriceInfo.xsl.
5. La struttura in XACML per Reaction, storePrivateDataXACML.xml, è praticamente identica alla struttura utilizzata nello scenario StoreWSP. La differenza consiste nel consentire l'accesso solo al ruolo Manager.

storeCallPDP.xsl

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

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

Risorse WSRR create in SOA Policy Gateway Basic Runtime Sample

Le risorse WSRR create nel pattern SOA Policy Gateway Basic Runtime Sample e come vengono utilizzate dall'esempio.

Tabella 14. Risorse WSRR create per il pattern SOA Policy Gateway Basic Runtime Sample

Oggetto	Descrizione
Organizzazione	Warehouse di Bob. Questa è l'area di business che possiede il servizio Store
Capability di business	Warehouse. Esso rappresenta tutte le versioni del servizio Store ed è posseduto dall'organizzazione del warehouse di Bob.
Versione del servizio	Store. Esso rappresenta la versione 1.0 del servizio Store.
WSDL	Store.wsdl
XSD	Company.xsd
Politica	• Validate.xml • RouteForGold.xml • LogEveryTime.xml • RejectAfter5MsgIn90Seconds.xml
SLD	SLD Store. Tutte le politiche allegate qui si applicano a qualsiasi richiesta per questo servizio.
SLA Gold	SLA Gold. L'esistenza di questo SLA indica che le richieste Gold del consumer CEO non devono essere conteggiate come anonime. Tutte le politiche allegate qui vengono applicate su richieste Gold dal CEO.
SLA Silver	SLA Silver. L'esistenza di questo SLA indica che le richieste Silver del consumer CEO non vengono conteggiate come anonime. Con nessuna politica allegata, la richiesta è comunque consentita.
SLA anonimo	Utenti anonimi. Le politiche allegate qui vengono applicate a qualsiasi richiesta che non dispone di uno SLA corrispondente. In questo esempio, qualsiasi richiesta di un consumer diverso da CEO, oppure qualsiasi richiesta da CEO che non è Gold o Silver ha le politiche di SLA anonimo applicate ad essa.

Risorse DataPower create in SOA Policy Gateway Basic Runtime Sample

Le risorse DataPower create nel pattern SOA Policy Gateway Basic Runtime Sample.

Tabella 15. Risorse DataPower create per il pattern SOA Policy Gateway Basic Runtime Sample

Tipo	Nome	Scopo
Proxy dei servizi Web	StoreWSP	Il servizio principale.
Firewall XML	StoreAddLTPA StoreMockService StoreAlternateMockService StoreXACMLFW	Autentica ed aggiunte il token LTPA. Il provider del servizio dei clienti non Gold Il provider del servizio dei clienti Gold Verifica l'accesso a PriceInfo.
Server WSRR	WSRRSVR	La connessione a WSRR.
Sottoscrizione WSRR	StoreSub	Fornisce informazioni di ricerca per l'oggetto, lo spazio dei nomi WSRR e così via.
Politica AAA	StoreAddLTPA	Identificazione ed autenticazione di base per LDAP. Controlla l'autenticazione. Aggiunge il token LTPA alla richiesta.
Politica AAA	StoreWSDLAAA	Identificazione ed autenticazione LTPA. Associazione gruppi per l'autorizzazione. Autorizzazione XACML.
Politica AAA	StoreXACMLFWAZ	Autorizzazione XACML per PriceInfo.
Profilo del proxy SSL	WSRRPP	Profilo del proxy SSL del server WSRR.
Profilo crittografato	WSRRCP	Il profilo crittografato del server WSRR.
Credenziali di convalida	WSRRVC	Credenziali di convalida contengono il certificato crittografato WSRRCERT. Tutte le altre impostazioni sono predefinite.
Certificato crittografato	WSRRCERT	WSRRCERT utilizza il certificato del firmatario. Questo certificato è stato estratto dal NodeDefaultKeyStore, dal certificato predefinito di un singolo server, o dal certificato predefinito CMSKeyStore nel caso di un ambiente ND in cui è presente un IBM HTTP Server.

Le regole di elaborazione del WSP (Web Service Proxy) StoreWSP

Il gateway centrale dell'esempio è StoreWSP. La politica del gateway contiene una regola di richiesta e risposta.

Regola di richiesta

L'azione della politica primaria della StoreWSP_default_request-rule è denominata AAA. Nell'azione AAA, il token LTPA viene convalidato, i gruppi di utenti vengono richiamati, e viene effettuata un'autorizzazione per verificare se l'utente è contenuto nel gruppo LDAP Manager, Commessi o Clienti del gruppo LDAP. Questa convalida viene eseguita quando il passo AZ di AAA chiama il PDP (Policy Decision Point) StoreWSDLPDP, sul dispositivo DataPower. Questo PDP utilizza la politica XACML storeWSPXACML.xml.

Regola di risposta

Nella regola di risposta, StoreWSP_default_response-rule, la trasformazione chiama il servizio firewall XML StoreXACMLFW.

Questa trasformazione determina se l'utente è autorizzato ad accedere alle informazioni sul prezzo in base a se l'utente è un membro del gruppo Manager. Se lo è, la variabile *var:///context/response/displayFilter* è impostata su `local:///allData.xsl`. Se non è membro del gruppo LDAP Manager, la variabile *var:///context/response/displayFilter* è impostata su `local:///noPriceInfo.xsl`.

La trasformazione esegue quindi le azioni del foglio di stile sulla risposta.

Regole di elaborazione StoreXAMLFW

Il foglio di stile personalizzato storeSendToPDP.xsl chiama il firewall XML locale StoreXACMLFW. In questo firewall vengono utilizzate due regole di elaborazione. StoreXACMLFW_request contiene una singola azione della politica AAA che utilizza la trasformazione allData.xsl. Questa azione AAA, StoreXACMLFWAZ, a sua volta chiama l'azione StorePDP del PDP XACML. Utilizzando la politica XACML storePrivateDataXACML.xml, si verifica se l'utente è autorizzato ad accedere alle informazioni sui prezzi.

Fogli di stile XSL di esempio

L'applicazione di esempio contiene i seguenti fogli di stile che terminano con `.xsl`, presenti nella directory locale del dominio installato.

Tabella 16. Fogli di stile nell'applicazione di esempio

Foglio di stile	Scopo
`allData.xsl`	Un foglio di stile dell'identità che copia tutti i dati dall'origine alla destinazione. Viene utilizzato sia per la funzione di redazione che per la chiamata al gateway XML XACML.
`apil-xacml-binding-new.xsl`	Utilizza le informazioni di associazione delle credenziali per creare una richiesta SOAP che può essere elaborata dal dispositivo DataPower PDP (Policy Decision Point). Questo foglio di stile è una modifica del foglio di stile tspm-xacml-binding-sample.xsl fornito nella directory di archivio del dispositivo DataPower. La funzionalità chiave fornita da questo script adattato è di aggiungere una variabile accessibile esternamente che rende le informazioni sull'oggetto della richiesta XACML disponibile al foglio di stile di redazione.
`noPriceInfo.xsl`	Questo foglio di stile imposta l'elemento prezzo a un valore pari a 0.0.

Tabella 16. Fogli di stile nell'applicazione di esempio (Continua)

Foglio di stile	Scopo
rgxacml.xsl	Questo foglio di stile è una personalizzazione del foglio di stile tspm-retrieve-groups.xsl nella directory di archivio del dispositivo DataPower. Lo scopo primario di questo foglio di stile è di fornire il DN LDAP, il nome host, la password, la porta e così via, in modo che l'utente in entrata possa essere ricercato e le relative informazioni sul gruppo richiamate.
soavars.xsl	Questo foglio di stile è un esempio che definisce le informazioni LDAP in variabili utilizzate dal foglio di stile rgxacml.xsl. Nell'esempio la password è decodificata, che non è una pratica di produzione.
storeCallPDP.xsl	Questo foglio di stile dispone del codice per chiamare il gateway XACML, gestisce la decisione Consenti/Nega e imposta la variabile di filtro per eseguire allData.xsl o noPriceInfo.xsl.
storeSendToPDP.xsl	Questo foglio di stile crea una richiesta SOAP inviata al gateway XACML. Include le informazioni sull'oggetto ottenute dal foglio di stile apil-xacml-binding-new.xsl e le informazioni sulla risorsa, sull'azione e sull'ambiente.

Oggetti DataPower che utilizzano i fogli di stile XSL

Gli oggetti DataPower utilizzano alcuni fogli di stile XSL forniti con l'applicazione di esempio.

Tabella 17. Oggetti DataPower che utilizzano i fogli di stile XSL

Foglio di stile	Scopo
allData.xsl	Utilizzato internamente nel foglio di stile storeCallPDP.xsl. Il foglio di stile è utilizzato come conversione personalizzata in AAA policy StoreXACMLFWAZ.
apil-xacml-binding-new.xsl	Utilizzato nel foglio di stile personalizzato del passo StoreWSDLAAA AAA policy AZ.
noPriceInfo.xsl	Utilizzato nel foglio di stile storeCallPDP.xsl.
soavars.xsl	Utilizzato internamente nel foglio di stile rgxacml.xsl.
storeCallPDP.xsl	Chiamato come conversione nella regola Store_default-response.
storeSendToPDP.xsl	Utilizzato internamente nel foglio di stile storeCallPDP.xsl.

Capitolo 6. Utilizzo dell'istanza distribuita

Una volta distribuito uno dei IBM SOA Policy Gateway Pattern, è possibile visualizzare l'istanza distribuita facendo clic su **Istanze** > **Sistemi virtuali** in Workload Console.

