IBM InfoSphere Information Services Director
Versão 8 Release 7

Guia para Publicação de Serviços Seguros

S517-0025-00

IBM InfoSphere Information Services Director
Versão 8 Release 7

Guia para Publicação de Serviços Seguros

S517-0025-00

Nota

Antes de utilizar essas informações e o produto suportado por elas, leia as informações em "Avisos e Marcas Registradas" na página 53.

Índice

Publicando Serviços Seguros

Depois de projetar e implementar um serviço usando o IBM® InfoSphere Information Services Director, use o IBM InfoSphere Information Server Console ou uma ferramenta de montagem para proteger esse serviço.

Antes de Iniciar

- Esses tópicos assumem que você esteja usando IBM InfoSphere Information Server e InfoSphere Information Services Director 8.5 com IBM WebSphere Application Server, Versões 6.1 ou 7.0, nos níveis de fix pack correspondentes suportados. Para localizar o nível de fix pack suportado para sua versão instalada do WebSphere Application Server, consulte a página de requisitos do sistema IBM InfoSphere Information Server: http://www.ibm.com/software/data/infosphere/info-server/overview/requirements.html

Sobre Esta Tarefa

- Essas tarefas assumem que você esteja familiarizado com serviços da Web, SOAP sobre HTTP ou SOAP sobre JMS e outros conceitos da Arquitetura Orientada a Serviços (SOA) e tenha experiência com o InfoSphere Information Services Director e o design, implementação e teste de serviços utilizando o InfoSphere Information Server.
- Os exemplos de proteção de serviços implementados nessas tarefas usam a ligação SOAP sobre HTTP.
- Muitas tarefas consistem na modificação de arquivos descritores de implementação de serviços. Você pode usar uma ferramenta de montagem, como IBM Rational Application Developer ou IBM WebSphere Application Server Toolkit, para manipular esses diversos arquivos do descritor. As tarefas nesses tópicos usam o Rational Application Developer 7.0 e o IBM WebSphere Application Server Toolkit 6.0. A ferramenta de montagem que é usada para a maioria desses procedimentos é Rational Application Developer, Versão 7.5.4.
  - O Rational Application Developer e o Rational Software Architect compartilham o mesmo código base, portanto o Rational Application Developer pode ser trocado com o Rational Software Architect futuramente. O Rational Software Architect é um superconjunto do Rational Application Developer e outras ofertas do IBM Rational (Rational Web Developer e Rational Software Modeler, por exemplo.
  - Entre as diversas ferramentas de montagem disponíveis da IBM, o Rational Software Architect ou o Rational Application Developer oferecem melhor suporte para segurança de serviços da Web, em especial com a automação da maioria das tarefas e abstração da maioria dos detalhes de segurança licalizados nos descritores de implementação por meio de uma série de assistentes. Com exceção dos assistentes, as interfaces com o usuário e os editores no Rational Application Developer 7.0 e no IBM WebSphere Application Server Toolkit 6.0 são quase idênticos.

Visão Geral da Segurança dos Serviços da Web

A segurança dos serviços da Web é um padrão de mercado que descreve como a segurança específica à carga útil pode ser aplicada aos serviços da Web padrão baseados no SOAP.

Nota: Embora o termo "serviços da Web" refira-se geralmente a mensagens formatadas pelo SOAP transportadas em HTTP, este tópico fala sobre uma série de padrões chamados de WS-Security ou Segurança de Serviços da Web. Por exemplo, a autenticação de token de nome de usuário do WS-Security é uma das muitas tecnologias de segurança que fazem parte dos padrões WS-Security. Alguns mecanismos de segurança não fazem parte do WS-Security, por exemplo, autenticação básica HTTP, autorização J2EE, criptografia SSL.

A segurança dos serviços da Web depende de outros padrões aceitos como assinatura digital e criptografia XML, e aproveita os algoritmos matemáticos, técnicas e recursos de software existentes que há tempos têm sido utilizados para comunicação e segurança de dados na Internet e outras trocas seguras mais antigas, como transações Electronic Data Interchange (EDI). A segurança dos serviços da Web é necessária porque o HTTPS com SSL é insuficiente para aplicativos complexos, especialmente aqueles que exigem fluxos de processo demorados com manipuladores (aplicativos) diferentes que fazem parte da “conversação” ou atividade do serviço da Web inteiro.

Uma ilustração utilizada com frequência é um serviço que abrange um pedido de compra inteiro. Ele pode conter detalhes do cartão de crédito para o departamento de faturamento, informações de atualização da conta para o atendimento ao cliente e informações simples do número do produto para preencher um pedido para que seja entregue. Em um ambiente de serviço distribuído, diferentes aplicativos na empresa funcionam juntos para oferecer o serviço completo. Pode ser crítico se o aplicativo de inventário tiver acesso à determinação dos detalhes de solicitação do produto se o produto desejado estiver em estoque, mas igualmente crítico se o aplicativo de inventário não tiver acesso a informações detalhadas da conta ou números de cartão de crédito. É importante que as partes envolvidas nas interações de serviços da Web consigam validar a outra parte para garantir que ninguém alterou o conteúdo da mensagem enquanto estava em trânsito.

Autenticação, integridade e sigilo são os principais recursos de segurança da segurança dos serviços da Web. Outros aspectos da segurança, como irrecusabilidade, podem ser derivados das principais funções na estrutura de segurança dos serviços da Web.

A segurança, especificamente a segurança dos serviços da Web, está cada vez mais sendo abordada em discussões sobre a Arquitetura Orientada a Serviços (SOA) e Informações como um Serviço. A adoção do padrão de segurança dos serviços da Web tem sido lenta por fornecedores e clientes, mas já se passaram muitos anos desde que o primeiro nível de padrões de segurança dos serviços da Web foi confirmado, e o interesse tem aumentado. Os motivos para a adoção lenta incluem complexidade, questões sobre desempenho, falta de ferramentas suportadas pelo fornecedor, imaturidade de padrões (ou medo dele) e o simples fato de que, para muitas implementações de serviços da Web, a segurança dos serviços da Web não é considerada necessária. O HTTPS com SSL tem sido aceitável para a maioria das implementações de serviços da Web de ponto a ponto, e saltos múltiplos complexos, em que a segurança dos serviços da Web torna-se imperativa, é ainda muito recente para a maioria das empresas. Além disso, muitas implementações de serviços da Web de produção existem atrás de firewalls ou não expõem informações importantes, o que elimina a necessidade de segurança dos serviços da Web.

Agora que a SOA é mais comum (pelo menos em discussões corporativas de arquitetura e planejamento) e os serviços da Web estão sendo prescritos com mais frequência para soluções complexas de saltos múltiplos em que muitas partes

"tocam" a carga útil de uma mensagem, a segurança dos serviços da Web está ganhando mais atenção. Consequentemente, a segurança dos serviços da Web, e a capacidade do IBM InfoSphere Information Services Director para suportá-la, está na mente de arquitetos e aqueles que tomam decisões dentro e fora da IBM.

A segurança dos serviços da Web não e fácil. Sua implementação requer um alto grau de planejamento e disciplina e cooperação entre as equipes de implementação do cliente e servidor. Isso envolve todo um raciocínio cauteloso sobre coisas como:

- Quais tipos de segurança dos serviços da Web eu preciso e desejo? (Autenticação, assinatura, criptografia, etc.)
- Quais direções? (Cliente para host? Host de volta para o cliente? Ambas as direções para todos os tipos de segurança dos serviços da Web? Redirecionamento e intermediários?)
- Quais partes e subpartes de uma mensagem? Quais tecnologias (X.509, por exemplo)?

De uma perspectiva da tecnologia, a maioria da tecnologia do tempo de execução definida pela segurança dos serviços da Web já existe. As técnicas comprovadas do segmento de mercado para assinatura digital, algoritmos de criptografia de chave privada e integração com vários protocolos são utilizadas na segurança dos serviços da Web. O que é novo é a sintaxe e as regras para a definição da segurança dos serviços da Web para mecanismos do solicitante e provedor e os nomes específicos de arquivo, extensões e propriedades customizadas representadas pela implementação de cada fornecedor.

Incluindo Segurança Usando o IBM InfoSphere Information Server Console

Usando o IBM InfoSphere Information Services Director no IBM InfoSphere Information Server Console, você pode incluir autenticação básica HTTP, autenticação de token do nome do usuário do WS-Security ou sigilo de dados que usa criptografia SSL.

Sobre Esta Tarefa

Você pode incluir segurança em seus serviços de duas formas: usando o IBM InfoSphere Information Server Console ou usando uma ferramenta de montagem. O uso de IBM InfoSphere Information Server Console é o método preferencial porque o o IBM InfoSphere Information Server Console automatiza algumas tarefas para você

Incluindo Autenticação Básica HTTP Usando o IBM InfoSphere Information Server Console

Conclua esta tarefa para incluir autenticação básica HTTP em seu serviço.

Sobre Esta Tarefa

Esta tarefa assume que a ligação conectada ao serviço é SOAP sobre HTTP. A configuração é semelhante para as outras ligações, tais como REST, REST 2.0, RSS ou EJB.

Procedimento

1. Na área de trabalho Aplicativo de Serviços de Informações, selecione um aplicativo e clique em **Abrir**.

2. Clique em **Editar**.
3. Dê um clique duplo no serviço que deseja proteger com autenticação básica HTTP.
4. Na área de janela Visão Geral do serviço, selecione **Requer Autenticação** no painel Segurança.
5. Clique na área de janela Ligações do serviço.
6. No menu **Suporte de Autenticação**, selecione **Básico HTTP**.
7. Clique em **Salvar Aplicativo**.
8. Clique em **Fechar Aplicativo**.

O que Fazer Depois

Você deve reimplementar o serviço para que as alterações sejam efetivadas.

Quando você inclui autenticação HTTP em um serviço utilizando o IBM InfoSphere Information Server Console, o IBM InfoSphere Information Services Director inclui uma regra de autorização padrão que permite que apenas os usuários com a função de Consumidor, Administrador ou Catálogo do InfoSphere Information Services Director chame as operações nesses serviços.

Incluindo Autenticação do Token do Nome do Usuário Usando o IBM InfoSphere Information Server Console

Conclua esta tarefa para incluir autenticação do token do nome do usuário em seu serviço.

Sobre Esta Tarefa

Esta tarefa assume que a ligação conectada ao serviço é SOAP sobre HTTP.

Procedimento

1. Na área de trabalho Aplicativo de Serviços de Informações, selecione um aplicativo e clique em **Abrir**.
2. Clique em **Editar**.
3. Dê um clique duplo no serviço que deseja proteger com autenticação do token do nome do usuário.
4. Na área de janela Visão Geral do serviço, selecione **Requer Autenticação** no painel Segurança.
5. Clique na área de janela Ligações do serviço.
6. No menu **Suporte de Autenticação**, selecione **Token do Nome do Usuário do WS-Security**.
7. Clique em **Salvar Aplicativo**.
8. Clique em **Fechar Aplicativo**.

O que Fazer Depois

Você deve reimplementar o serviço para que as alterações sejam efetivadas.

Quando você inclui autenticação em um serviço utilizando o IBM InfoSphere Information Server Console, o IBM InfoSphere Information Services Director inclui uma regra de autorização padrão que permite que apenas os usuários com a função de Consumidor, Administrador ou Catálogo do InfoSphere Information Services Director chame as operações nesses serviços.

Incluindo Sigilo de Dados de Criptografia SSL Usando o IBM InfoSphere Information Server Console

Conclua esta tarefa para incluir sigilo de dados de criptografia SSL em seu serviço.

Sobre Esta Tarefa

Esta tarefa assume que a ligação conectada ao serviço é SOAP sobre HTTP. A configuração é semelhante para as outras ligações, tais como Texto Sobre HTTP, REST, REST 2.0 ou RSS.

Procedimento

1. Na área de trabalho Aplicativo de Serviços de Informações, selecione um aplicativo e clique em **Abrir**.
2. Clique em **Editar**.
3. Dê um clique duplo no serviço que deseja proteger com sigilo de dados de criptografia SSL.
4. Na área de janela Visão Geral do serviço, selecione **Requer Sigilo** no painel Segurança. Se você clicar na área de janela Ligações do serviço, verá que o HTTPS é necessário para chamar esse serviço.
5. Clique em **Salvar Aplicativo**.
6. Clique em **Fechar Aplicativo**.

O que Fazer Depois

O servidor de aplicativos deve ser configurado para HTTPS e SSL para utilizar um serviço criptografado por SSL.

Incluindo Segurança Usando uma Ferramenta de Montagem

Usando uma ferramenta de montagem, você pode incluir autenticação, autorização, sigilo e integridade de dados.

Sobre Esta Tarefa

Você pode incluir segurança em seus serviços de duas formas: usando o IBM InfoSphere Information Server Console ou usando uma ferramenta de montagem. A utilização do IBM InfoSphere Information Server Console automatiza algumas tarefas que você deve executar manualmente com uma ferramenta de montagem. No entanto, o uso de uma ferramenta de montagem permite proteger um serviço de maneiras que não são possíveis usando o IBM InfoSphere Information Server Console.

Visão Geral da Estrutura de Ligação

Para ativar os recursos de segurança sem utilizar um aplicativo como uma ferramenta de montagem, é necessário compreender a estrutura básica interna de ligações para modificar suas configurações.

Esta seção oferece uma visão geral da estrutura interna de duas ligações populares: SOAP sobre HTTP e SOAP sobre JMS.

SOAP sobre JMS

SOAP sobre JMS é um tipo de ligação que pode ser anexado a um serviço. Leia este tópico para compreender a estrutura básica de uma ligação SOAP sobre JMS,

que é útil para saber se você deseja ativar configurações de segurança sem utilizar um aplicativo como uma ferramenta de montagem.

A ligação SOAP sobre JMS é responsável pela operação de unmarshall de pedidos SOAP enviados sobre uma fila ou tópico JMS para o serviço, redirecionando-os para a implementação do serviço do IBM InfoSphere Information Server como chamadas EJB e pela operação de marshall da resposta em uma mensagem SOAP enviada de volta para a fila ou tópico JMS.

Uma ligação SOAP sobre JMS consiste nos seguintes artefatos:

- Um arquivo WSDL que descreve o serviço.
- Um bean acionado por mensagens (MDB) do roteador específico ao servidor de aplicativos que atende pedidos SOAP sobre JMS que chegam.
- Um EJB de sessão sem estado de fachada que redireciona pedidos para a implementação de serviço real do InfoSphere Information Server, que contém a lógica de negócios que um cliente está buscando chamar.
- Um conjunto de classes de serializador e desserializador que mapeiam mensagens SOAP para objetos Java (tipos WSDL no tipo Java, por exemplo) de acordo com as especificações JAX-RPC.

Esses artefatos são empacotados em:

- Um jar MDB (soapjrouter.jar) que contém o MDB do roteador e os descritores de implementação.
- Um jar EJB (soapjbinding.jar) que contém o EJB de fachada, os descritores de implementação, o arquivo WSDL e as classes de serializador e desserializador.

Depois que o IBM InfoSphere Information Services Director cria um arquivo enterprise archive (EAR) do serviço antes que seja implementado, o InfoSphere Information Server cria e compacta os módulos MDB e EJB no arquivo EAR de implementação do serviço quando o serviço é implementado, conforme mostrado no diagrama a seguir.

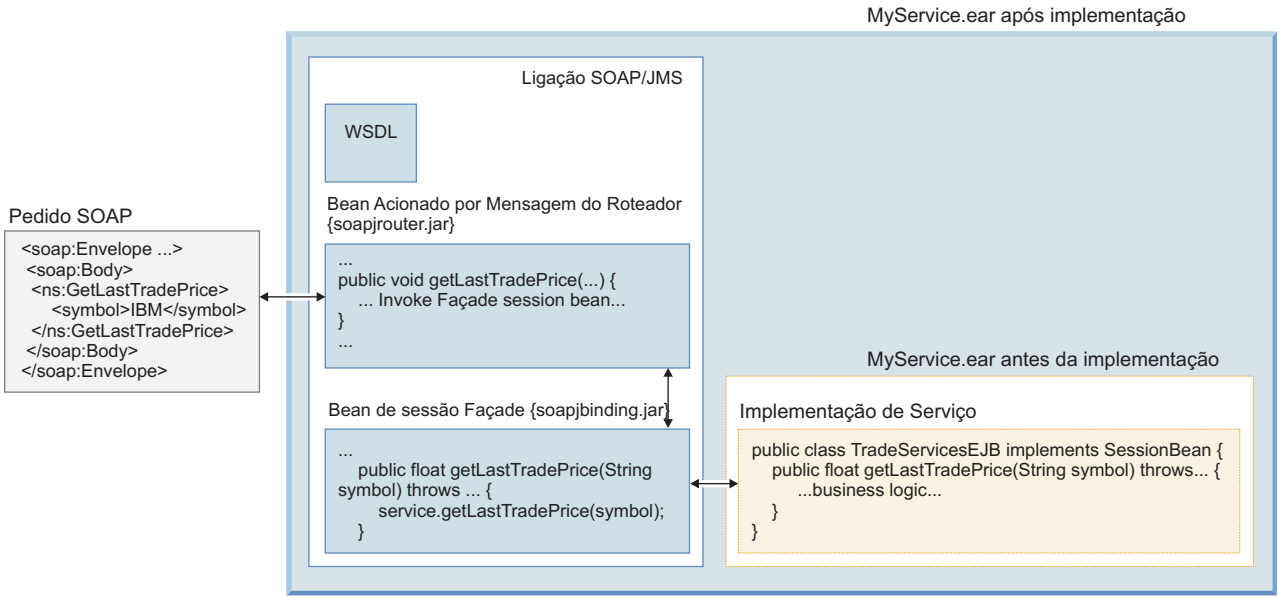

Figura 1. Um Serviço Implementado com Ligação SOAP sobre JMS

SOAP sobre HTTP

SOAP sobre HTTP é um tipo de ligação que pode ser anexado a um serviço. Leia este tópico para compreender a estrutura básica de uma ligação SOAP sobre HTTP, que é útil para saber se você deseja ativar configurações de segurança sem utilizar um aplicativo como uma ferramenta de montagem.

A ligação SOAP sobre HTTP pode ser vista como um componente de proxy do lado do servidor localizado entre clientes e serviços. É responsável pela operação de unmarshall de pedidos SOAP enviados sobre HTTP para o serviço, redirecionando-os para a implementação do serviço do IBM InfoSphere Information Server como chamadas EJB e pela operação de marshall da resposta em uma mensagem SOAP enviada sobre HTTP de volta ao cliente.

Uma ligação SOAP sobre HTTP consiste efetivamente nos seguintes artefatos:

- Um arquivo WSDL que descreve o serviço.
- Um servlet do roteador específico ao servidor de aplicativos que atende pedidos SOAP sobre HTTP que chegam.
- Um EJB de sessão sem estado de fachada que redireciona pedidos para a implementação de serviço real, que contém a lógica de negócios que um cliente está buscando chamar.
- Um conjunto de classes de serializador e desserializador que mapeiam mensagens SOAP para objetos Java (tipos WSDL no tipo Java, por exemplo) de acordo com as especificações JAX-RPC.

Esses artefatos são empacotados em:

- Um módulo da Web (soaprouter.war) que contém o servlet do roteador e os descritores de implementação.
- Um jar EJB (soapbinding.jar) que contém o EJB de fachada, os descritores de implementação, o arquivo WSDL e as classes de serializador e desserializador.

Depois que o IBM InfoSphere Information Services Director cria um arquivo enterprise archive (EAR) do serviço antes que seja implementado, o InfoSphere Information Server cria e compacta os módulos da Web e EJB no arquivo EAR de implementação do serviço quando o serviço é implementado, conforme mostrado no diagrama a seguir.

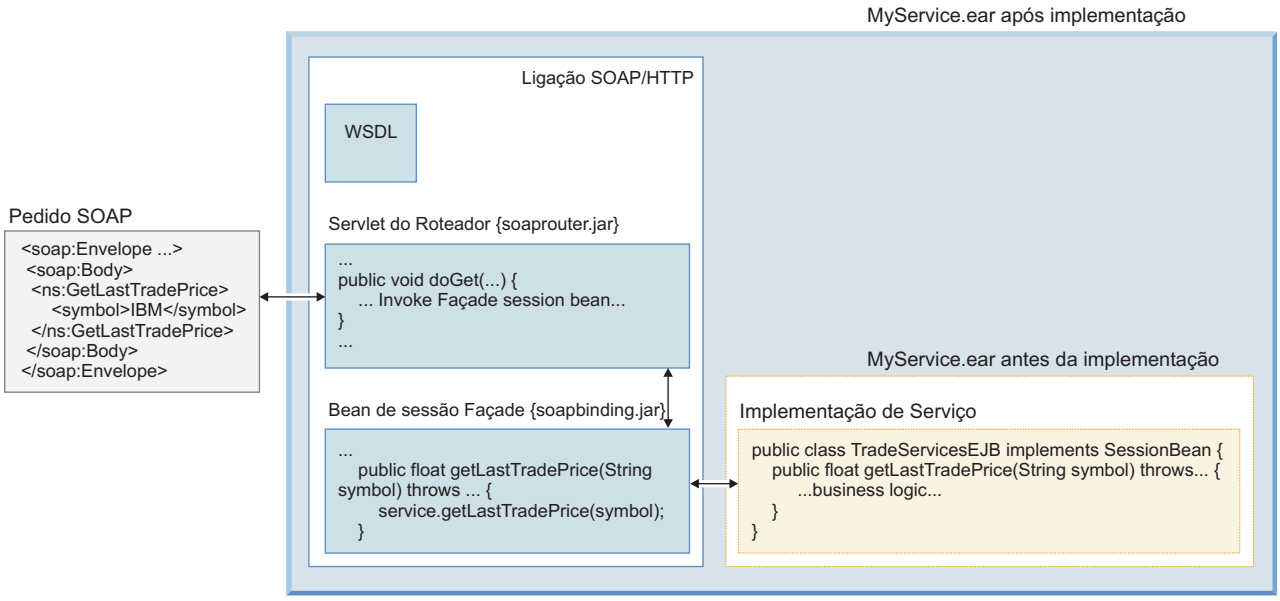

Figura 2. Um Serviço Implementado com Ligação SOAP sobre HTTP

Configurando uma Ferramenta de Montagem com o IBM InfoSphere Information Server

Para publicar serviços seguros, configure uma ferramenta de montagem para auxiliá-lo a modificar os arquivos descritores para ligações de serviço.

Sobre Esta Tarefa

O IBM InfoSphere Information Server Versão 8.5 inclui IBM WebSphere Application Server 6.1 ou 7.0 e precisa estar refletido na configuração da ferramenta de montagem. (Para os níveis de fix pack WebSphere Application Server suportados, consulte a página de requisitos do sistema IBM InfoSphere Information Server: http://www.ibm.com/software/data/infosphere/info-server/overview/requirements.html.) Mais precisamente, as bibliotecas de tempo de execução do WebSphere Application Server 6.0 ou 7.0 devem ser disponibilizadas para a ferramenta de montagem. Isso evitará vários erros e avisos ao importar o arquivo enterprise archive (EAR) do aplicativo do InfoSphere Information Server na ferramenta de montagem e também evitará erros de tempo de execução, se você planeja testar seu serviço utilizando um cliente de teste de proxy gerado pela ferramenta de montagem.

O seguinte procedimento descreve como configurar o IBM Rational Application Developer com IBM WebSphere Application Server, Versão 6.1 ou Versão 7.0. As etapas para configurar o IBM WebSphere Application Server Toolkit são idênticas.