Visualizzazione dei dettagli dell'istanza

È possibile visualizzare i dettagli di un'istanza distribuita selezionandola dall'elenco delle istanze nella finestra Istanze del sistema virtuale. Vengono visualizzati i dettagli dell'istanza del sistema virtuale. I dettagli includono un elenco delle macchine virtuali di cui è stato eseguito il provisioning nell'infrastruttura cloud per tale distribuzione, l'indirizzo IP e lo stato della macchina virtuale.

Per visualizzare lo stato di distribuzione e provisioning dell'istanza, osservare il valore **Stato corrente** nella vista dettagli.

Per visualizzare lo stato degli script e delle macchine virtuali durante il provisioning, espandere la sezione **Cronologia** nella vista dettagli.

Per visualizzare i dettagli dei log degli script e delle macchine virtuali, espandere la sezione **Macchine virtuali** nella vista dettagli. L'host e l'indirizzo IP del sistema sono il valore **Interfaccia di rete 0** nella sezione **Hardware e rete**. I log degli script sono accessibili nella sezione **Package di script**. È possibile effettuare a qualsiasi console disponibile utilizzando i link nella sezione **Console**.

Accesso alle istanze distribuite

Una volta distribuito un pattern del sistema virtuale, è possibile visualizzare le istanze del sistema virtuale create per visualizzare il proprio ambiente IBM SOA Policy Gateway Pattern ed accedere alle relative parti.

Prima di iniziare

Per visualizzare un'istanza del sistema virtuale, è necessario prima distribuire un pattern del sistema virtuale.

Informazioni su questa attività

La distribuzione di un pattern crea un'istanza del sistema virtuale oppure un ambiente runtime IBM SOA Policy Gateway Pattern di cui è appena stato eseguito il provisioning. Una volta completata la distribuzione, l'istanza del sistema virtuale è in esecuzione.

Procedura

Per gestire le istanze del sistema virtuale IBM SOA Policy Gateway Pattern, effettuare le operazioni riportate di seguito:

1. Fare clic su **Istanze** > **Sistemi virtuali** per visualizzare la finestra Istanze del sistema virtuale.

2. Dall'elenco delle istanze nella finestra Istanze del sistema virtuale, selezionare l'istanza distribuita.
3. Se l'istanza è in esecuzione, è possibile accedere ai componenti del sistema virtuale dai link della console nella vista del sistema virtuale. I componenti disponibili dipendono dal pattern creato. Essi possono includere:
   - Console di gestione di WebSphere Application Server
   - UI Web di WSRR
   - WSRR Business Space
   - WebGUI DataPower

Connessione a WSRR - Business Space

Utilizzare l'interfaccia utente Business Space per utilizzare WSRR.

Informazioni su questa attività

Business Space è una delle due interfacce grafiche che è possibile utilizzare con WSRR. Una descrizione completa dell'utilizzo di Business Space con WSRR è disponibile nel Centro informazioni di WSRR (consultare il link correlato).

È possibile effettuare la connessione a Business Space dell'istanza WSRR nel pattern distribuito facendo clic su un link in Workload Console oppure immettendo l'URL in un browser Web.

Procedura

1. Per effettuare la connessione da Workload Console:
   a. Fare clic su **Istanze** > **Sistemi virtuali** per visualizzare la finestra Istanze del sistema virtuale.
   b. Dall'elenco delle istanze nella finestra Istanze del sistema virtuale, selezionare il proprio sistema distribuito.
   c. Fare clic su **Macchine virtuali** nella vista dettagli del sistema distribuito per espandere l'elenco.
   d. Individuare WSRR nell'elenco delle macchine virtuali e fare clic sul simbolo di addizione per visualizzare i dettagli.
   e. Nella sezione **Console**, fare clic su **WSRR_Business_Space**.
   f. Immettere l'ID utente di gestione di WSRR e la password.
2. Per effettuare la connessione da un browser Web:
   a. Aprire un browser Web.
   b. Individuare il nome host ed i numeri di porta per WSRR. Visualizzare i dettagli della propria distribuzione come descritto al passo 1. Espandere la sezione **Macchine virtuali** e selezionare la macchina virtuale per il server WSRR per visualizzare i dettagli della macchina virtuale. Nella sezione **Hardware e rete**, il nome host è il valore **Interfaccia di rete 0**.
   c. Immettere l'URL della UI Web WSRR: http://*hostname*:9443/BusinessSpace, dove *hostname* è il nome host del server WSRR.
   d. Immettere l'ID utente di gestione di WSRR e la password.

Risultati

Viene visualizzata l'interfaccia Business Space, che può essere utilizzata per aggiungere, modificare o rimuovere politiche di mediazione ed altre risorse utente WSRR.

Operazioni successive

Se Business Space viene utilizzato sul sistema WSRR per la prima volta, consultare "Configurazione di Business Space per il primo utilizzo" e seguire i passi per la creazione dello spazio SOA Governance.

Informazioni correlate:

Centro informazioni di IBM WebSphere Service Registry and Repository Versione 8.0

Configurazione di Business Space per il primo utilizzo

Prima di poter utilizzare l'interfaccia utente Business Space per creare politiche, è necessario creare lo spazio SOA Governance.

Prima di iniziare

Per informazioni relative all'accesso a Business Space, consultare "Connessione a WSRR - Business Space" a pagina 82.

Informazioni su questa attività

Per utilizzare i widget di Business Space, è necessario creare uno spazio. Gli spazi sono definiti per ruoli specifici. L'authoring della politica è più adatto per l'utilizzo nello spazio SOA Governance. Se uno spazio SOA Governance non esiste ancora, è necessario crearlo. Per creare uno spazio basato sul template Registro del servizio per SOA Governance, effettuare le operazioni riportate di seguito:

Procedura

1. Fare clic su **Gestisci spazi** nella parte superiore della pagina. Viene visualizzata la finestra Gestore spazio.
2. Fare clic su **Crea spazio**. Viene visualizzata la finestra di dialogo Crea spazio.
3. Immettere un nome nel campo **Nome spazio**; ad esempio, `SOA Governance`. Come opzione, immettere una descrizione.
4. Selezionare **Registro del servizio per SOA Governance** dall'elenco **Crea un nuovo spazio utilizzando un template**, quindi fare clic su **Salva**.
5. Il nuovo spazio viene visualizzato nell'elenco **Gestore spazio**. Fare clic sul nuovo spazio per aprirlo.

Risultati

Viene creato lo spazio SOA Governance. Per aprire lo spazio SOA Governance:

1. Fare clic su **Vai a spazi** nella parte superiore della pagina. Viene visualizzata la finestra di dialogo Vai a spazi.
2. Fare clic sullo spazio per gli utenti SOA Governance. Il nome specifico dipende dalle informazioni specificate durante la creazione dello spazio.

Operazioni successive

È possibile aggiungere ulteriori azioni al widget Azioni del registro del servizio:

1. In Business Space, fare clic su **Modifica pagina**.
2. Nel widget Azioni del registro del servizio, fare clic su **Modifica impostazioni**.
3. Selezionare le seguenti azioni per la visualizzazione:
   - Crea una SLD (Service Level Definition)

- Crea una versione servizio
- Crea uno SLA (Service Level Agreement)
- Crea una capability di business

4. Nel widget Azioni del registro del servizio, fare clic su **Salva e chiudi**.
5. Fare clic su **Termina modifica**.

Connessione a WSRR - UI Web di WSRR

Utilizzare la UI Web di WSRR per utilizzare WSRR.

Informazioni su questa attività

La UI Web di WSRR è una delle due interfacce grafiche che è possibile utilizzare con WSRR. Una descrizione completa relativa all'utilizzo della UI Web WSRR è disponibile nel centro informazioni di WSRR (vedere il link correlato). Nella maggior parte dei casi, potrebbe essere preferibile utilizzare l'interfaccia Business Space, ma alcune attività (come la creazione delle politiche di monitoraggio) devono essere completate nella UI Web di WSRR.

È possibile effettuare la connessione alla UI Web di WSRR di un'istanza WSRR nel proprio pattern distribuito facendo clic su un link in Workload Console oppure immettendo l'URL in un browser Web.

Procedura

1. Per effettuare la connessione da Workload Console:
   a. Fare clic su **Istanze** > **Sistemi virtuali** per visualizzare la finestra Istanze del sistema virtuale.
   b. Dall'elenco delle istanze nella finestra Istanze del sistema virtuale, selezionare il proprio sistema distribuito.
   c. Fare clic su **Macchine virtuali** nella vista dettagli del sistema distribuito per espandere l'elenco.
   d. Individuare WSRR nell'elenco delle macchine virtuali e fare clic sul simbolo di addizione per visualizzare i dettagli.
   e. Nella sezione **Console**, fare clic su **WSRR_Web_UI**.
   f. Immettere l'ID utente di gestione di WSRR e la password.
2. Per effettuare la connessione da un browser Web:
   a. Aprire un browser Web.
   b. Individuare il nome host ed i numeri di porta per WSRR. Visualizzare i dettagli della propria distribuzione come descritto al passo 1. Espandere la sezione **Macchine virtuali** e selezionare la macchina virtuale per il server WSRR per visualizzare i dettagli della macchina virtuale. Nella sezione **Hardware e rete**, il nome host è il valore **Interfaccia di rete 0**.
   c. Immettere l'URL della UI Web di WSRR: http://*hostname*:9443/ServiceRegistry, dove *hostname* è il nome host del server WSRR.
   d. Immettere l'ID utente di gestione di WSRR e la password.