Procedimento

1. No Rational Application Developer, clique em **Janela** > **Preferências**.
2. Na lista de preferências, selecione **Servidor** > **Tempos de Execução Instalados**.
3. Na janela Ambientes de Tempo de Execução do Servidor Instalados, clique em **Incluir** para incluir as bibliotecas de tempo de execução do InfoSphere Information Server.

A janela lista os tempos de execução do IBM WebSphere Application Server, da versão 6.1 à versão 7.0. Algumas bibliotecas de tempo de execução podem ser stubs; outras podem conter o código de implementação completo, dependendo do que você selecionou durante o processo de instalação do Rational Application Developer.

4. Na janela Novo Tempo de Execução do Servidor, selecione **WebSphere Application Server v6.1** ou **WebSphere Application Server v7.0** na pasta **IBM** e clique em **Avançar**.
5. No campo **Nome**, digite `Information Server WAS v6.1` ou `Information Server WAS v7.0` e o diretório de instalação (por exemplo, `C:\IBM\WebSphere\AppServer`) para este tempo de execução e clique em **Concluir**.
6. Clique em **OK** para sair da janela Preferências.

Desativando um Serviço Não Seguro Usando o IBM InfoSphere Information Server Console

Antes de parar e exportar um serviço usando o console do IBM WebSphere Application Server, você deve desativar a unidade da lógica de negócios (uma tarefa IBM InfoSphere DataStage, por exemplo) que o serviço contém. Para desativar o serviço, utilize o IBM InfoSphere Information Server Console.

Antes de Iniciar

- Criar um Serviço

Procedimento

1. Efetue login no IBM InfoSphere Information Server Console e abra o projeto que contém o serviço que você deseja desativar.
2. Selecione **OPERAR** > **Aplicativos de Serviços de Informações Implementados**.
3. Na área de janela Visualizar, selecione o aplicativo que contém o serviço que você deseja desativar.
4. Clique em **Editar**.
5. Na parte inferior da área de janela Visualizar, clique em **Desativar** e selecione **Desativar**.
6. Clique em **Salvar** e em **Fechar**.

Exportando um Serviço Usando o Console do WebSphere Application Server

Antes que você possa ativar os recursos de segurança para um serviço, exporte o aplicativo que contém o serviço para criar um arquivo enterprise archive (EAR). O arquivo EAR contém os arquivos descritores que você deve modificar para ativar os recursos de segurança, como autenticação.

Antes de Iniciar

- Criar um Serviço
- Desativar o Serviço Não Seguro conforme Descrito em "Desativando um Serviço Não Seguro Usando o IBM InfoSphere Information Server Console"

Procedimento

1. No WebSphere Application Server, Versão 6.1, selecione **Aplicativos** > **Aplicativos Corporativos**.

   No WebSphere Application Server, Versão 7.0, selecione **Aplicativos** > **Tipos de Aplicativos** > **WebSphere Enterprise Applications**.

2. Selecione o aplicativo que contém o serviço que deseja exportar e clique em **Parar**.
3. Selecione o aplicativo novamente e clique em **Exportar**.
4. Na janela Exportar Arquivos EAR do Aplicativo, clique no nome do aplicativo.
5. Salve o arquivo em um diretório no sistema.
6. Na janela Exportar Arquivos EAR do Aplicativo, clique em **Voltar** para voltar para a janela Aplicativos Corporativos.

Importando um Arquivo EAR do Serviço Não Seguro para uma Ferramenta de Montagem

Depois de desativar o serviço não seguro e exportá-lo como um arquivo enterprise archive (EAR), você pode utilizar uma ferramenta de montagem para importar o arquivo enterprise archive (EAR) e ativar recursos de segurança, como autenticação, autorização ou sigilo para um serviço.

Antes de Iniciar

- Criar um Serviço
- Configurar uma Ferramenta de Montagem Conforme Descrito em "Configurando uma Ferramenta de Montagem com o IBM InfoSphere Information Server" na página 8
- Desativar o Serviço Não Seguro conforme Descrito em "Desativando um Serviço Não Seguro Usando o IBM InfoSphere Information Server Console" na página 9
- Exportar o Serviço para Criar um Arquivo EAR do Serviço Conforme Descrito em "Exportando um Serviço Usando o Console do WebSphere Application Server" na página 9

Sobre Esta Tarefa

Este procedimento mostra como importar um arquivo EAR de serviço no IBM Rational Application Developer. As etapas são semelhantes se você usa o IBM WebSphere Application Server Toolkit para importar o arquivo EAR do serviço.

Procedimento

1. Na guia **Explorer do Projeto**, clique com o botão direito do mouse e selecione **Importar** > **Arquivo EAR**.
2. Na janela Importar, clique em **Procurar** para selecionar o local do arquivo EAR.
3. Selecione um nome de projeto.
4. Selecione o ambiente de tempo de execução de destino especificado quando você configurou a ferramenta de montagem. Se você seguiu a tarefa para configurar o Rational Application Developer com InfoSphere Information Server, o ambiente de tempo de execução correto será **Information Server WAS v6.1** ou **Information Server WAS v7.0**.

   Importante: Se você selecionar um ambiente de tempo de execução diferente daquele que você selecionou quando configurou a ferramenta de montagem, o arquivo EAR pode não ser importado corretamente.
5. Clique em **Avançar** para mover para a próxima janela Importar.
6. Clique em **Avançar** para mover para a janela Módulo EAR e Projetos JAR do Utilitário.
7. Clique em **Concluir**.

Resultados

O arquivo EAR será importado para a ferramenta de montagem. Agora você pode visualizar o arquivo EAR e os módulos internos, como soapbinding, na guia **Explorer do Projeto**.

Nota: Você pode ignorar o seguinte aviso se for exibido na guia **Problemas**: **CHKJ2874W: Migre a ligação padrão da origem de dados deste módulo EJB para uma ligação padrão da Connection Factory CMP**.

Protegendo um Serviço

Há quatro formas de proteger um serviço.

Incluindo Autorização Usando Restrições de Segurança J2EE

Inclua autorização como uma forma para proteger um serviço.

Sobre Esta Tarefa

Para incluir autorização, defina as permissões do método EJB no descritor de implementação EJB. Você pode editar o descritor de implementação no arquivo XML ou pode usar uma ferramenta de montagem como o IBM WebSphere Application Server Toolkit.

No modelo de segurança definido pelas especificações J2EE, defina permissões do método EJB de forma declarativa no descritor de implementação, em vez de defini-los programaticamente na implementação do serviço.

Você pode, por exemplo, restringir o acesso a um serviço apenas aos usuários que tenham a função de Administrador do Conjunto no IBM InfoSphere Information Server. Nesse caso, edite o descritor de implementação do bean de sessão do serviço `ejb-jar.xml` para definir funções de segurança e permissões do método de segurança.

Incluindo Restrições de Segurança J2EE Sem Usar uma Ferramenta de Montagem:

Conforme definido pelo modelo de segurança da especificação J2EE, inclua autorização para um serviço editando o descritor de implementação EJB. Você pode editar o descritor de implementação no arquivo XML, conforme descrito nesta tarefa.

Antes de Iniciar

- Criar um Serviço
- Desativar o Serviço Não Seguro conforme Descrito em "Desativando um Serviço Não Seguro Usando o IBM InfoSphere Information Server Console" na página 9
- Exportar o Serviço para Criar um Arquivo EAR do Serviço Conforme Descrito em "Exportando um Serviço Usando o Console do WebSphere Application Server" na página 9

Procedimento

1. Descompacte o conteúdo do arquivo *`applicationName`*`.ear` em um diretório de trabalho temporário.

2. Edite o descritor de implementação do bean de sessão do serviço *serviceName*.jar#META-INF/ejb-jar.xml e inclua os seguintes elementos de segurança no elemento **<assembly-descriptor>**.

   security-role
   Este elemento é necessário e pode aparecer várias vezes. Declara as funções de segurança que têm permissão para chamar métodos definidos neste EJB. Se você especificar uma função utilizada pelos elementos **<method-permission>**, certifique-se de declará-la no elemento **<security-role>**. As definições exatas de quais funções podem chamar qual método EJB estão no elemento **<method-permission>**.

   description
   Este é um elemento-filho do elemento **<security-role>** e é opcional. Uma descrição de texto desta função de segurança.

   role-name
   Este é um elemento-filho do elemento **<security-role>** e é necessário. Um nome de função para a qual foram concedidas algumas permissões para acessar o EJB.

   method-permission
   Este elemento é necessário e pode aparecer várias vezes. Define quais funções podem chamar quais métodos EJB.

   role-name
   Este é um elemento-filho do elemento **<method-permission>**. Este elemento é opcional e pode aparecer várias vezes. Um nome de função que pode chamar os métodos definidos pelos elementos **<method>**. Não pode ser especificado junto com um elemento **<unchecked>**.

   unchecked
   Este é um elemento-filho do elemento **<method-permission>** e é opcional. Especifica que nenhuma permissão de acesso é necessária para chamar os métodos definidos pelos elementos **<method>**. Não pode ser especificado juntamente com um elemento **<role-name>**.

   method Este é um elemento-filho do elemento **<method-permission>**. Este elemento é necessário e pode aparecer várias vezes. Define um método EJB que está sujeito a uma permissão de acesso **<role-name>** ou **<unchecked>**.

   ejb-name
   Este é um elemento-filho do subelemento **<method>** e é necessário. O nome do EJB onde este método está definido.

   method-name
   Este é um elemento-filho do subelemento **<method>** e é necessário. O nome do método EJB.

   Nota: Os elementos necessários devem ser considerados no contexto da ativação da autorização. Um elemento necessário não é necessariamente requerido pelo Esquema XML ejb-jar.xml, mas é requerido para ativar a autorização.
3. Compacte o descritor de implementação editado com o restante dos arquivos inalterados de volta para o arquivo *applicationName*.ear.

Exemplo

O exemplo a seguir mostra os arquivos `web.xml` e `ejb-jar.xml` da ligação SOAP sobre HTTP em que a autenticação básica HTTP (sem criptografia SSL) foi ativada para todos os usuários que fazem parte das funções SuiteUser e SuiteAdmin:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE ejb-jar PUBLIC "-//Sun Microsystems, Inc.
//DTD Enterprise JavaBeans 2.0//EN"
"http://java.sun.com/dtd/ejb-jar_2_0.dtd">
<ejb-jar id="ejb-jar_ID">
<description/>
    <display-name>MyApp</display-name>
    <enterprise-beans>
      <session id="MyService">
         <description/>
         <display-name>MyService</display-name>
         <ejb-name>MyService</ejb-name>
         <home>com.ibm.isd.MyApp.MyService.server.MyServiceHome
         </home>

<remote>com.ibm.isd.MyApp.MyService.server.MyServiceRemote
</remote>
         <ejb-class>com.ibm.isd.MyApp.MyService.server.impl.
         MyServiceBean</ejb-class>
         <session-type>Stateless</session-type>
         <transaction-type>Container</transaction-type>
         <resource-ref id="ResRef_MyService_Ref">
           <res-ref-name>jca/AgentConnectionFactory
           </res-ref-name>
           <res-type>com.ascential.asb.agent.ra.ConnectionFactory
           </res-type>
           <res-auth>Application</res-auth>
           <res-sharing-scope>Unshareable</res-sharing-scope>
         </resource-ref>
      </session>
    </enterprise-beans>
    <assembly-descriptor>
      <security-role>
        <role-name>SuiteUser</role-name>
      </security-role>
      <method-permission>
        <role-name>SuiteUser</role-name>
        <method>
          <ejb-name>MyService</ejb-name>
          <method-name>doNothing</method-name>
          <method-params>
            <method-param>int</method-param>
          </method-params>
        </method>
      </method-permission>
    </assembly-descriptor>
</ejb-jar>
```

Incluindo Restrições de Segurança J2EE Usando uma Ferramenta de Montagem:

Conforme definido pelo modelo de segurança da especificação J2EE, inclua autorização para um serviço editando o descritor de implementação EJB. Você pode editar o descritor de implementação no arquivo XML ou pode usar uma ferramenta de montagem. Esta tarefa documenta o método da ferramenta de montagem usando o IBM WebSphere Application Server Server Toolkit.

Antes de Iniciar

- Criar um Serviço

- Configurar uma Ferramenta de Montagem Conforme Descrito em "Configurando uma Ferramenta de Montagem com o IBM InfoSphere Information Server" na página 8
- Desativar o Serviço Não Seguro conforme Descrito em "Desativando um Serviço Não Seguro Usando o IBM InfoSphere Information Server Console" na página 9
- Exportar o Serviço para Criar um Arquivo EAR do Serviço Conforme Descrito em "Exportando um Serviço Usando o Console do WebSphere Application Server" na página 9
- Importar o Arquivo EAR de Serviço em uma Ferramenta de Montagem se Você Deseja Usar a Ferramenta para Ativar os Recursos de Segurança Conforme Descrito em "Importando um Arquivo EAR do Serviço Não Seguro para uma Ferramenta de Montagem" na página 10

Procedimento

1. Na guia **Explorer do Projeto**, expanda **Projetos EJB** > **svcs** e dê um clique duplo no arquivo do descritor de implementação para editá-lo.
2. Clique em **Montagem**.
3. Na seção **Funções de Segurança**, digite o nome da função (SuiteUser, por exemplo) que deseja incluir no campo **Nome** e clique em **Incluir**.
4. Na seção **Permissões de Método**, clique em **Incluir**.
5. Na janela Incluir Permissão de Método, selecione a função de segurança que deseja incluir e clique em **Concluir**.
6. Clique em **Salvar** para salvar suas alterações.

Incluindo Mecanismos de Autenticação

Inclua autenticação como uma forma de proteger um serviço.

Sobre Esta Tarefa

Os métodos de autenticação abordados nesta tarefa são:

- Tokens de segurança não assinados
- Tokens de segurança assinados
- Autenticação básica HTTP

Incluindo Tokens de Segurança Não Assinados Usando o Assistente do WS-Security:

Um token de segurança não assinado que autentica pedidos de serviço que chegam é uma forma de proteger um serviço. Geralmente, um token de segurança não assinado refere-se a um token do nome do usuário.

Antes de Iniciar

- Criar um Serviço
- Configurar uma Ferramenta de Montagem Conforme Descrito em "Configurando uma Ferramenta de Montagem com o IBM InfoSphere Information Server" na página 8
- Desativar o Serviço Não Seguro conforme Descrito em "Desativando um Serviço Não Seguro Usando o IBM InfoSphere Information Server Console" na página 9
- Exportar o Serviço para Criar um Arquivo Enterprise Archive (EAR) do Serviço conforme descrito em "Exportando um Serviço Usando o Console do WebSphere Application Server" na página 9

- Importar o Arquivo EAR de Serviço em uma Ferramenta de Montagem se Você Deseja Usar a Ferramenta para Ativar os Recursos de Segurança Conforme Descrito em "Importando um Arquivo EAR do Serviço Não Seguro para uma Ferramenta de Montagem" na página 10

Sobre Esta Tarefa

Você pode executar esta tarefa utilizando o Assistente do WS-Security ou o Editor de Serviços da Web. O método Editor de Serviços da Web é o mais manual. O seguinte procedimento descreve como incluir um token de nome de usuário em seu serviço usando o assistente do WS-Security.

Procedimento

1. Altere para a **Perspectiva Java EE**.
2. Na guia **Explorador de Projetos**, expanda **soapbinding** do serviço que você importou e, em seguida, expanda **Serviços**.
3. Clique com o botão direito no serviço e selecione **Serviço da Web Seguro** > **Incluir Token de Segurança Independente**.
4. Na janela Assistente do WS-Security - Token de Segurança Independente do Lado do Servidor, selecione o tipo de token **Token do Nome do Usuário**.
5. Selecione o nome da configuração JAAS **system.wssecurity.UsernameToken**. Esse nome indica que os pedidos de login que chegam serão processados pela pilha de módulos de login definida na configuração de login JAAS `system.wssecurity.UsernameToken`.
6. Clique em **Concluir**.
7. Para validar se os descritores de implementação de serviço foram corretamente atualizados, na guia **Explorador de Projetos**, expanda **soapbinding** > **Services** e clique com o botão direito no seu serviço. Selecione **Mostrar** e, em seguida, clique em **Descritor de Implementação**. O Editor de Serviços da Web é aberto.
8. Clique na guia **Extensões** para verificar se um token do nome do usuário foi criado em **Solicitar Detalhes da Configuração de Serviço do Consumidor** > **Token de Segurança Necessário**.
9. Clique na guia **Ligações** para verificar se um token do nome do usuário foi criado em **Solicitar Detalhes da Configuração de Ligação do Consumidor** > **Consumidor do Token**.

Incluindo Tokens de Segurança Não Assinados Usando o Editor de Serviços da Web:

Um token de segurança não assinado que autentica pedidos de serviço que chegam é uma forma de proteger um serviço. Geralmente, um token de segurança não assinado refere-se a um token do nome do usuário.

Antes de Iniciar

- Criar um Serviço
- Configurar uma Ferramenta de Montagem Conforme Descrito em "Configurando uma Ferramenta de Montagem com o IBM InfoSphere Information Server" na página 8
- Desativar o Serviço Não Seguro conforme Descrito em "Desativando um Serviço Não Seguro Usando o IBM InfoSphere Information Server Console" na página 9
- Exportar o Serviço para Criar um Arquivo Enterprise Archive (EAR) do Serviço conforme descrito em "Exportando um Serviço Usando o Console do WebSphere Application Server" na página 9

- Importar o Arquivo EAR de Serviço em uma Ferramenta de Montagem se Você Deseja Usar a Ferramenta para Ativar os Recursos de Segurança Conforme Descrito em "Importando um Arquivo EAR do Serviço Não Seguro para uma Ferramenta de Montagem" na página 10

Sobre Esta Tarefa

Você pode executar esta tarefa utilizando o Assistente do WS-Security ou o Editor de Serviços da Web. O método Editor de Serviços da Web é o mais manual. Este procedimento descreve como incluir um token de nome de usuário em seu serviço usando o Editor de Serviços da Web.

Procedimento

1. Na guia **Explorer do Projeto** do Rational Application Developer, expanda **soapbinding** > **ejbModule** > **META-INF** e dê um clique duplo no arquivo descritor **webservice.xml**.
2. Clique na guia **Extensões** no Editor de Serviços da Web.
3. Expanda **Extensão da Descrição de Serviços da Web** e selecione a descrição para seu serviço.
4. Expanda **Ligação do Componente de Porta** e selecione a ligação para seu serviço.
5. Expanda **Solicitar Detalhes da Configuração de Serviço do Consumidor** > **Token de Segurança Necessário**.
6. Clique em **Incluir**.
7. Na janela Token de Segurança Necessário, selecione o tipo de token **Token do Nome do Usuário** e conclua os campos restantes.
8. Clique em **OK**. O token do nome do usuário é exibido em **Solicitar Detalhes da Configuração de Serviço do Consumidor** > **Token de Segurança Necessário**.
9. Clique na guia **Configurações de Ligações** e expanda **Consumidor do Token**.
10. Clique em **Incluir**.
11. Na janela **Consumidor do Token**, preencha os campos de nome, classe, token de segurança, tipo de valor e URI. Certifique-se de selecionar o token de segurança recém-criado na lista suspensa **Token de Segurança**. Além disso, certifique-se de selecionar a caixa de opção **Usar jaas.config** e especifique `system.wssecurity.UsernameToken` no campo **jaas.config name**. Para todos os outros campos, é possível usar os valores-padrão.
12. Clique em **OK**. O consumidor do token é exibido em **Solicitar Detalhes da Configuração de Ligação do Consumidor** > **Consumidor do Token**.

Incluindo Tokens de Segurança Assinados Usando o Editor de Serviços da Web:

Um token de segurança assinado que autentica pedidos de serviço que chegam é uma forma de proteger um serviço.

Antes de Iniciar

- Criar um Serviço
- Configurar uma Ferramenta de Montagem Conforme Descrito em "Configurando uma Ferramenta de Montagem com o IBM InfoSphere Information Server" na página 8
- Desativar o Serviço Não Seguro conforme Descrito em "Desativando um Serviço Não Seguro Usando o IBM InfoSphere Information Server Console" na página 9

- Exportar o Serviço para Criar um Arquivo Enterprise Archive (EAR) do Serviço conforme descrito em "Exportando um Serviço Usando o Console do WebSphere Application Server" na página 9
- Importar o Arquivo EAR de Serviço em uma Ferramenta de Montagem se Você Deseja Usar a Ferramenta para Ativar os Recursos de Segurança Conforme Descrito em "Importando um Arquivo EAR do Serviço Não Seguro para uma Ferramenta de Montagem" na página 10

Sobre Esta Tarefa

Exemplos de tokens de segurança assinados são tokens de bilhete Kerberos, tokens de certificado X.509 ou tokens Lightweight Third Party Authentication (LTPA). Nesse procedimento, o IBM Rational Application Developer é usado para ilustrar a definição de um token de certificado X.509 como o mecanismo de autenticação para solicitações de serviço recebidas.

Procedimento

1. Na guia **Explorer do Projeto** do Rational Application Developer, expanda **soapbinding** > **ejbModule** > **META-INF** e dê um clique duplo no arquivo descritor `webservice.xml`.
2. Clique na guia **Extensões** no Editor de Serviços da Web.
3. Expanda **Extensão da Descrição de Serviços da Web** e selecione a descrição para seu serviço.
4. Expanda **Ligação do Componente de Porta** e selecione a ligação para seu serviço.
5. Expanda **Solicitar Detalhes da Configuração de Serviço do Consumidor** > **Token de Segurança Necessário**.
6. Clique em **Incluir**.
7. Na janela Token de Segurança Necessário, selecione o tipo de token **token de certificado x509** e conclua os campos restantes.
8. Clique em **OK**. O token de certificado x509 é exibido em **Solicitar Detalhes da Configuração de Serviço do Consumidor** > **Token de Segurança Necessário**.
9. Clique na guia **Configurações de Ligações** e expanda **Consumidor do Token**.
10. Clique em **Incluir**.
11. Na janela **Consumidor do Token**, preencha os campos de nome, classe, token de segurança, tipo de valor e URI. Os outros campos podem ser deixados com seus valores-padrão.
12. Clique em **OK**. O consumidor do token aparece em **Solicitar Detalhes da Configuração de Ligação do Consumidor** > **Consumidor do Token**.

Incluindo Autenticação Básica HTTP sem Usar uma Ferramenta de Montagem:

Use o método de autenticação básica HTTP para proteger um serviço em uma rede segura, como HTTPS ou uma intranet. Para ativar a autenticação básica HTTP, edite os descritores de implementação J2EE definidos no módulo de ligação SOAP.

Antes de Iniciar

- Criar um Serviço
- Desativar o Serviço Não Seguro conforme Descrito em "Desativando um Serviço Não Seguro Usando o IBM InfoSphere Information Server Console" na página 9

- Exportar o Serviço para Criar um Arquivo EAR do Serviço Conforme Descrito em "Exportando um Serviço Usando o Console do WebSphere Application Server" na página 9

Sobre Esta Tarefa

Para incluir autenticação em um serviço, edite o descritor de implementação EJB. Você pode editar o descritor de implementação no arquivo XML ou pode utilizar uma ferramenta de montagem como o IBM Rational Application Developer.

Procedimento

1. Descompacte o conteúdo do arquivo EAR para um diretório de trabalho temporário.
2. Edite o descritor de implementação da Web do servlet do roteador `soaprouter.war#WEB-INF/web.xml` e inclua os seguintes elementos de segurança no elemento-raiz **<web-app>**.

   security-constraint
   Este elemento é necessário. Define os privilégios de acesso para um conjunto de recursos definidos pelo subelemento **<web-resource-collection>**.

   web-resource-collection
   Este é um elemento-filho do elemento **<security-constraint>** e é necessário. Define os componentes do aplicativo da Web para os quais esta restrição de segurança é aplicada.

   web-resource-name
   Este é um elemento-filho do subelemento **<web-resource-collection>** e é necessário. Define o nome desta coleta de recursos da Web.

   description
   Este é um elemento-filho do subelemento **<web-resource-collection>** e é opcional. Uma descrição de texto desta coleta de recursos da Web.

   url-pattern
   Este é um elemento-filho do subelemento **<web-resource-collection>** e é necessário. Define para quais padrões de URL esta restrição de segurança se aplica. No caso do servlet do roteador SOAP, o padrão de URL `/*` deve ser utilizado. O asterisco (`*`) sozinho não é válido.

   http-method
   Este é um elemento-filho do subelemento **<web-resource-collection>**. Este elemento é opcional e pode aparecer várias vezes. Utilize um ou mais elementos **<http-method>** para declarar quais métodos HTTP (GET ou POST, por exemplo) estão sujeitos a restrição de segurança. Por padrão, isso se aplica a todos os métodos HTTP. No caso do servlet do roteador SOAP/HTTP, os pedidos são feitos utilizando o método POST. Se você especificar o elemento **<http-method>**, certifique-se de que o método POST esteja listado. Para proteger o arquivo WSDL, certifique-se de especificar o método GET também.

auth-constraint

Este é um elemento-filho do elemento **<security-constraint>** e é necessário. Define quais grupos ou diretores têm acesso à coleta de recursos da Web definidos nesta restrição de segurança.

description

Este é um elemento-filho do subelemento **<auth-constraint>** e é opcional. Uma descrição de texto desta restrição de segurança.

role-name

Este é um elemento-filho do subelemento **<auth-constraint>**. Este elemento é necessário e pode aparecer várias vezes. Define quais funções de segurança podem acessar os recursos definidos nesta restrição de segurança (SuiteUser ou SuiteAdmin, por exemplo). Replica as funções que foram definidas para a implementação do serviço.

user-data-constraint

Este é um elemento-filho do elemento **<security-constraint>** e é opcional. Define como o cliente se comunica com o servidor. Geralmente utilizado apenas para ativar o SSL.

description

Este é um elemento-filho do subelemento **<user-data-constraint>** e é opcional. Uma descrição de texto desta restrição de dados do usuário.

transport-guarantee

Este é um elemento-filho do subelemento **<user-data-constraint>** e é opcional. Especifica o tipo de restrição de segurança a ser imposta sobre os dados transferidos entre o cliente e o servidor:

- NENHUM (sem restrição)
- INTEGRAL (integridade de dados)
- CONFIDENCIAL (que é basicamente o SSL)

login-config

Este elemento é necessário. Define como um usuário é autenticado.

auth-method

Este é um elemento-filho do elemento **<login-config>** e é necessário. Especifica o método utilizado para autenticar um usuário. Nesse caso, configure como BÁSICO apenas.

realm-name

Este é um elemento-filho do elemento **<login-config>** e é opcional. Este elemento é opcional. O nome da região referenciada para autenticar credenciais do usuário.

security-role

Este elemento é necessário e pode aparecer várias vezes. Declara funções de segurança. Deve haver um elemento **<security-role>** para cada função listada no elemento **<auth-constraint>**.

description

Este é um elemento-filho do elemento **<security-role>** e é opcional. Uma descrição de texto desta função de segurança.

role-name
Este é um elemento-filho do elemento **<security-role>** e é necessário. Um nome de função para a qual foram concedidas algumas permissões neste módulo da Web.

Nota: Os elementos necessários devem ser considerados no contexto da ativação da autenticação básica HTTP. Um elemento necessário não é necessariamente requerido pelo Esquema XML `web.xml`, mas é requerido para ativar a autenticação básica HTTP.

3. Edite o descritor de implementação EJB da ligação `soapbinding.jar#META-INF/ejb-jar.xml` e inclua os seguintes elementos de segurança no elemento **<assembly-descriptor>**.

security-role
Este elemento é necessário e pode aparecer várias vezes. Declara as funções de segurança que têm permissão para chamar métodos definidos neste EJB. Se você especificar uma função utilizada pelos elementos **<method-permission>**, certifique-se de declará-la no elemento **<security-role>**. As definições exatas de quais funções podem chamar qual método EJB estão no elemento **<method-permission>**.

description
Este é um elemento-filho do elemento **<security-role>** e é opcional. Uma descrição de texto desta função de segurança.

role-name
Este é um elemento-filho do elemento **<security-role>** e é necessário. Um nome de função para a qual foram concedidas algumas permissões para acessar o EJB.

method-permission
Este elemento é necessário e pode aparecer várias vezes. Define quais funções podem chamar quais métodos EJB.

role-name
Este é um elemento-filho do elemento **<method-permission>**. Este elemento é opcional e pode aparecer várias vezes. Um nome de função que pode chamar os métodos definidos pelos elementos **<method>**. Não pode ser especificado junto com um elemento **<unchecked>**.

unchecked
Este é um elemento-filho do elemento **<method-permission>** e é opcional. Especifica que nenhuma permissão de acesso é necessária para chamar os métodos definidos pelos elementos **<method>**. Não pode ser especificado juntamente com um elemento **<role-name>**.

method Este é um elemento-filho do elemento **<method-permission>**. Este elemento é necessário e pode aparecer várias vezes. Define um método EJB que está sujeito a uma permissão de acesso **<role-name>** ou **<unchecked>**.

ejb-name
Este é um elemento-filho do subelemento **<method>** e é necessário. O nome do EJB onde este método está definido.

method-name
Este é um elemento-filho do subelemento **<method>** e é necessário. O nome do método EJB.

Nota: Os elementos necessários devem ser considerados no contexto da ativação da autenticação básica HTTP. Um elemento necessário não é necessariamente requerido pelo Esquema XML `web.xml`, mas é requerido para ativar a autenticação básica HTTP.

4. Compacte os descritores de implementação editados juntamente com o restante dos arquivos inalterados de volta para o arquivo *applicationName*`.ear`.

Exemplo

O exemplo a seguir mostra os arquivos `web.xml` e `ejb-jar.xml` da ligação SOAP sobre HTTP em que a autenticação básica HTTP (sem criptografia SSL) foi ativada para todos os usuários que fazem parte das funções SuiteUser e SuiteAdmin:

Exemplo do arquivo `web.xml`