Informazioni correlate:

Centro informazioni di IBM WebSphere Service Registry and Repository Versione 8.0

Connessione alla console di gestione di WebSphere Application Server

Utilizzare la console di gestione di WebSphere Application Server per ottimizzare le impostazioni di sicurezza e completare altre attività di gestione.

Informazioni su questa attività

I dettagli completi relativi all'utilizzo della console di gestione di WebSphere Application Server sono contenuti nel Centro informazioni. Seguire il link correlato.

È possibile effettuare la connessione alla console di gestione di WebSphere Application Server nel proprio pattern distribuito facendo clic su un link in Workload Console oppure immettendo l'URL in un browser Web.

Procedura

1. Per effettuare la connessione da Workload Console:
   a. Fare clic su **Istanze** > **Sistemi virtuali** per visualizzare la finestra Istanze del sistema virtuale.
   b. Dall'elenco delle istanze nella finestra Istanze del sistema virtuale, selezionare il proprio sistema distribuito.
   c. Fare clic su **Macchine virtuali** nella vista dettagli del sistema distribuito per espandere l'elenco.
   d. Individuare WSRR nell'elenco delle macchine virtuali e fare clic sul simbolo di addizione per visualizzare i dettagli.
   e. Nella sezione **Console**, fare clic su **WebSphere**.
   f. Immettere l'ID utente di gestione di WSRR e la password.
2. Per effettuare la connessione da un browser Web:
   a. Aprire un browser Web.
   b. Individuare il nome host ed i numeri di porta per WSRR. Visualizzare i dettagli della propria distribuzione come descritto al passo 1. Espandere la sezione **Macchine virtuali** e selezionare la macchina virtuale per il server WSRR per visualizzare i dettagli della macchina virtuale. Nella sezione **Hardware e rete**, il nome host è il valore **Interfaccia di rete 0**.
   c. Immettere l'URL della UI Web WSRR: http://*hostname*:9043/ibm/console, dove *hostname* è il nome host del server WSRR.
   d. Immettere l'ID utente di gestione di WSRR e la password.

Informazioni correlate:

Centro informazioni di WebSphere Application Server V8.0

Connessione alla console di un DataPower virtuale

Utilizzare la console DataPower per configurare il PEP (Policy Enforcement Point).

Informazioni su questa attività

I dettagli completi relativi alla configurazione del gateway sono contenuti nel Centro informazioni di WebSphere DataPower. Seguire il link correlato.

La connessione alla console viene effettuata utilizzando un browser Web. È possibile richiamare i dettagli della connessione visualizzando i dettagli del pattern distribuito in Workload Console.

Procedura

1. Richiamare i dettagli necessari utilizzando Workload Console:
   a. Fare clic su **Istanze** > **Sistemi virtuali** per visualizzare la finestra Istanze del sistema virtuale.
   b. Dall'elenco delle istanze nella finestra Istanze del sistema virtuale, selezionare il proprio sistema distribuito.
   c. Nella vista dettagli, espandere la sezione **Macchine virtuali** e selezionare la macchina virtuale per il dispositivo DataPower per visualizzare i dettagli della macchina virtuale. Nella sezione **Hardware e rete**, il nome host è il valore **Interfaccia di rete 0**.
2. Aprire un browser Web ed immettere l'URL `https://`*`hostname`*`:9090/dp`, dove *hostname* è il nome host del dispositivo virtuale.

Informazioni correlate:

Centro informazioni di WebSphere DataPower V6.0

Connessione alla console di monitoraggio

Utilizzare la console di monitoraggio per visualizzare le informazioni relative al monitoraggio.

Informazioni su questa attività

Accedere alla console di monitoraggio dalla finestra Istanze del sistema virtuale.

La funzione di monitoraggio è fornita da ITCAM for SOA. Scaricare la documentazione dal link correlato per ulteriori informazioni e ricercare le informazioni relative alle installazioni di DataPower.

Procedura

1. Fare clic su **Istanze** > **Sistemi virtuali** per visualizzare la finestra Istanze del sistema virtuale.
2. Dall'elenco delle istanze nella finestra Istanze del sistema virtuale, selezionare l'istanza distribuita. Vengono visualizzati i dettagli dell'istanza.
3. Espandere la sezione **Macchine virtuali** e selezionare la macchina virtuale che si desidera monitorare.
4. In **Informazioni generali**, individuare **Monitoraggio** e fare clic sul link **Fare clic per aprire**.

Informazioni correlate:

Documentazione di ITCAM for SOA 7.2.1 (da Fix Central)

Arresto e avvio dell'istanza distribuita

È possibile arrestare e avviare l'istanza distribuita dalla console del carico di lavoro. È anche possibile arrestare e avviare singole macchine virtuali nel pattern.

Per arrestare un'istanza distribuita in esecuzione:

1. Selezionare **Istanze** > **Sistemi virtuali** e quindi l'istanza dall'elenco **Istanze del sistema virtuale**.
2. Fare clic sull'icona **Arresta** nella barra del titolo dell'istanza.

Per avviare un'istanza distribuita arrestata:

1. Selezionare **Istanze** > **Sistemi virtuali** e quindi l'istanza dall'elenco **Istanze del sistema virtuale**.
2. Fare clic sull'icona **Avvia** nella barra del titolo dell'istanza.

Nota: Un difetto noto in DB2 10.1.0.2 fa sì che i processi DB2 non vengono sempre riavviati quando l'istanza viene arrestata e riavviata. In questo caso, è necessario avviare manualmente il processo DB2, accedendo al nodo DB2 come db2inst1 ed eseguendo **db2start**. Potrebbe anche essere necessario riavviare i processi WSRR sui nodi WSRR.

Per arrestare singole macchine virtuali.

1. Espandere la sezione **Macchine virtuali** della vista Istanza.
2. Selezionare il link **Gestisci** per la macchina che si desidera arrestare.
3. Fare clic sull'icona di arresto nella barra di gestione.

Per avviare singole macchine virtuali.

1. Espandere la sezione **Macchine virtuali** della vista Istanza.
2. Selezionare il link **Gestisci** per la macchina che si desidera arrestare.
3. Fare clic sull'icona di avvio nella barra di gestione.

È anche possibile arrestare e avviare WSRR e DB2 dalla riga comandi. Fare clic sul link **Login** per connettersi utilizzando la console SSH.

È possibile arrestare e avviare WSRR arrestando e avviando il profilo WebSphere Application Server. Consultare Gestione di profili mediante comandi nel centro informazioni di WebSphere Application Server.

Nel pattern Advanced, dopo il riavvio di DMGR e dei nodi personalizzati, il cluster WSRR deve essere avviato. Per effettuare ciò, aprire la console di gestione WebSphere Application Server e selezionare **Server** > **Cluster** > **WebSphere Application Server Cluster**. Selezionare **WSRRCluster_1**, quindi fare clic su **Avvia**.

È possibile arrestare e avviare DB2 mediante i comandi di sistema. Consultare System Commands nel centro informazioni di DB2.

Configurazione dei pattern dopo la distribuzione

Dopo la distribuzione dei pattern, è necessario configurare la sicurezza ed altre impostazioni.

Configurazione del PEP (Policy Enforcement Point)

L'istanza o il dispositivo DataPower rappresentano il PEP (Policy Enforcement Point) di IBM SOA Policy Gateway Pattern. Quando viene distribuito il dominio dell'applicazione, è possibile creare il contenuto di tale dominio.

Procedura

Durante l'impostazione delle configurazioni, verificare che siano utilizzati nomi di dominio differenti su ciascun dispositivo DataPower; in caso contrario, gli spazi di lavoro della topologia ITCAM for SOA non visualizzano i dati corretti.
Creare un WSP (Web Service Proxy):

1. Dal Pannello di controllo DataPower, fare clic su **WSP (Web Service Proxy)**.
2. Fare clic su **Aggiungi** ed immettere un nome per il proxy.

3. Aprire la scheda **Sottoscrizione WSRR**. Nell'elenco Server WSRR, fare clic su **WSRRSVR**.
4. Fornire le altre informazioni richieste, come, ad esempio, Gestore front side, lo spazio dei nomi, il nome dell'oggetto e così via, per creare la configurazione del WSP (Web Service Proxy).

Creare le politiche per il WSP:

5. Aprire la scheda **Politica** per l'Editor WSP.
6. Fare clic su **Regole di elaborazione** al livello appropriato. È possibile creare una nuova regola oppure modificare la regola predefinita fornita. L'azione della politica chiave da aggiungere è l'**Azione AAA**. Tale azione gestisce l'identificazione, l'autenticazione e l'autorizzazione che sono elementi fondamentali per il pattern.

   I fattori fondamentali che è necessario specificare per l'azione AAA includono l'input e l'output e la politica AAA. È possibile creare la politica durante la creazione dell'azione della politica AAA oppure, in precedenza, utilizzando l'editor AAA.

   - L'identificazione è la fase durante la quale l'utente viene identificato. Nell'esempio, sono utilizzati due tipi di identificazione. Nel firewall XML StoreAddLTPA, l'identificazione ha utilizzato l'autenticazione di base. Nel firewall StoreWSP, l'identificazione è stata fornita dal token LTPA.
   - L'autenticazione è la fase in cui l'utente viene riconosciuto dal sistema. Sono disponibili diverse opzioni. Nell'esempio, sono presenti due esempi; il primo in cui l'utente viene ricercato utilizzando LDAP ed il secondo in cui viene accettato un token LTPA valido.
   - L'autorizzazione è la fase in cui l'utente viene autorizzato per la risorsa, in questo caso le operazioni del servizio Web. Per utilizzare l'autorizzazione PDP XACML inclusa, è necessario specificare i seguenti elementi chiave:
     - Metodo: **Utilizza autorizzazione XACML**.
     - Versione XACML; ad esempio, 2.0.
     - Tipo PDP; ad esempio, PDP basato sulla negazione.
     - Utilizza PDP incluso: **Attivo**
     - Il nome del PDP, con XACML specificato.
     - Configurare il PDP. Per ulteriori informazioni, consultare “Modifica del PDP XACML PDP in DataPower” a pagina 71.
     - Il foglio di stile XSL personalizzato per eseguire il bind di AAA e XACML: utilizzare `apil-xacml-bindingnew.xsl` come punto di partenza.