```
soaprouter.jar#WEB-INF/web.xml
<?xml version="1.0" encoding="UTF-8"?>
<web-app xmlns="http://java.sun.com/xml/ns/j2ee"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://java.sun.com/xml/ns/j2ee
http://java.sun.com/xml/ns/j2ee/web-app_2_4.xsd" id="WebApp_ID" version="2.4">
  <display-name>MyAppSOAPBinding_HTTPRouter</display-name>
  <servlet>
    <display-name>Web services Router servlet for port-componentMyServiceSOAP
    </display-name>
    <servlet-name>MyServiceSOAP</servlet-name>
    <servlet-class>com.ibm.ws.webservices.engine.transport.http.WebServicesServlet
    </servlet-class>
  </servlet>
  <servlet-mapping>
    <servlet-name>MyServiceSOAP</servlet-name>
    <url-pattern>MyService</url-pattern>
  </servlet-mapping>
  <security-constraint>
    <display-name>SoapRouterConstraints</display-name>
    <web-resource-collection>
      <web-resource-name>SecuredSoapRouterServlet</web-resource-name>
      <url-pattern>/*</url-pattern>
      <http-method>GET</http-method>
      <http-method>POST</http-method>
    </web-resource-collection>
    <auth-constraint>
      <description>Authorized roles</description>
      <role-name>SuiteUser</role-name>
      <role-name>SuiteAdmin</role-name>
    </auth-constraint>
    <user-data-constraint>
      <transport-guarantee>NONE</transport-guarantee>
    </user-data-constraint>
  </security-constraint>
  <login-config>
    <auth-method>BASIC</auth-method>
  </login-config>
  <security-role>
    <role-name>SuiteUser</role-name>
  </security-role>
  <security-role>
    <role-name>SuiteAdmin</role-name>
  </security-role>
</web-app>
```

Exemplo do arquivo ejb-jar.xml

```
soapbinding.jar#META-INF/ejb-jar.xml
<?xml version="1.0" encoding="UTF-8"?>
<ejb-jar xmlns="http://java.sun.com/xml/ns/j2ee"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" id="ejb-jar_ID"
version="2.1" xsi:schemaLocation="http://java.sun.com/xml/ns/j2ee
http://java.sun.com/xml/ns/j2ee/ejb-jar_2_1.xsd">
  <enterprise-beans>
    <session id="MyServiceSOAP">
      <description></description>
      <ejb-name>MyServiceSOAP</ejb-name>
      <home>com.ibm.isd.MyApp.MyService.server.MyServiceHome
      </home>
      <remote>com.ibm.isd.MyApp.MyService.server.MyServiceRemote
      </remote>
      <service-endpoint>com.ibm.isd.MyApp.MyService.MyService
      </service-endpoint>
      <ejb-class>com.ibm.isd.MyApp.MyService.MyServiceSOAPBindingBean
      </ejb-class>
      <session-type>Stateless</session-type>
      <transaction-type>Container</transaction-type>
      <ejb-ref id="EjbRef_MyService_Ref">
        <ejb-ref-name>ejb/MyService</ejb-ref-name>
        <ejb-ref-type>Session</ejb-ref-type>
        <home>com.ibm.isd.MyApp.MyService.server.MyServiceHome</home>
        <remote>com.ibm.isd.MyApp.MyService.server.MyServiceRemote</remote>
      </ejb-ref>
    </session>
  </enterprise-beans>
    <assembly-descriptor>
      <security-role>
        <role-name>SuiteUser</role-name>
      </security-role>
      <security-role>
        <role-name>SuiteAdmin</role-name>
      </security-role>
      <method-permission>
        <role-name>SuiteUser</role-name>
        <role-name>SuiteAdmin</role-name>
        <method>
          <ejb-name>MyServiceSOAP</ejb-name>
          <method-intf>Remote</method-intf>
          <method-name>doNothing</method-name>
          <method-params>
          <method-param>int</method-param>
          </method-params>
        </method>
      </method-permission>
      <method-permission>
        <unchecked/>
        <method>
          <ejb-name>MyServiceSOAP</ejb-name>
          <method-intf>Home</method-intf>
          <method-name>create</method-name>
          <method-params>
          </method-params>
        </method>
        <method>
          <ejb-name>MyServiceSOAP</ejb-name>
          <method-intf>Home</method-intf>
          <method-name>remove</method-name>
        </method>
      </method-permission></assembly-descriptor>
    </assembly-descriptor>
  </ejb-jar>
```

Incluindo Autenticação Básica HTTP Usando uma Ferramenta de Montagem:

Use o método de autenticação básica HTTP para proteger um serviço em uma rede segura, como HTTPS ou uma intranet. Para ativar a autenticação básica HTTP, edite os descritores de implementação J2EE definidos no módulo de ligação SOAP.

Antes de Iniciar

- Criar um Serviço
- Configurar uma Ferramenta de Montagem Conforme Descrito em "Configurando uma Ferramenta de Montagem com o IBM InfoSphere Information Server" na página 8
- Desativar o Serviço Não Seguro conforme Descrito em "Desativando um Serviço Não Seguro Usando o IBM InfoSphere Information Server Console" na página 9
- Exportar o Serviço para Criar um Arquivo EAR do Serviço Conforme Descrito em "Exportando um Serviço Usando o Console do WebSphere Application Server" na página 9
- Importar o Arquivo EAR de Serviço em uma Ferramenta de Montagem se Você Deseja Usar a Ferramenta para Ativar os Recursos de Segurança Conforme Descrito em "Importando um Arquivo EAR do Serviço Não Seguro para uma Ferramenta de Montagem" na página 10

Sobre Esta Tarefa

Para incluir autenticação em um serviço, edite o descritor de implementação EJB. Você pode editar o descritor de implementação no arquivo XML. Como alternativa, é possível usar uma ferramenta de montagem como IBM Rational Application Developer, conforme descrito neste procedimento.

Procedimento

1. Na guia **Explorer do Projeto**, expanda o módulo **soaprouter**.
2. Dê um clique duplo no arquivo descritor de implementação da Web para editá-lo.
3. Clique na guia **Páginas**.
4. Na seção **Login**, selecione o **Método de Autenticação** > **BÁSICO** e salve a alteração.
5. Clique na guia **Segurança**.
6. Na seção **Funções de Segurança**, digite o nome da função que deseja incluir no campo **Nome** e clique em **Incluir**.
7. Na seção **Restrições de Segurança**, clique em **Incluir**.

   Faça as restrições de segurança para a autenticação iguais às restrições de segurança definidas ao incluir a autorização no serviço.
8. Digite um nome para a restrição e clique em **Avançar**.
9. Digite um nome de recurso da Web, selecione **POST** e **GET** para o **método HTTP** e inclua `/*` no campo **Padrão**. Para proteger o WSDL do serviço, você deve proteger o método GET HTTP.
10. Clique em **Concluir**.
11. Na seção **Funções Autorizadas**, clique em **Incluir**.
12. Selecione o **Nome da Função** incluído na seção **Funções de Segurança** e clique em **Concluir**.
13. Na seção **Restrição de Dados do Usuário**, selecione **NENHUM** e salve as alterações. Essa restrição é utilizada apenas para conexões SSL.

14. Na seção **Projetos EJB** da guia **Explorer do Projeto**, expanda o módulo **soapbinding**.
15. Dê um clique duplo no arquivo descritor de implementação EJB para editá-lo.
16. Clique na guia **Montagem**.
17. Na seção **Funções de Segurança**, clique em **Incluir** e digite o mesmo nome da função incluído no descritor de implementação da Web.
18. Na seção **Permissões de Método**, clique em **Incluir**.
19. Na janela Permissão de Método, selecione a função de segurança e clique em **Avançar**.
20. Na janela Seleção do Enterprise Bean, selecione o enterprise bean para seu serviço e clique em **Avançar**.
21. Na janela Elementos do Método, selecione os métodos que deseja proteger. Em uma situação típica, selecione todos os métodos.
22. Clique em **Concluir** e salve as alterações.

Incluindo Sigilo de Dados Usando a Criptografia SSL

Inclua sigilo de dados como uma forma de proteger um serviço.

Sobre Esta Tarefa

Inclua a confidencialidade de dados usando o protocolo Secure Sockets Layer (SSL). Conclua esta tarefa para ativar o SSL no lado do servidor do serviço. Em seguida, você deve fazer as mesmas alterações na configuração do lado do cliente. Por exemplo, se você alterar a configuração do lado do servidor para usar o protocolo Transport Secure Layer (TSL), em vez do SSL, você também deve configurar o cliente para usar TSL.

O protocolo SSL é baseado na infraestrutura da chave pública (PKI). Assim, as chaves públicas para o cliente e o servidor devem ser geradas e armazenadas, respectivamente, em keystores e truststores para que a conexão SSL seja concluída. Essa tarefa usa keystores e certificados auto-assinados de amostra. Use keystores de amostra apenas para testes. Em um ambiente de produção real, implemente sua própria PKI.

Esta é uma visão geral do processo para ativação do SSL:

- O cliente autentica o servidor; depois disso, uma sessão é iniciada. Essa autenticação é chamada de protocolo de negociação SSL. Opcionalmente, o cliente também pode ser autenticado no servidor.
- Se a negociação SSL for bem-sucedida, a transferência de dados será, então, iniciada e criptografada. Isso é chamado de protocolo de relatório SSL.
- Se houver alarmes em qualquer momento durante a sessão, um pacote de alerta será enviado para o destinatário apropriado. Esse pacote de alerta é chamado de protocolo de alerta SSL.

A tarefa a seguir descreve como incluir sigilo de dados utilizando a criptografia SSL:

Configurando um Serviço para Usar Criptografia SSL:

Depois de criar um repertório Secure Sockets Layer (SSL) no IBM WebSphere Application Server, conclua esta tarefa para ativar o SSL no lado do servidor do serviço. Em seguida, você deve fazer as mesmas alterações na configuração do lado

do cliente. Por exemplo, se você alterar a configuração do lado do servidor para usar o protocolo Transport Secure Layer (TSL), em vez do SSL, você também deve configurar o cliente para usar TSL.

Antes de Iniciar

- Criar um Serviço
- Configurar uma Ferramenta de Montagem Conforme Descrito em "Configurando uma Ferramenta de Montagem com o IBM InfoSphere Information Server" na página 8
- Desativar o Serviço Não Seguro conforme Descrito em "Desativando um Serviço Não Seguro Usando o IBM InfoSphere Information Server Console" na página 9
- Exportar o Serviço para Criar um Arquivo EAR do Serviço Conforme Descrito em "Exportando um Serviço Usando o Console do WebSphere Application Server" na página 9
- Importar o Arquivo EAR de Serviço em uma Ferramenta de Montagem se Você Deseja Usar a Ferramenta para Ativar os Recursos de Segurança Conforme Descrito em "Importando um Arquivo EAR do Serviço Não Seguro para uma Ferramenta de Montagem" na página 10

Procedimento

1. Na guia **Explorer do Projeto** do IBM Rational Application Developer, expanda **soaprouter** e dê um clique duplo no descritor de implementação para editá-lo.
2. Selecione a guia **Segurança**.
3. Na seção **Restrições de Segurança**, clique em **Incluir**.
4. Digite um nome para a restrição na página **Incluir Restrições** e clique em **Avançar**.
5. Digite um nome para o recurso na página **Incluir Recurso da Web**.
6. Selecione um método HTTP na lista **Métodos HTTP**. Selecione pelo menos o método POST para proteger seu serviço. Se não quiser que a restrição de segurança seja aplicada ao arquivo Web Services Description Language (WSDL), não selecione o método GET.
7. Inclua `/*` no campo **Padrão** para especificar o padrão de URL que é aplicado à restrição de segurança.
8. Clique em **Concluir**.
9. Na seção **Restrição de Dados do Usuário**, selecione **CONFIDENCIAL** no campo **Tipo**.
10. Salve as alterações.

O que Fazer Depois

Incluindo a Integridade de Dados

Inclua a integridade de dados usando um assinatura digital XML como uma forma de proteger um serviço.

Sobre Esta Tarefa

Visão geral do processo de assinatura digital:

- O cliente (remetente) assina partes da mensagem de pedido utilizando uma chave privada. A chave privada do cliente é armazenada no keystore do cliente.
- O servidor (receptor) valida as assinaturas digitais do cliente na mensagem de pedido utilizando a chave pública do cliente. A chave pública do cliente é armazenada no keystore do servidor.

Incluindo uma Assinatura Digital XML:

Para incluir integridade de dados em seu serviço utilizando uma assinatura digital XML, edite o arquivo descritor de implementação utilizando uma ferramenta de montagem como o IBM Rational Application Developer.

Antes de Iniciar

- Criar um Serviço
- Configurar uma Ferramenta de Montagem Conforme Descrito em "Configurando uma Ferramenta de Montagem com o IBM InfoSphere Information Server" na página 8
- Desativar o Serviço Não Seguro conforme Descrito em "Desativando um Serviço Não Seguro Usando o IBM InfoSphere Information Server Console" na página 9
- Exportar o Serviço para Criar um Arquivo Enterprise Archive (EAR) do Serviço conforme descrito em "Exportando um Serviço Usando o Console do WebSphere Application Server" na página 9
- Importar o Arquivo EAR de Serviço em uma Ferramenta de Montagem se Você Deseja Usar a Ferramenta para Ativar os Recursos de Segurança Conforme Descrito em "Importando um Arquivo EAR do Serviço Não Seguro para uma Ferramenta de Montagem" na página 10

Sobre Esta Tarefa

Restrições

Nesta tarefa, utilize o Editor de Serviços da Web no IBM Rational Application Developer para editar o arquivo descritor de implementação. Não utilize o assistente de segurança do Rational Application Developer para editar o arquivo descritor de implementação. O assistente não permite controlar recursos de assinatura digital XML como algoritmos de assinatura e transformação.

Esta tarefa mostra como assinar e validar assinaturas digitais para mensagens de pedido, não mensagens de resposta. No entanto, o procedimento para assinar e validar assinaturas digitais para mensagens de resposta é quase idêntico e, portanto, não está documentado aqui. Para resumir essa tarefa, configure o consumidor da resposta (lado do cliente) e o gerador de resposta (lado do servidor) da mesma forma que o gerador de pedido (lado do cliente) e o consumidor do pedido (lado do servidor) são configurados nesta seção.

Procedimento

1. Na guia **Explorador de Projetos** do Rational Application Developer, expanda **soapbinding** > **Services** e clique com o botão direito em seu serviço. Selecione **Mostrar** e, em seguida, clique em **Descritor de Implementação**. O Editor de Serviços da Web é aberto.
2. Clique na guia **Extensões** no Editor de Serviços da Web.
3. Expanda **Extensão da Descrição de Serviços da Web** e selecione a descrição para seu serviço.
4. Expanda **Ligação do Componente de Porta** e selecione a ligação para seu serviço.
5. Expanda **Solicitar Detalhes da Configuração de Serviço do Consumidor** > **Integridade Necessária**.