Per configurare il gateway per l'utilizzo della revisione:

7. Modificare il file `.xml` XACML in modo da corrispondere alle particolari politiche di sicurezza che si desidera applicare per la revisione.
8. Creare un firewall XML con un'azione AAA che segue l'esempio di revisione.
9. Modificare il PDP utilizzato dall'azione AAA precedente in modo da puntare al foglio di stile utilizzato per applicare la revisione.
10. Copiare e modificare il foglio di stile `storeCallPDP.xsl`, che crea il payload SOAP per il servizio XACML. In particolare, verificare l'azione e la risorsa corrispondano ai requisiti per il documento della politica XACML creato.
11. Verificare che il foglio di stile modificato richiami la porta corretta per il nuovo firewall XML XACML.

Oggetti DataPower creati nei pattern Basic runtime e Advanced runtime

Una panoramica sugli oggetti DataPower creati nei pattern Basic runtime e Advanced runtime e delle relative funzioni.

Tabella 18. Oggetti del pattern DataPower

Oggetto	Descrizione
Dominio	Un dominio che può essere utilizzato per le applicazioni degli utenti.
Server WSRR	Denominato WSRRSVR. L'URL SOAP, il nome utente e la password vengono configurati assieme al profilo del proxy SSL con le credenziali di convalida.
Profilo del proxy SSL	Denominato WSRRPP, è un profilo di inoltro (client). Utilizza il profilo crittografato WSRRCP. Vengono utilizzate tutte le altre impostazioni predefinite.
Profilo crittografato	WSRRCP contiene un oggetto delle credenziali di convalida WSRRVC, che contiene il certificato del firmatario caricato come parte degli script pattern.
Credenziali di convalida	Le credenziali di convalida WSRR contengono il certificato crittografato WSRRCERT. Tutte le altre impostazioni sono predefinite.
Certificato crittografato	WSRRCERT utilizza il certificato del firmatario. Questo certificato è stato estratto dal NodeDefaultKeyStore, dal certificato predefinito di un singolo server, o da un certificato predefinito CMSKeyStore nel caso di un ambiente ND in cui è presente un IBM HTTP Server.

Esempio di utilizzo del server di definizione WSRR in un Proxy del servizio Web:

1. Dal pannello di controllo DataPower Pannello di controllo, fare clic su **Proxy del servizio Web**.
2. Fare clic su **Aggiungi** e fornire un **Nome** per il proxy.
3. Successivamente, selezionare la scheda **Sottoscrizione WSRR**
4. Selezionare server WSRR nel menu. L'oggetto WSRRSVR è disponibile.
5. Fornire le altre informazioni richieste come il gestore Front Side, lo spazio dei nomi, il nome dell'oggetto e così via, per creare la configurazione del proxy del servizio Web.

Valori DN del certificato per i certificati DataPower

Quando con i IBM SOA Policy Gateway Pattern forniti si utilizza SSL, la verifica dell'host DN è più rigida rispetto alla sicurezza del WebSphere Application Server predefinito. (Questo argomento si applica ai dispositivi DataPower esterni.)

La verifica dell'host DN in WebSphere Application Server per impostazione predefinita non è abilitata. Tuttavia, nei package di script utilizzati dai IBM SOA Policy Gateway Pattern, la verifica dell'host DN è attiva e non può essere disattivata. Un certificato specifico valido tra il WebSphere Application Server predefinito e DataPower potrebbe non funzionare per il package di script “SOA Policy Gateway 2.5.0.0 – Security” o per quello “SOA Policy Gateway 2.5.0.0 - Sample” utilizzato con IBM SOA Policy Gateway Pattern. Ad esempio, un DN `myserver.yourcompany.com` potrebbe essere accettato dalle impostazioni predefinite di WebSphere Application Server, ma non dai package di script. Per aggiungere o

rimuovere i certificati DataPower utilizzati con la distribuzione, consultare “Rimozione o aggiunta di certificati DataPower al truststore WSRR”.

Rimozione o aggiunta di certificati DataPower al truststore WSRR

Questa attività descrive come aggiungere o rimuovere i certificati DataPower. Questo argomento è valido per i pattern distribuiti con dispositivi DataPower esterni.

Informazioni su questa attività

I certificati DataPower vengono caricati sul truststore WSRR per rendere più semplice l'aggiornamento della sincronizzazione tra WSRR e DataPower per gli aggiornamenti della politica. Se questa capability non è necessaria, è possibile rimuovere i certificati DataPower. È anche possibile aggiungere nuovi certificati DataPower se è necessario modificare i certificati.

Procedura

1. Per rimuovere i certificati:
   a. Accedere alla console di gestione di WebSphere Application Server all'indirizzo `https://hostname:9043/ibm/console`, dove *hostname* è il nome host del sistema WSRR. Immettere il nome utente di gestione e la password.
   b. Passare a **Sicurezza, Gestione chiavi e certificati SSL**.
   c. Fare clic su **Keystore e certificati**.
   d. Fare clic su **NodeDefaultTrustStore** se la propria distribuzione è basata su un pattern di runtime di base oppure su **CellDefaultTruststore** se è stato distribuito un pattern di runtime avanzato.
   e. Fare clic su **Certificati firmatario**.
   f. Selezionare le caselle di spunta relative ai certificati che si desidera rimuovere.
   g. Fare clic su **Elimina**.
   h. Fare clic su **Salva**.
2. Per aggiungere nuovi certificati DataPower, fare clic su **Aggiungi** per aggiungere il nuovo certificato.
   a. Accedere alla console di gestione di WebSphere Application Server all'indirizzo `https://hostname:9043/ibm/console`, dove *hostname* è il nome host del sistema WSRR. Immettere il nome utente di gestione e la password.
   b. Passare a **Sicurezza, Gestione chiavi e certificati SSL**.
   c. Fare clic su **Keystore e certificati**.
   d. Fare clic su **NodeDefaultTrustStore** se la propria distribuzione è basata su un pattern di runtime di base oppure su **CellDefaultTruststore** se è stato distribuito un pattern di runtime avanzato.
   e. Fare clic su **Certificati firmatario**.
   f. Fare clic su **Aggiungi** e specificare i nuovi certificati.
   g. Fare clic su **Salva**.

Modifica delle chiavi LTPA

Questa procedura descrive come modificare la chiave LTPA. La chiave LTPA è condivisa tra tutte le celle nei pattern. Non viene utilizzata nel pattern SOA Policy

Gateway Basic Runtime Sample. La chiave LTPA viene esportata da Governance Master ed importata negli ambienti di runtime, come l'ambiente di staging o di produzione.

Informazioni su questa attività

Effettuare le azioni riportate di seguito nella console di gestione di WebSphere Application Server. Per ulteriori informazioni, seguire il link correlato.

Procedura

1. Esportare la nuova chiave LTPA dalla macchina virtuale Dmgr WSRR Governance Master.
2. Importare la chiave LTPA nelle istanze WSRR di runtime, che sono Dmgr o Stand Alone.
3. Se l'istanza di runtime è basata su un pattern di runtime avanzato, effettuare le seguenti operazioni in ordine:
   a. Sincronizzare tutti i nodi.
   b. Arrestare il cluster WSRR.
   c. Arrestare gli agent del nodo.
   d. Arrestare Dmgr.
4. Se il sistema WSRR è basato su un pattern di runtime avanzato, è necessario riavviarlo in ordine inverso:
   a. Avviare Dmgr.
   b. Avviare gli agent del nodo.
   c. Avviare il cluster WSRR.
5. Se WSRR è un server Standalone (basato su un pattern di runtime di base), è necessario arrestarlo e riavviarlo affinché la modifica alla chiave LTPA diventi effettiva.

Informazioni correlate:

Centro informazioni di WebSphere Application Server V8.0

Creazione e governance del servizio

Utilizzare l'interfaccia utente WSRR Business Space per creare e governare i servizi di business e i relativi oggetti associati.

Lo spazio SOA Governance deve essere creato in Business Space prima che sia possibile creare le politiche. Se lo spazio SOA Governance non esiste, consultare “Configurazione di Business Space per il primo utilizzo” a pagina 83 e seguire i passi per creare lo spazio.

Per ulteriori informazioni sulla creazione di un nuovo servizio governato, consultare Centro informazioni di IBM WebSphere Service Registry and Repository Versione 8.0 - Tutorial: Governing a new service.

Per ulteriori informazioni sul governo di un servizio esistente, consultare Centro informazioni di IBM WebSphere Service Registry and Repository Versione 8.0 - Tutorial: Governing an existing service.

Attività correlate:

“Connessione a WSRR - Business Space” a pagina 82
Utilizzare l'interfaccia utente Business Space per utilizzare WSRR.

Politiche

Dettagli di implementazione per l'utilizzo di WSRR come PAP (Policy Authoring Point) e di WebSphere DataPower come PEP (Policy Enforcement Point) quando si creano le politiche di mediazione.

Politiche in WSRR

È possibile utilizzare WSRR per creare tutte le politiche SOA, incluso le politiche SLA (Service Level Agreement), le politiche di mediazione, le politiche di monitoraggio e le politiche personalizzate. Con l'utilizzo dell'interfaccia utente di Business Space, è possibile creare, aggiornare o eliminare un documento della politica in WSRR. Il documento della politica può contenere un'espressione che specifica un numero di politiche per un particolare dominio della politica. In alternativa, è possibile creare un documento della politica che assembla le politiche esistenti di altri documenti. Le politiche individuali vengono indicate utilizzando gli identificativi della politica, che vengono specificati quando si aggiungono politiche al proprio documento. Un'espressione della politica rappresenta la dichiarazione di una politica ed è equivalente a un elemento `<wsp:Policy>` in un documento WS-Policy.

Per creare una politica di mediazione in Business Space, consultare “Authoring di nuove politiche di mediazione” a pagina 97.

Asserzioni della politica di mediazione

Gli SLA (Service Level Agreement) hanno origine da un requisito di business che indica che la qualità fornita da un servizio soddisfa uno specifico standard. Durante la progettazione di un servizio, i requisiti funzionali vengono creati per guidare la logica di esecuzione del servizio. I requisiti non funzionali vengono specificati in parallelo come parte dell'analisi e della progettazione di tale servizio per definire la qualità che si prevede che il servizio fornisca. Ad esempio, l'azienda potrebbe avere un servizio che fornisce informazioni in risposta a una query internet del cliente. L'obiettivo è di restituire la risposta entro 3 secondi. Come parte del processo di progettazione della transazione end-to-end, è stato stabilito che questo servizio deve restituire le relative informazioni entro 2 secondi per soddisfare i requisiti non funzionali di business.

È possibile scrivere una politica che implementa le verifiche di runtime sulle prestazioni del servizio e che agisce quando i requisiti vengono soddisfatti per garantire che il servizio corrisponda ai requisiti SLA. Ad esempio, si potrebbe avere un endpoint primario del servizio che è normalmente (95% delle volte) in grado di fornire la risposta del servizio entro due secondi. L'architettura SOA crea un endpoint secondario su un altro server che può essere utilizzato come modello hot standby per interruzioni dell'endpoint primario, ma se ne consente l'utilizzo per il traffico in eccedenza quando l'endpoint primario non è in grado di tenere il passo con il caricamento della transazione. È possibile scrivere una politica che controlla il tempo di risposta del servizio e reindirizza il traffico quando necessario per soddisfare gli SLA.

Un altro esempio in cui gli SLA vengono conservati attraverso la politica di runtime è quello in cui un servizio risponde alle transazioni che hanno diversi consumer, ognuno con un diverso livello di priorità. Un esempio semplice potrebbe avere clienti “gold” e “bronze”, laddove il business garantisce solo una specifica qualità del servizio per clienti “gold”. In questo esempio, è possibile controllare se il consumer è “gold” ed eseguire il reinstradamento verso l'endpoint secondario,

lasciando che il cliente “bronze” gestisca un tempo di risposta più lento. La decisione assunta dal business deriva da incrementi insufficienti dei ricavi da parte di clienti “bronze”, e giustifica i costi di progettazione necessari per ottenere un tempo di risposta che soddisfi l'accordo SLA dei clienti “gold”.

In un terzo esempio, si potrebbe verificare una situazione in cui un servizio si comporta nel migliore modo possibile, ma quando rileva di essere sotto carico, accoda o addirittura rifiuta i messaggi dai servizi consumer con bassa priorità. Un esempio si verifica quando la routine del batch invia al sistema richieste del consumer in tempi non previsti. Per tutelare la qualità del servizio, è possibile creare una politica di runtime attiva solo durante le ore lavorative e che rifiuti tutte le richieste in batch durante questo periodo.

A livello generale, la politica di mediazione consente la convalida e la trasformazione del messaggio in entrata dal client (consumer) prima della presentazione al server (provider).

Le politiche supportano questo tipo di convalida e trasformazione del messaggio. Le politiche possono essere specificate solo per un servizio del provider, per una coppia consumer-provider specifica o per consumer anonimi per un servizio del provider. Le politiche per i clienti anonimi forniscono una modalità di definizione di una politica predefinita che si applica solo ai consumer per cui non vengono applicate altre politiche. L'utilizzo di questa funzione consente di specificare le politiche per consumer anomali che non si identificano. I servizi consumer di questo tipo possono quindi avere le relative transazioni rifiutate. Ciò può essere utile per impedire attacchi DoS (denial of service) dagli hacker consumer che tentano di bloccare il sistema con transazioni che servono a interrompere i servizi del provider.

Condizioni della politica di mediazione

Le asserzioni della mediazione possono essere effettuate in modo da consentire alla politica runtime di controllare lo SLA del servizio, la trasformazione dei messaggi da consumer a provider, o per convalidare lo schema di messaggio del messaggio consumer.

Le condizioni della politica SLA, un tipo particolare di politica di mediazione, consente un costrutto if-then-else classico con una condizione ed un'insieme di azioni da eseguire a seconda di come viene valutata la condizione. La specifica di una condizione è facoltativa. Se non viene specificata alcuna condizione, la condizione logica è equivalente a quella che si assume con il valore True, e tutte le azioni specificate vengono applicate di conseguenza.

La condizione, se specificata, deve essere costituita da un'espressione booleana o da una specifica di pianificazione, oppure includere entrambe.

Pianificazione

La pianificazione, se specificata, identifica quando la politica è valida. La data e l'ora sono valutate dal PEP (Policy Enforcement Point) locale, mentre il fuso orario utilizzato è quello del PEP (Policy Enforcement Point). Se non viene specificata alcuna pianificazione, la politica inizia non appena viene scaricata dal PAP (Policy Authoring Point) al PEP (Policy Enforcement Point) e continua indefinitamente.

La pianificazione definisce una data di inizio e una data di fine facoltative, un intervallo di tempo giornaliero facoltativo e un elenco di giorni della settimana

facoltativi. Ad esempio, una pianificazione può essere definita come valida dal 1° ottobre 2012 al 30 ottobre 2012, dalle ore 8 alle ore 17 tutti i mercoledì e le domeniche.

I parametri per la pianificazione che possono essere specificati sono riportati di seguito:

- **StartDate** - Questo attributo facoltativo specifica in formato xs:date la data in cui la pianificazione diventa valida. StartDate è inclusivo e se questo attributo non è presente, la pianificazione diventa valida in modo immediato oggi. Fare clic sul collegamento ipertestuale xs:time per comprendere questo standard del settore.
- **StopDate** - Questo attributo facoltativo specifica in formato xs:date la data in cui la pianificazione termina di essere valida. StopDate è esclusivo e la data specificata deve essere successiva alla data di inizio. Quando la data di fine è precedente o uguale alla data di inizio, la pianificazione non è mai valida. Se questo attributo non è presente, la pianificazione è valida indefinitamente.
- **Daily** - Questo elemento facoltativo specifica l'intervallo di tempo giornaliero durante il quale la pianificazione è valida. Se questo elemento non è presente, la pianificazione è valida tutto il giorno.
  - **StartTime** – Se Daily è specificato, questo attributo è obbligatorio. Specifica in formato xs:time l'ora in cui ha inizio la pianificazione durante il giorno. Fare clic sul collegamento ipertestuale xs:time per comprendere questo standard del settore.
  - **StopTime** – Se Daily è specificato, questo attributo è obbligatorio. Specifica in formato xs:time l'ora in cui ha fine la pianificazione durante il giorno. StopTime è esclusivo e se l'ora specificata è precedente o uguale all'ora di inizio giornaliero, la pianificazione si arresta nell'ora di fine specificata del giorno successivo.
- **Weekdays** - Questo elemento facoltativo specifica i giorni della settimana inclusi nella pianificazione. Se questo elemento non è presente, nella pianificazione saranno inclusi tutti i giorni della settimana. Questo elemento influisce solo sull'inizio dell'intervallo di tempo giornaliero, poiché le esecuzioni delle pianificazioni sono consentite dopo la mezzanotte. Ad esempio, se una pianificazione è impostata per iniziare alle ore 23, e viene eseguita per 2 ore ogni mercoledì, la pianificazione termina effettivamente il giovedì alle ore 01:00.
  - **Days** – Se Weekdays è specificato, questo attributo è obbligatorio. Elenca i giorni della settimana inclusi nella pianificazione, come un elenco di nomi separati con il segno più ('+'); ad esempio, “Monday+Tuesday+Wednesday+Thursday+Friday+Saturday+Sunday”.

Espressione della condizione della politica di mediazione

L'espressione della condizione, se specificata, è un elemento non ripetuto che specifica un'espressione Booleana.

L'espressione contiene tre parametri: Attributo, Operatore e Valore, piu i parametri facoltativi Intervallo e Limite. Se l'applicazione dell'Operatore su Attributo e Valore, oltre a Intervallo e Limite quando necessari, assume il valore True, anche l'espressione assume il valore True. L'elemento Limite viene utilizzato solo con gli operatori HighLow e TokenBucket. Se non specificato, il valore di Limite è 0. Se l'intervallo non è specificato, il valore predefinito è 60 secondi.

I parametri per l'espressione che possono essere specificati sono riportati di seguito:

- **Attribute** - La seguente tabella riepiloga gli attributi definiti e il relativo tipo.

Tabella 19. Attributi definiti

Attributo	**Descrizione e tipo**
ErrorCount	Il numero di errori osservati durante questo intervallo di monitoraggio.
MessageCount	Il numero di messaggi effettivi intercettati durante l'intervallo di monitoraggio.
InternalLatency	La latenza interna (tempo di elaborazione) in secondi.
BackendLatency	La latenza dispositivo-a-server in secondi.
TotalLatency	La somma della latenza backend ed interna in secondi.

- **Operator** - La seguente tabella riepiloga gli operatori disponibili e il loro significato:

Tabella 20. Operatori

Operatore	**Significato**
GreaterThan	Un algoritmo numerico semplice che assume il valore True quando Attributo è maggiore del valore definito.
LessThan	Un algoritmo numerico semplice che assume il valore True quando Attributo è minore del valore definito.
TokenBucket	Un algoritmo basato sulla frequenza che consente la suddivisione. L'algoritmo consiste di un bucket con una capacità massima di token Limite. Il bucket viene riempito ad una frequenza costante di token Valore per Intervallo, mentre per ciascuna unità di Attributo viene rimosso un token. Questo algoritmo assume il valore True quando non ci sono token nel bucket e il valore False in caso contrario. Di seguito è riportato un esempio che descrive l'algoritmo: Limit=100, Value=5, Interval=1 secondo e Attribute=MessageCount. 1. Il bucket viene avviato pieno con una capacità massima di 100 token 2. Quando si riceve un messaggio, l'algoritmo controlla se il bucket contiene eventuali token: a. In tal caso, l'algoritmo assume il valore False e un token è rimosso dal bucket b. In caso contrario, l'algoritmo assume il valore True. 3. Durante tutto il periodo, ogni secondo, l'algoritmo restituisce 5 token al bucket in base allo spazio.
HighLow	Un algoritmo che assume il valore True quando Attributo raggiunge la soglia superiore specificata come Valore e quindi continua ad assumere il valore True fino a quando Attributo non raggiunge la soglia inferiore specificata come Limite.

- **Value** – Si tratta di un elemento intero positivo. “0” è valido.
- **Interval** - Questo elemento facoltativo definisce in formato xs:duration l'intervallo di tempo, utilizzato come finestra scorrevole, per misurare wsme:Attribute durante la valutazione dell'espressione. Se non specificato, l'intervallo utilizzato è di 60 secondi. Se specificato, è necessario indicare un valore ragionevole, considerando le capability configurate del PEP (Policy Enforcement Point). Ossia, più alto è il valore in questione, maggiore è la memoria richiesta dal PEP (Policy Enforcement Point) per tenere traccia

dell'attributo. Fare clic sul collegamento ipertestuale xs:duration per comprendere questo standard del settore.

- **Limit** - Questo elemento intero facoltativo definisce l'argomento Limite aggiuntivo richiesto quando wsme:Operator è TokenBucket o HighLow. L'unità dipende dal wsme:Operator specificato.

  Se wsme:Operator è HighLow, definisce la soglia inferiore mentre wsme:Value definisce la soglia superiore. La soglia specificata deve essere inferiore a quella di wsme:Value. Se non specificato il limite predefinito è 0.

  Se wsme:Operator è TokenBucket, definisce la dimensione massima della suddivisione, o il numero massimo di token nel bucket, mentre Valore specifica la frequenza con cui il bucket viene riempito, in numero di token per Intervallo. Se non specificato il limite predefinito è 0 e TokenBucket è equivalente a un'operazione GreaterThan.

Azioni della politica di mediazione

L'elemento Azione di mediazione specifica le azioni da intraprendere. Nonostante la sintassi consenta molte combinazioni, non tutte hanno un senso e quando vengono specificate le azioni in conflitto, come la richiesta che un messaggio sia accodato e rifiutato, il comportamento viene rifiutato dal PAP (Policy Authoring Point). Le azioni della politica di mediazione consentite sono:

- **QueueMessage** – Questa azione specifica che le transazioni sono accodate quando viene soddisfatta la condizione logica. L'elaborazione dei messaggi non riprende fino a quando la condizione logica non è più soddisfatta. La metodologia di accodamento e qualsiasi timeout associato sono definiti dal PEP (Policy Enforcement Point), in questo caso WebSphere DataPower. Quando sono specificate diverse azioni all'interno di un singolo elemento Azione, QueueMessage deve essere la prima azione.
- **RejectMessage** – Questa azione specifica che le transazioni sono rifiutate quando la condizione logica è soddisfatta. Le transazioni continuano ad essere rifiutate fino a quando la condizione logica non è più soddisfatta. Quando le transazioni vengono rifiutate, un errore SOAP viene restituito al servizio client (consumer). Quando sono specificate diverse azioni all'interno di un singolo elemento Azione, RejectMessage deve essere la prima azione. QueueMessage e RejectMessage si escludono reciprocamente.
- **Notify** - Questo elemento facoltativo specifica che una notifica viene generata quando la condizione logica è soddisfatta. Per DataPower, un messaggio viene scritto nel log di sistema DataPower.
- **RouteMessage** - Questo elemento facoltativo specifica che i messaggi vengono instradati verso la destinazione di endpoint specificata quando la condizione logica è soddisfatta. I messaggi continuano ad essere instradati all'endpoint specificato fino a quando la condizione logica non è più soddisfatta.
  - **EndPoint** – Questo parametro è obbligatorio quando viene specificata un'azione RouteMessage. Il valore di endpoint supportato può essere un indirizzo IP, un nome host o un host virtuale; ad esempio un gruppo bilanciatore di carico.
- **ValidateMessage** - Questo elemento facoltativo specifica che i messaggi vengono convalidati rispetto alle grammatiche specificate. I messaggi vengono rifiutati quando la convalida ha esito negativo. XSD o WSDL deve essere specificato come parametro secondario se ValidateMessage è specificato. SCOPE è facoltativo e se non specificato, SOAPBody viene utilizzato per la convalida.
  - **XSD** - Specifica che i messaggi vengono convalidati rispetto allo schema XML identificato dall'URI che contiene.

– **WSDL** - Specifica che i messaggi vengono convalidati rispetto alla descrizione dei servizi Web (WSDL) identificata dall'URI che contiene.
– **SCOPE** – Specifica la parte del messaggio che viene convalidata. La seguente tabella elenca i possibili valori e il loro significato:

Tabella 21. Elementi ValidateMessage

Valore	Descrizione
SOAPBody	Il contenuto dell'elemento SOAP Body, senza particolare elaborazione per errori SOAP. (Impostazione predefinita)
SOAPBodyOrDetails	Il contenuto dell'elemento dettagli per errori SOAP, altrimenti il contenuto di Body.
SOAPEnvelope	L'intero messaggio SOAP, compresa la busta.
SOAPIgnoreFaults	Nessuna convalida se il messaggio è un errore SOAP, altrimenti il contenuto dell'elemento SOAP Body.

- **ExecuteXSL** - Specifica l'esecuzione di una trasformazione XSL con il foglio di stile e i parametri specificati. Le transazioni vengono rifiutate quando l'esecuzione ha esito negativo. Le informazioni sul foglio di stile devono essere specificate, mentre i parametri sono facoltativi e devono essere specificati come richiesto dal particolare foglio di stile specificato.
  – **Stylesheet** - Specifica che l'operazione di trasformazione utilizza il foglio di stile specificato dall'URI contenuto. Il foglio di stile DEVE essere un file XSLT.
  – **Parameter** - Questo elemento facoltativo ripetitivo specifica un parametro del foglio di stile da utilizzare per l'operazione ExecuteXSL.
    - **Name** – Questo attributo è obbligatorio per ciascun parametro Parameter corrispondente e specifica il nome del parametro.
    - **Value** - Questo attributo è obbligatorio per ciascun parametro Name corrispondente e specifica il valore del parametro.

Authoring di nuove politiche di mediazione

È possibile creare nuove politiche di mediazione utilizzando l'interfaccia utente Business Space. Quando vengono create le politiche di mediazione, vengono specificate le condizioni e le azioni per la politica.

Prima di iniziare

Per informazioni relative all'accesso a Business Space, consultare “Connessione a WSRR - Business Space” a pagina 82.

È necessario creare lo spazio SOA Governance prima che sia possibile creare le politiche. Se lo spazio SOA Governance non esiste, consultare “Configurazione di Business Space per il primo utilizzo” a pagina 83 e seguire i passi per la creazione dello spazio.

È necessario configurare Business Space per creare le politiche di mediazione WS-MediationPolicy 1.7 dal widget Azioni. Consultare Service Registry Actions widget

Informazioni su questa attività

Creare le nuove politiche utilizzando lo spazio SOA Governance.

Procedura

1. Aprire lo spazio SOA Governance:
   a. Fare clic su **Vai a spazi**. Viene visualizzata la finestra di dialogo Vai a spazi.
   b. Fare clic sullo spazio per gli utenti SOA Governance. Il nome specifico dipende dalle informazioni specificate durante la creazione dello spazio.
2. Nella scheda Panoramica, fare clic su **Crea una politica di mediazione**.
3. Immettere un nome significativo ed una descrizione facoltativa.
4. Aggiungere le condizioni e le azioni come richiesto. Per ulteriori informazioni relative alle condizioni ed alle azioni, consultare “Politiche” a pagina 92 e Centro informazioni di IBM WebSphere Service Registry and Repository Versione 8.0 - Creating a mediation policy.
5. Fare clic su **Fine**.

Risultati

La politica viene creata e memorizzata in WSRR. Per visualizzare il documento della politica per la politica creata, selezionare il documento della politica nel widget Navigator del registro del servizio. In alternativa, ricercare il nome specificato, includendo `.xml` alla fine. Il documento della politica è visualizzato nel widget Dettagli del registro del servizio a destra.

Concetti correlati:

“Politiche” a pagina 92
Dettagli di implementazione per l'utilizzo di WSRR come PAP (Policy Authoring Point) e di WebSphere DataPower come PEP (Policy Enforcement Point) quando si creano le politiche di mediazione.

Informazioni correlate:

Centro informazioni di IBM WebSphere Service Registry and Repository Versione 8.0 - Creazione di una politica di mediazione

Authoring di nuove politiche di monitoraggio

È possibile creare nuove politiche di monitoraggio utilizzando l'interfaccia utente Web WSRR. Quando vengono create le politiche di monitoraggio, vengono specificate le condizioni e le azioni per le politiche.

Prima di iniziare

Per informazioni relative all'accesso all'interfaccia utente Web WSRR, consultare “Connessione a WSRR - UI Web di WSRR” a pagina 84.

Procedura

1. Aprire l'interfaccia utente Web WSRR.
2. Fare clic su **Visualizza** > **Documenti del servizio** > **Documenti della politica** e nella vista di raccolta fare clic su **Nuovo**.
3. Dall'elenco dei framework della politica disponibili, selezionare **Monitoraggio**. Fare clic su **Avanti**. Viene creato un documento della politica contenente un'espressione della politica root.
4. Immettere un nome significativo ed una descrizione facoltativa.
5. Fare clic sulla scheda Politica, fare clic su **Modifica documento della politica** ed aggiungere le condizioni e le azioni come richiesto. Per ulteriori informazioni relative alle condizioni ed alle azioni, seguire i link correlati.
6. Fare clic su **Pubblica**.

Risultati

La politica viene creata e memorizzata in WSRR. È possibile visualizzare il documento della politica per la politica in Business Space; selezionare il documento della politica nel widget Navigatore del registro del servizio. In alternativa, ricercare il nome specificato, includendo `.xml` alla fine. Il documento della politica è visualizzato nel widget Dettagli del registro del servizio a destra.

Concetti correlati:

"Politiche" a pagina 92
Dettagli di implementazione per l'utilizzo di WSRR come PAP (Policy Authoring Point) e di WebSphere DataPower come PEP (Policy Enforcement Point) quando si creano le politiche di mediazione.

Informazioni correlate:

Attività di authoring della politica

Utilizzo dello strumento di authoring delle politiche

Gestione delle politiche

È possibile modificare o rimuovere le politiche utilizzando l'interfaccia utente Business Space.

Prima di iniziare

Configurare lo spazio SOA Governance. Per ulteriori informazioni, consultare "Configurazione di Business Space per il primo utilizzo" a pagina 83.

Procedura

1. Per aprire il documento della politica per la politica, selezionarlo nel widget Navigator del registro del servizio nell'angolo in basso a sinistra. In alternativa, ricercare il nome specificato, includendo `.xml` alla fine. Il documento della politica è visualizzato nel widget Dettagli del registro del servizio a destra.
2. Per modificare i dettagli della politica:
   a. Fare clic sull'icona Modifica in questo widget per modificare il documento della politica. Viene visualizzata una finestra con le opzioni per la modifica dei dettagli della politica.
   b. Se la politica dispone di condizioni o azioni, tali elementi vengono visualizzati. Creare e modificare le condizioni e le azioni come richiesto.
   c. Fare clic su **Fine** per salvare e chiudere l'editor delle politiche. Il widget Dettagli del registro del servizio viene aggiornato in modo da mostrare le modifiche apportate.
3. Per eliminare la politica:
   a. Trasferire la politica ad uno stato governance che consente la modifica o l'eliminazione del documento della politica. Per ulteriori informazioni sulla transizione di una politica attraverso il ciclo di vita della politica SOA, consultare "Gestione del ciclo di vita della politica" a pagina 100.
   b. Fare clic su **Azione** > **Elimina**. L'opzione Elimina viene visualizzata nel menu.
   c. Selezionare **Elimina** per eliminare la politica.
   d. Fare clic su **Sì** per confermare l'eliminazione.

Informazioni correlate:

Centro informazioni di IBM WebSphere Service Registry and Repository Versione 8.0

Centro informazioni di IBM WebSphere Service Registry and Repository Versione 8.0 - Policies in the governance enablement profile

Gestione del ciclo di vita della politica

Le politiche possono essere trasferite da uno stato di governance all'altro utilizzando l'interfaccia utente Business Space. Per essere applicate da DataPower, le politiche devono trovarsi nello stato Approvato.

Informazioni su questa attività

Per ulteriori informazioni relative alla governance, consultare “Ciclo di vita della politica SOA” a pagina 5.

Procedura

Per trasferire una politica ad uno stato del ciclo di vita differente, effettuare le operazioni riportate di seguito. Ripetere questi passi tutte le volte necessarie per raggiungere lo stato del ciclo di vita desiderato.

1. In Business Space, aprire il documento della politica per la politica selezionandolo nel widget Navigator del registro del servizio. In alternativa, ricercare il nome specificato, includendo `.xml` alla fine. Il documento della politica viene viene visualizzato nel widget Dettagli del registro del servizio. La proprietà **Stato governance** visualizza lo stato governance corrente per il profilo.
2. Fare clic su **Azione**. Viene visualizzato un elenco delle transizioni del ciclo di vita possibili insieme ad altre operazioni possibili.
3. Selezionare la transizione del ciclo di vita richiesta per trasferire la politica allo stato richiesto. La proprietà **Stato governance** della politica viene aggiornata in modo da mostrare il nuovo stato del ciclo di vita.

Concetti correlati:

“Ciclo di vita della politica SOA” a pagina 5
Le politiche sono governate dal ciclo di vita della politica SOA. Il ciclo di vita consiste in una identificazione iniziale della politica, in una sua successiva distribuzione in produzione e, infine, quando non più utilizzata, in un suo abbandono.

Informazioni correlate:

Centro informazioni di IBM WebSphere Service Registry and Repository Versione 8.0 - SOA policy lifecycle

Politiche allegate ad un servizio

Le politiche possono essere allegate ad un servizio utilizzando WSRR.

Per ulteriori informazioni, consultare Centro informazioni di IBM WebSphere Service Registry and Repository Versione 8.0 - Policy attachment tasks.

Capitolo 7. Risoluzione dei problemi

Richiedere assistenza con la diagnosi di problemi che si potrebbero avere prima, durante e dopo la distribuzione del pattern.

Utilizzare i link per trovare gli argomenti relativi a un problema con i pattern.

Risoluzione dei problemi con la distribuzione

È possibile risolvere i problemi comuni che si incontrano quando si distribuiscono i pattern in IBM SOA Policy Gateway Pattern.

Errore di connessione al dispositivo DataPower esterno durante la distribuzione

Provare le seguenti soluzioni:

- Verificare con l'amministratore DataPower che l'utente e la password siano validi:
  - In DataPower, la GUI Web convalida che l'utente esiste passando al **Pannello di controllo** > **Gestisci account utente**.
  - Verificare che l'account esista.
  - Verificare che l'utente sia autorizzato ad utilizzare l'interfaccia di gestione XML; ad esempio, l'amministratore di sistema.
  - L'amministratore DataPower deve controllare se l'account utente è abilitato nelle impostazioni dell'agent utente; ad esempio le impostazioni di autenticazione di base.
- Verificare che il nome host DataPower sia corretto
- Verificare che l'interfaccia di gestione XML DataPower sia abilitata.

Risoluzione di un errore per il dominio già presente

Provare la seguente soluzione:

- Nel pannello di controllo DataPower, aprire i domini di applicazioni. Controllare se il dominio esiste già.

Risoluzione di un errore di sovrapposizione della porta per l'applicazione di esempio

Se uno dei servizi di esempio non è disponibile, verificare se le porte nel proprio dominio sono in conflitto con altri domini.

Provare le seguenti soluzioni:

- Accedere a DataPower e passare al dominio di esempio. Quindi, aprire il pannello di controllo e fare clic sull'icona Firewall XML. Accertarsi che i firewall XML siano tutti nello stato Attivo.
- Ricercare il gestore frontside HTTP. Controllare che il singolo gestore frontside HTTP sia nello stato Attivo.

Risoluzione dell'errore di promozione

Molti problemi potrebbero sorgere durante la promozione, incluso l'errore di connessione a Governance Master durante la distribuzione.

Provare le seguenti soluzioni:

- Controllare i parametri:
  - Controllare l'utente di WSRRCELL Governance Master.
  - Controllare la password per l'utente della cella WSRR Governance Master.
  - Controllare il nome host della cella WSRR Governance Master.
  - Controllare il nome CELL della cella WSRR Governance Master.
- Controllare lo scambio di certificati del firmatario:
  - Passare all'archivio trust predefinito della cella Governance Master e accertarsi che vi sia una voce di certificato per il server Dmgr o Standalone dell'ambiente runtime.
  - Passare a ciascun ambiente runtime e controllare l'archivio CellDefaultTrust (per l'ambiente ND) o NodeDefaultTrustStore (per i server WSRR Standalone) per essere certi che vi sia un certificato per il Dmgr di Governance Master.
  - Esportare le chiavi LTPA da entrambe le celle utilizzando la stessa password ed accertarsi che esse siano uguali (ad esempio, in numero di byte).
- Accertarsi che il file delle proprietà della promozione contenga le sezioni server con la porta e l'host appropriati e le informazioni sull'utente e sulla password. Queste informazioni possono essere trovate nella console ServiceRegistry per il Governance Master:
  - Passare a GovernanceMasterDMgrHost o ServiceRegistry e attivare la prospettiva Configurazioni. Nella sezione Azioni, individuare **Promotion** e aprire il file delle proprietà della promozione. Per ogni ambiente, vi devono essere elementi XML per ciascun server nel cluster o nodo WSRR di staging. Se esiste un nodo o cluster di produzione, vi devono essere delle voci server:port per entrambi, oltre a informazioni sull'utente e sulla password.
- Controllare che la versione del servizio e l'endpoint SOAP abbiano entrambi la classificazione per le funzioni di staging e di produzione.
  - Nella console del registro del servizio, selezionare la prospettiva SOA Governance. Aprire la versione del servizio e selezionare la scheda Classificazioni. Le funzioni di staging e di produzione devono essere abilitate.

Risoluzione degli errori CLI personalizzati

Provare le seguenti soluzioni:

- Controllare il file defaultLog per messaggi di errore nel dominio DataPower.
- Abilitare il programma di debug CLI e controllare tali log prima di eventuali esecuzioni aggiuntive della CLI.

Risoluzione di problemi nell'istanza distribuita

È possibile risolvere i problemi comuni nell'istanza distribuita.

Connessioni non riuscite al server LDAP o alla porta DataPower StoreWSP

Si potrebbe verificare un problema con le impostazioni del dominio se i log DataPower mostrano un errore di connessione al gateway LDAP o StoreWSP e se

si sta utilizzando il nome alias dell'host; ad esempio, `xyz` anziché il nome host completo `xyz.company.com` per uno dei seguenti parametri nel package di script:

- Il nome host DataPower
- Il nome host LDAP

Provare la seguente soluzione:

1. Nella console di gestione DataPower, passare al dominio predefinito.
2. Ricercare `Configura impostazioni DNS`.
3. Fare clic sulla scheda Ricerca domini.
4. Assicurarsi che il dominio, ad esempio `company.com`, sia nell'elenco. Se non è presente nell'elenco fare clic su `Aggiungi` e aggiungerlo all'elenco.

Problemi con il monitoraggio

Se il monitoraggio non è disponibile nei nodi distribuiti, è necessario accertarsi che i servizi condivisi richiesti siano in esecuzione. Passare a **Istanze** > **Servizi condivisi**

Accertarsi che il monitoraggio di sistema e il monitoraggio di sistema per WebSphere DataPower siano in esecuzione nello stesso gruppo cloud delle istanze distribuite. Per il monitoraggio WSRR, accertarsi inoltre che il monitoraggio di sistema per WebSphere Application Server sia in esecuzione nel proprio gruppo cloud.

Raccolta delle informazioni di diagnostica

È possibile utilizzare i log per individuare e risolvere i problemi. I log sono archiviati sul dispositivo e possono essere visualizzati dall'interfaccia utente oppure scaricati sul file system locale.

Procedura

Per raccogliere le informazioni di diagnostica, effettuare le operazioni riportate di seguito:

1. Visualizzare le istanze virtuali:
   a. Fare clic su **Istanze** > **Sistema virtuale**.
   b. Selezionare l'istanza nell'elenco delle istanze nella finestra Istanze del sistema virtuale.
2. Per la macchina virtuale WSRR:
   a. Nella sezione **Macchine virtuali**, espandere la macchina virtuale WSRR e ricercare gli errori nella sezione **Package di script**. Se uno dei package di script contiene errori, fare clic sui link del log per **remote_std_out.log** e **remote_std_err.log** accanto ai nomi dei package di script.
   b. Accedere all'istanza WSRR e verificare gli errori del server.
   c. Fare riferimenti alle guide per la risoluzione dei problemi di WSRR: http://pic.dhe.ibm.com/infocenter/sr/v8r0/topic/com.ibm.sr.doc/cwsr_troubleshootingandsupport.html
3. Per DataPower:
   a. Richiamare il file **default.log** per il dominio creato dal pattern.
   b. Richiamare il file **default.log** per il dominio predefinito.
4. Per i problemi di monitoraggio, raccogliere tali log dai nodi WSRR e del sistema operativo di base (esclusi i nodi personalizzati WSRR):

- /0config/0config.log
- /opt/IBM/maestro/ITCAMSOADP/lx8266/d4/KD4/logs/* (x86)
- /opt/IBM/maestro/ITCAMSOADP/aix523/d4/KD4/logs/* (Power)

Capitolo 8. Manutenzione e supporto

È possibile eseguire operazioni di manutenzione, come, ad esempio, l'applicazione di fix di emergenza.

Aggiunta di una fix di emergenza al catalogo

Le fix temporanee ed i fix pack vengono applicati alle istanze del sistema virtuale come fix di emergenza. È possibile aggiungere le fix di emergenza al proprio catalogo per applicarle alle proprie immagini virtuali.

Prima di iniziare

Per eseguire queste operazioni, è necessario disporre dell'autorizzazione *Crea nuovo contenuto del catalogo* del ruolo *Amministratore* del dispositivo IBM Workload Deployer con autorizzazioni complete.

Informazioni su questa attività

Le fix sono fornite da IBM oppure da un provider di immagini e devono essere scaricate. Le nuove fix vengono scaricate da IBM Fix Central. Le fix vengono quindi caricate nel catalogo e possono essere applicate a tutte le istanze del sistema virtuale applicabili.

Procedura

Effettuare le operazioni riportate di seguito per aggiungere una fix di emergenza al proprio catalogo.

1. Individuare e scaricare le fix di emergenza da Fix Central.
2. Opzionale: È possibile aggiungere più fix temporanee contemporaneamente. Per aggiungere più fix contemporaneamente, scaricare i file compressi da Fix Central e comprimerli in un singolo file compresso.
3. Dal menu, selezionare **Catalogo** > **Fix di emergenza**.
4. Fare clic sull'icona Aggiungi nel pannello di sinistra.
5. Immettere un nome per la fix da aggiungere. Come opzione, è anche possibile aggiungere una descrizione della fix che si sta aggiungendo. La fix viene mostrata nel pannello di sinistra della finestra Fix di emergenza e le relative informazioni vengono visualizzate nel pannello di destra.
6. Passare al percorso in cui è stata memorizzata la fix e fare clic su **Carica**. Per sicurezza, è possibile caricare solo file .zip, .tgz e .pak. È supportato anche Red Hat RPM.
7. Completare le informazioni relative alla fix. È possibile concedere l'accesso agli utenti e fornire una valutazione di severità. Utilizzare il campo **Applicabile a** per specificare l'immagine o le immagini virtuali a cui viene applicata questa fix.

Risultati

La fix di emergenza è presente nel catalogo e disponibile per essere applicata alle immagini del sistema virtuale.

Applicazione di una fix di emergenza

Le fix temporanee ed i fix pack vengono applicati alle istanze del sistema virtuale come fix di emergenza. È possibile applicare le fix di emergenza alle proprie immagini del sistema virtuale.

Prima di iniziare

Per eseguire queste operazioni, è necessario disporre di accesso completo all'istanza del sistema virtuale oppure del ruolo di gestione Dispositivo con autorizzazioni complete. Per la pianificazione o l'applicazione del servizio, l'istanza del sistema virtuale deve essere avviata. La fix di emergenza deve essere aggiunta al catalogo prima che sia possibile applicarla ad un sistema virtuale.

Informazioni su questa attività

Quando viene aggiunta una fix di emergenza, vengono definite le immagini a cui la fix è applicabile. L'elenco delle fix disponibili durante la pianificazione di una richiesta di servizio viene creato utilizzando tutte le fix applicabili all'immagine virtuale utilizzata per creare la propria istanza del sistema virtuale. Se una fix è già stata applicata al proprio sistema, è visualizzata nell'elenco **Cronologia** e non è inclusa nell'elenco delle fix disponibili.

Nota: Prima di installare una fix di emergenza, è necessario arrestare tutti i processi WAS e WSRR. Accedere utilizzando SSH a tutti i nodi WSRR ed arrestare i processi con i comandi **`stopServer.sh`** e **`stopNode.sh`** (solo nodi personalizzati).

Procedura

Per applicare una fix temporanea, effettuare le operazioni riportate di seguito.

1. Selezionare un'istanza del sistema virtuale a cui applicare la fix dalla finestra Istanza del sistema virtuale.
2. Fare clic sull'icona **Applica servizio**.
3. Opzionale: Pianificare una richiesta di servizio. Per impostazione predefinita, la fix viene applicata immediatamente. Per pianificare l'applicazione in un momento successivo, fare clic su **Pianifica servizio** e fornire le informazioni necessarie.
4. Fare clic su **Seleziona livello di servizio o fix**.
5. Fare clic su **Applica fix di emergenza** per visualizzare e selezionare la fix da applicare. La fix di emergenza viene applicata a tutte le macchine virtuali nell'istanza del sistema virtuale. Lo stato dell'istanza del sistema virtuale indica che il servizio è stato applicato al sistema virtuale.
6. Controllare gli errori. Controllare i seguenti file per assicurarsi che non si siano verificati errori durante il processo di applicazione delle fix di emergenza:
   - Remote_std_out.log
   - Remote_std_err.log

   È possibile accedere ai file di log dalla finestra Istanze del sistema virtuale.

Capitolo 9. Appendice

Notices

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

COPYRIGHT LICENSE:

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

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

Programming interface information

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

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

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

Trademarks

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

Sending your comments to IBM

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

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

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

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

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

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

- By mail, to this address:

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

WINCHESTER,
Hampshire
SO21 2JN
United Kingdom

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

Whichever method you use, ensure that you include:

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