6. Na janela Integridade Necessária, clique em **Incluir**.

7. No campo **Nome da Integridade Necessária** da janela Sigilo Necessário, digite um nome.
8. No campo **Tipo de Uso**, selecione **Necessário** se quiser que a integridade seja necessária ou **Opcional** se quiser que a integridade seja opcional.
9. No campo **Partes da Mensagem**, selecione as partes da mensagem que deseja que sejam assinadas. Você pode utilizar palavras-chave ou expressões XPath para assinar as partes da mensagem. Se quiser incluir partes da mensagem:
   a. Clique em **Incluir**.
   b. Você pode utilizar palavras-chave para identificar partes genéricas da mensagem; selecione **http://www.ibm.com/websphere/webservices/wssecurity/dialect-was** na coluna Dialeto de Partes e selecione a parte da mensagem que deseja assinar na coluna Palavra-chave de Partes.
   c. Você pode utilizar expressões XPath para identificar partes mais específicas da mensagem; selecione **http://www.w3.org/TR/1999/REC-xpath-19991116** na coluna Dialeto de Partes.
   d. Opcional: No campo **Partes da Mensagem**, especifique a ocasião para evitar ataques de resposta.
   e. Opcional: No campo **Partes da Mensagem**, especifique um registro de data e hora para designar uma vida útil para a mensagem.
10. Clique na guia **Configurações de Ligações** no Editor de Serviços da Web.
11. Expanda **Solicitar Configuração de Ligação do Consumidor** > **Âncora de Confiança** e clique em **Incluir**.
12. Na janela Âncora de Confiança:
    a. Digite um nome para a âncora de confiança.
    b. Digite uma senha para o keystore.
    c. Digite o caminho completo para o keystore do lado do servidor, por exemplo, `C:\sampleks\receiverkeys.jks`.
    d. Selecione o tipo de keystore.
    e. Clique em **OK**.
13. No Editor de Serviços da Web, expanda **Solicitar Configuração de Ligação do Consumidor** > **Consumidor do Token** e clique em **Incluir**.
14. Na janela Consumidor do Token:
    a. Digite um nome de consumidor do token.
    b. Selecione **com.ibm.wssip.wssecurity.token.X509TokenConsumer** como a classe do consumidor do token.
    c. Não selecione um token de segurança. Para assinatura, não é necessário especificar um token de segurança nas extensões do serviço.
    d. Selecione **Utilizar tipo de valor** e selecione o tipo de valor **Token v3 do certificado X509**.
    e. Selecione **Utilizar jaas.config** e digite `system.wssecurity.X509BST` no campo **nome jaas.config**.
    f. Selecione **Utilizar configurações do caminho do certificado** e **Referência do caminho do certificado** ou **Confiar em qualquer certificado**. Se você selecionar **Utilizar configurações do caminho do certificado**, selecione o nome da âncora de confiança criada acima.
    g. Clique em **OK**.
15. No Editor de Serviços da Web, expanda **Solicitar Configuração de Ligação do Consumidor** > **Localizador de Chaves** e clique em **Incluir**.
16. Na janela Localizador de Chaves:

a. Digite um nome de localizador de chaves.
b. Selecione uma implementação de classe do localizador de chaves. Utilize **com.ibm.wsspi.wssecurity.keyinfo.X509TokenKeyLocator** se estiver utilizando o token de segurança X.509 da mensagem do remetente para validação de assinatura digital.
c. Clique em **OK**.

17. No Editor de Serviços da Web, expanda **Solicitar Configuração de Ligação do Consumidor** > **Informações Chave** e clique em **Incluir**.
18. Na janela Informações Chave:
    a. Digite um nome de informações chave.
    b. Selecione um tipo de informações chave. Utilize **STRREF** como o tipo de informações chave se o token de segurança utilizado para validação da assinatura digital for referenciado diretamente utilizando um URI na mensagem do remetente.
    c. Selecione uma classe de informações chave. Se você selecionou **STRREF** como o tipo de informações chave, **com.ibm.ws.webservices.wssecurity.keyinfo. STRReferenceContentConsumer** será selecionado automaticamente.
    d. Selecione **Utilizar localizador de chaves** e selecione o nome do localizador de chaves criado na seção Localizador de Chaves.
    e. Selecione **Utilizar token** e selecione o nome do consumidor do token criado na seção Consumidor do Token.
    f. Clique em **OK**.
19. No Editor de Serviços da Web, expanda **Solicitar Configuração de Ligação do Consumidor** > **Informações sobre Assinatura** e clique em **Incluir**.
20. Na janela Informações sobre Assinatura:
    a. Digite um nome de informações sobre assinatura.
    b. Selecione um algoritmo do método de canonicalização. O valor-padrão é **http://www.w3.org/2001/10/xml-exc-c14n#**.
    c. Selecione um algoritmo do método de assinatura. O valor-padrão é **http://www.w3.org/2000/09/xmldsig#rsa-sha1**.
    d. Clique em **Incluir**, selecione o elemento de informações chave criado na seção Informações Chave e digite um nome de informações chave.
    e. Clique em **OK**.
21. No Editor de Serviços da Web, expanda **Solicitar Configuração de Ligação do Consumidor** > **Referência da Parte** e clique em **Incluir**.
22. Na janela Referência da Parte:
    a. Digite um nome de referência da parte.
    b. Selecione uma parte de integridade necessária criada na seção Integridade Necessária.
    c. Selecione um algoritmo do método de compilação. O valor-padrão é **http://www.w3.org/2000/09/xmldsig#sha1**.
    d. Clique em **OK**.
23. No Editor de Serviços da Web, expanda **Solicitar Configuração de Ligação do Consumidor** > **Transformações** e clique em **Incluir**. A seção Transformações é disponibilizada depois que você cria uma referência de parte. Os elementos de transformações armazenam informações sobre as operações que foram desempenhadas nos dados antes de serem assinados.
24. Na janela Transformação:

a. Digite um nome de transformação.
b. Selecione um algoritmo para desempenhar a operação. O valor-padrão é **http://www.w3.org/2002/10/xml-exc-c14n#**.
c. Clique em **OK**.

25. Salve suas alterações.

Exportando um Arquivo EAR do Serviço Seguro de uma Ferramenta de Montagem

Depois de ativar os recursos de segurança, como autenticação, autorização ou sigilo, para um serviço utilizando uma ferramenta de montagem, você pode exportar o serviço seguro como um arquivo enterprise archive (EAR).

Antes de Iniciar

- Criar um Serviço
- Configurar uma Ferramenta de Montagem Conforme Descrito em "Configurando uma Ferramenta de Montagem com o IBM InfoSphere Information Server" na página 8
- Desativar o Serviço Não Seguro conforme Descrito em "Desativando um Serviço Não Seguro Usando o IBM InfoSphere Information Server Console" na página 9
- Exportar o Serviço para Criar um Arquivo Enterprise Archive (EAR) do Serviço conforme descrito em "Exportando um Serviço Usando o Console do WebSphere Application Server" na página 9
- Importar o Arquivo EAR de Serviço em uma Ferramenta de Montagem se Você Deseja Usar a Ferramenta para Ativar os Recursos de Segurança Conforme Descrito em "Importando um Arquivo EAR do Serviço Não Seguro para uma Ferramenta de Montagem" na página 10
- Proteger um Serviço Conforme Descrito em "Protegendo um Serviço" na página 11

Sobre Esta Tarefa

Este procedimento mostra como exportar um arquivo EAR de serviço do IBM Rational Application Developer. As etapas são semelhantes se você usa o IBM WebSphere Application Server Toolkit para exportar o arquivo EAR de serviço.

Procedimento

1. Na guia **Explorer do Projeto**, clique com o botão direito do mouse no arquivo EAR e selecione **Exportar** > **Arquivo EAR**.
2. Na janela Exportar, clique em **Procurar** para selecionar o local do arquivo EAR.
3. Selecione a caixa de opção **Sobrescrever Arquivo Existente** para sobrescrever o arquivo EAR de serviço não seguro.
4. Clique em **Concluir**.

Reimplementando um Serviço Seguro com o Console do IBM WebSphere Application Server

Depois de ativar os recursos de segurança, como autenticação, autorização ou sigilo, para um serviço e exportar o serviço seguro como um arquivo enterprise archive (EAR), reimplemente o serviço seguro utilizando o console do IBM WebSphere Application Server.

Antes de Iniciar

- Criar um Serviço
- Configurar uma Ferramenta de Montagem Conforme Descrito em "Configurando uma Ferramenta de Montagem com o IBM InfoSphere Information Server" na página 8
- Desativar o Serviço Não Seguro conforme Descrito em "Desativando um Serviço Não Seguro Usando o IBM InfoSphere Information Server Console" na página 9
- Exportar o Serviço para Criar um Arquivo Enterprise Archive (EAR) do Serviço conforme descrito em "Exportando um Serviço Usando o Console do WebSphere Application Server" na página 9
- Importar o Arquivo EAR de Serviço em uma Ferramenta de Montagem se Você Deseja Usar a Ferramenta para Ativar os Recursos de Segurança Conforme Descrito em "Importando um Arquivo EAR do Serviço Não Seguro para uma Ferramenta de Montagem" na página 10
- Proteger um Serviço Conforme Descrito em "Protegendo um Serviço" na página 11
- Exportar o Arquivo EAR que Contém o Serviço Conforme Descrito em "Exportando um Arquivo EAR do Serviço Seguro de uma Ferramenta de Montagem" na página 29

Procedimento

1. Selecione **Aplicativos** > **Aplicativos Corporativos**.
2. Se seu aplicativo não for parado (indicado por um X vermelho na coluna de status), selecione o aplicativo e clique em **Parar**.
3. Selecione o aplicativo e clique em **Desinstalar**.
4. Na janela Desinstalar Aplicativo, clique em **OK**.
5. Clique em **Salvar** para aplicar as alterações à configuração principal e clique em **Salvar** na janela que é exibida.
6. Na janela Aplicativos Corporativos, selecione o aplicativo e clique em **Instalar**.
7. Na janela Preparando a Instalação do Aplicativo, clique em **Procurar** para selecionar o local do arquivo EAR do serviço seguro e clique em **Avançar**.
8. Clique em **Avançar** até chegar ao resumo do aplicativo.
9. Clique em **Concluir**. Mensagens indicando o progresso da instalação são exibidas.
10. Clique em **Salvar na Configuração Principal** e em **Salvar** na janela que é exibida.
11. Na janela Aplicativo Corporativo, selecione o aplicativo recém-instalado e clique em **Iniciar**.

Ativando um Serviço Seguro Usando o IBM InfoSphere Information Server Console

Depois que o serviço seguro for reimplementado no console do IBM WebSphere Application Server, ative o serviço do IBM InfoSphere Information Server Console.

Antes de Iniciar

- Criar um Serviço
- Configurar uma Ferramenta de Montagem Conforme Descrito em "Configurando uma Ferramenta de Montagem com o IBM InfoSphere Information Server" na página 8

- Desativar o Serviço Não Seguro conforme Descrito em "Desativando um Serviço Não Seguro Usando o IBM InfoSphere Information Server Console" na página 9
- Exportar o Serviço para Criar um Arquivo Enterprise Archive (EAR) do Serviço conforme descrito em "Exportando um Serviço Usando o Console do WebSphere Application Server" na página 9
- Importar o Arquivo EAR de Serviço em uma Ferramenta de Montagem se Você Deseja Usar a Ferramenta para Ativar os Recursos de Segurança Conforme Descrito em "Importando um Arquivo EAR do Serviço Não Seguro para uma Ferramenta de Montagem" na página 10
- Proteger um Serviço Conforme Descrito em "Protegendo um Serviço" na página 11
- Exportar o Arquivo EAR que Contém o Serviço Conforme Descrito em "Exportando um Arquivo EAR do Serviço Seguro de uma Ferramenta de Montagem" na página 29
- Reimplementar o Arquivo EAR de Serviço Conforme Descrito em "Reimplementando um Serviço Seguro com o Console do IBM WebSphere Application Server" na página 29

Procedimento

1. Efetue login no IBM InfoSphere Information Server Console e abra um projeto que contém o serviço que você deseja ativar.
2. Selecione **OPERAR** > **Aplicativos de Serviços de Informações Implementados**.
3. Na área de janela Visualizar, selecione o aplicativo que contém o serviço que você deseja ativar.
4. Clique em **Editar**.
5. Na parte inferior da área de janela Visualizar, clique em **Desativar** e selecione **Ativar**.
6. Clique em **Salvar** e em **Fechar**.

Gerando um Cliente de Teste

Você pode gerar um cliente de teste para testar seus serviços. Você pode gerar o cliente de teste com a segurança ativada ou desativada.

Gerando um Cliente de Teste com a Segurança Desativada

Utilize esta tarefa para gerar um cliente de teste para um serviço com segurança que esteja desativada.

Antes de Iniciar

- Criar um Serviço
- Configurar uma Ferramenta de Montagem Conforme Descrito em "Configurando uma Ferramenta de Montagem com o IBM InfoSphere Information Server" na página 8

Sobre Esta Tarefa

Se você chamar um serviço seguro utilizando a autenticação do token do nome do usuário com um cliente de teste não seguro, você receberá a seguinte exceção de segurança:

```
exceção: com.ibm.wsspi.wssecurity.SoapSecurityException:
WSEC5509E: Um token de segurança cujo tipo seja
http://myapp.wisd.ibm.com#UsernameTokenhttp:
//docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-
token-profile-1.0#UsernameToken] é necessário.
```

Para um token de certificado X.509, você receberá a seguinte exceção de segurança:

```
exceção: com.ibm.wsspi.wssecurity.SoapSecurityException:
WSEC5509E: Um token de segurança cujo tipo seja
[X509Tokenhttp://docs.oasis-open.org/wss/2004
/01/oasis-200401-wss-x509-token-profile-1.0#X509] é necessário.
```

Procedimento

1. Na guia **Servidores** do IBM WebSphere Application Server, clique com o botão direito em qualquer lugar dentro da janela e clique em **Novo** > **Servidor**.
2. Na página **Definir um Novo Servidor** da janela Novo Servidor, insira um nome para o host do servidor, clique em **IBM** > **WebSphere v6.1 Server** ou **WebSphere v7.0 Server** como o tipo de servidor e clique em **Information Server WAS v6.1** ou **Information Server WAS v7.0** como o ambiente de tempo de execução do servidor.
3. Clique em **Avançar** e certifique-se de que as informações na página seguinte estejam corretas, incluindo o nome do perfil e as informações sobre autenticação. Opcionalmente, é possível clicar no link **Conexão de Teste** para assegurar-se de que o IBM Rational Application Developer possa se conectar ao WebSphere Application Server, usando as informações de autenticação recém-especificadas.
4. Clique em **Avançar**.
5. Na página **Incluir e Remover Projetos**, clique no arquivo *MyApp*`.ear` no campo **Projetos Disponíveis** e clique em **Incluir >** para incluí-lo na lista de projetos configurados.
6. Clique em **Avançar** e, em seguida, em **Concluir**. Com o servidor no lugar, sempre que necessário, agora é possível incluir um projeto neste servidor, clicando com o botão direito no servidor na guia **Servidores** e selecionando **Incluir e Remover Projetos**.
7. Na guia **Servidores**, selecione o servidor criado e clique no ícone **Iniciar o servidor**.
8. Selecione **Arquivo** > **Novo** > **Projeto** > **Projeto da Web Dinâmico**.
9. Na janela Novo Projeto da Web Dinâmico, insira um nome de projeto (MyAppClient, por exemplo), selecione a versão WebSphere Application Server apropriada como o tempo de execução de destino, selecione **Incluir Projeto em um EAR** e insira um nome de projeto de arquivo enterprise archive (EAR) (MyAppClient.ear, por exemplo) para o arquivo EAR que conterá o código do cliente.
10. Clique em **Concluir**.
11. Clique em **Arquivo** > **Novo** > **Outro**.
12. Na janela **Novo**, expanda **Serviços da Web**, selecione **Cliente de Serviço da Web** e clique em **Avançar**.
13. Na página **Serviços da Web** da janela Cliente de Serviço da Web, insira a URL do Web Services Description Language (WSDL) (por exemplo, http://localhost:9080/wisd/MyApp/MyService?wsdl) no campo **Definição de Serviço**.
14. Selecione **Cliente de Teste** como o nível de automação.
15. No painel Configuração, verifique estas configurações:

Servidor
Websphere v6.1 Server ou Websphere v7.0 Server

Tempo de Execução do Serviço da Web
IBM WebSphere JAX-RPC

Projeto do Cliente
MyAppClient

Projeto EAR do Cliente
MyAppClient.ear

16. Clique em **Concluir**.
17. Na página **Teste do Cliente de Serviço da Web**, selecione o recurso de teste **JSPs de Amostra do Serviço da Web** e o método que deseja testar. Utilize as configurações padrão para o restante desta página e clique em **Concluir**.
18. Para ver o cliente de teste no **Explorer do Projeto** em **Serviços da Web JSR-109** > **Clientes**, reinicie o IBM Rational Application Developer. Você precisará ver o cliente de teste se quiser utilizá-lo para executar os assistentes de segurança.
19. Opcional: Para testar seu serviço utilizando o cliente de teste, na guia **Cliente de Teste de Serviços da Web** que é aberta, selecione um método, digite qualquer número de entrada e clique em **Chamar**. A área de janela **Resultado** exibe o resultado.
20. Opcional: Para chamar o cliente de teste sem usar a ferramenta de montagem, use um navegador da Web e insira a URL `https://`*`hostname`*`:`*`WASSSLChannelPort`*`/`*`applicationName`*`/sample`*`serviceName`*`PortTypeProxy/TestClient.jsp`.

hostname
O nome do servidor hospedando seu cliente de teste (host local, por exemplo)

WASSSLChannelPort
O número da porta usado pelo canal de transporte SSL (9443 é o padrão)

applicationName
O nome do cliente de teste

serviceName
O nome do serviço que você deseja chamar

Gerando um Cliente de Teste com Autenticação Ativada

Utilize esta tarefa para gerar um cliente de teste para um serviço com autenticação que esteja ativada.

Antes de Iniciar

- Criar um Serviço
- Configurar uma Ferramenta de Montagem Conforme Descrito em "Configurando uma Ferramenta de Montagem com o IBM InfoSphere Information Server" na página 8
- Desativar o Serviço Não Seguro conforme Descrito em "Desativando um Serviço Não Seguro Usando o IBM InfoSphere Information Server Console" na página 9
- Exportar o Serviço para Criar um Arquivo Enterprise Archive (EAR) do Serviço conforme descrito em "Exportando um Serviço Usando o Console do WebSphere Application Server" na página 9

- Importar o Arquivo EAR de Serviço em uma Ferramenta de Montagem se Você Deseja Usar a Ferramenta para Ativar os Recursos de Segurança Conforme Descrito em “Importando um Arquivo EAR do Serviço Não Seguro para uma Ferramenta de Montagem” na página 10
- Incluir Autenticação no Serviço Conforme Descrito em “Incluindo Mecanismos de Autenticação” na página 14
- Exportar o Arquivo EAR que Contém o Serviço Conforme Descrito em “Exportando um Arquivo EAR do Serviço Seguro de uma Ferramenta de Montagem” na página 29
- Reimplementar o Arquivo EAR de Serviço Conforme Descrito em “Reimplementando um Serviço Seguro com o Console do IBM WebSphere Application Server” na página 29
- Ativar o Serviço Protegido Conforme Descrito em “Ativando um Serviço Seguro Usando o IBM InfoSphere Information Server Console” na página 30

Sobre Esta Tarefa

O assistente de segurança do IBM Rational Application Developer é utilizado nesta tarefa para mostrar como ativar a autenticação do Token do Nome do Usuário do WS-Security no cliente de teste. Alternativamente, você pode utilizar o editor do descritor de implementação do Rational Application Developer para ativar a segurança no cliente.

Se você chamar um serviço que requer autenticação, mas não especificar um nome de usuário e senha, a seguinte exceção de segurança ou semelhante será retornada:

```
exceção: com.ibm.wsspi.wssecurity.SoapSecurityException: WSEC5509E:
Um token de segurança cujo tipo seja [http://docs.oasis-open.org/wss/2004/
01/oasis-200401-wss-username-token-profile-1.0#UsernameToken] é necessário.
```

Da mesma forma, se você chamar um serviço que requer autenticação do Token do Nome do Usuário, mas especificar um nome de usuário e senha inválido, a seguinte exceção ou semelhante será retornada:

```
exceção: com.ibm.wsspi.wssecurity.SoapSecurityException: WSEC6521E:
Falha de login. A exceção é: javax.security.auth.login.LoginException:
WSEC6690E: Falha ao verificar o nome de usuário [admin] e a senha no
UserRegsitry: UserRegistryProcessor.checkRegistry()=false
```

Procedimento

1. Na guia **Servidores** do IBM WebSphere Application Server, clique com o botão direito em qualquer lugar dentro da janela e clique em **Novo** > **Servidor**.
2. Na página **Definir um Novo Servidor** da janela Novo Servidor, insira um nome para o host do servidor, selecione **IBM** > **WebSphere v6.1 Server** ou **WebSphere v7.0 Server** como o tipo de servidor e ambiente de tempo de execução do servidor. Se você seguiu a tarefa para configurar o IBM Rational Application Developer com IBM InfoSphere Information Server, o ambiente de tempo de execução correto será **Information Server WAS v6.1** ou **Information Server WAS v7.0**.
3. Clique em **Avançar** e certifique-se de que as informações na página seguinte estejam corretas, incluindo o nome do perfil e as informações sobre autenticação.
4. Clique em **Avançar**.
5. Na página **Incluir e Remover Projetos**, selecione o arquivo EAR seguro no campo **Projetos Disponíveis** e clique em **Incluir >** para incluí-lo na lista de projetos configurados.

6. Clique em **Avançar** e, em seguida, em **Concluir**.
7. Na guia **Servidores**, selecione o servidor criado e clique no ícone **Iniciar o servidor**.
8. Selecione **Arquivo** > **Novo** > **Projeto** > **Projeto da Web Dinâmico**.
9. Na janela Novo Projeto da Web Dinâmico, insira um nome de projeto (MyAppClient, por exemplo), selecione **Information Server WAS v6.1** ou **Information Server WAS v7.0** como o tempo de execução de destino, selecione **Incluir Projeto em um EAR** e insira um nome de projeto archive corporativo (EAR) (MyAppClient.ear, por exemplo) para o arquivo EAR que conterá o código do cliente.
10. Clique em **Concluir**.
11. Selecione **Arquivo** > **Novo** > **Outro**.
12. Na janela **Novo**, expanda **Serviços da Web**, selecione **Cliente de Serviço da Web** e clique em **Avançar**.
13. Na página **Serviços da Web** da janela Cliente de Serviço da Web, insira a URL do Web Services Description Language (WSDL) (por exemplo, `http://localhost:9080/wisd/MyApp/MyService?wsdl`) no campo **Definição de Serviço**.
14. Selecione **Cliente de Teste** como o nível de automação.
15. No painel Configuração, verifique estas configurações:

    Servidor
    Websphere v6.1 Server ou Websphere v7.0 Server

    Tempo de Execução do Serviço da Web
    IBM WebSphere JAX-RPC

    Projeto do Cliente
    MyAppClient

    Projeto EAR do Cliente
    MyAppClient.ear
16. Clique em **Concluir**.
17. Na página **Teste do Cliente de Serviço da Web**, selecione o recurso de teste **JSPs de Amostra do Serviço da Web** e o método que deseja testar. Utilize as configurações padrão para o restante desta página e clique em **Concluir**.
18. No **Explorer do Projeto**, expanda **Serviços da Web JSR-109** > **Clientes**.
19. Clique com o botão direito do mouse no cliente de teste que você acabou de criar e selecione **Cliente de Serviço da Web Seguro** > **Incluir Token de Segurança Independente** (assumindo que a segurança que foi ativada no serviço é um token de segurança do nome de usuário para autenticação). Se o cliente de teste não estiver na pasta **Clientes**, reinicie o Rational Application Developer.
20. No Assistente do WS-Security, selecione o tipo de token **Token do Nome do Usuário** e o manipulador de retorno de chamada **com.ibm.wsspi.wssecurity.auth.callback.NonPromptCallbackHandler**. Você especificará as credenciais de login na próxima página do assistente.
21. Clique em **Avançar**.
22. Digite um ID do usuário e senha válidos para o serviço e clique em **Concluir**.
23. Salve as alterações e reinicie o cliente de teste.

24. Opcional: Para testar seu serviço utilizando o cliente de teste, na guia **Cliente de Teste de Serviços da Web** que é aberta, selecione um método, digite qualquer número de entrada e clique em **Chamar**. A área de janela **Resultado** exibe o resultado.
25. Opcional: Para chamar o cliente de teste sem usar a ferramenta de montagem, use um navegador da Web e insira a URL `https://`*`hostname`*`:`*`WASSSLChannelPort`*`/`*`applicationName`*`/sample`*`serviceName`*`PortTypeProxy/TestClient.jsp` no campo do endereço.

    hostname
    O nome do servidor hospedando seu cliente de teste (host local, por exemplo).

    WASSSLChannelPort
    O número da porta utilizada pelo canal de transporte SSL (9443 é o padrão).

    applicationName
    O nome do cliente de teste.

    serviceName
    O nome do serviço que você deseja chamar.

Gerando Keystores, Chaves e Certificados de Amostra

Qualquer tipo de criptografia, incluindo SSL, requer que você gere keystores nos lados do cliente e do servidor. Os keystores contêm chaves que assinam e criptografam mensagens. Utilize os keystores de amostra neste tópico para testar a criptografia ou execute o script utilizando o utilitário keytool Java para gerar os keystores de amostra você mesmo.

Nota: Para manter este exemplo simples, os keystores de amostra foram gerados utilizando certificados auto-assinados, em vez de certificados assinados por uma Autoridade de Certificação (CA).

Utilize esses keystores de amostra apenas para testes. Implemente sua própria infraestrutura da chave pública (PKI) em um ambiente de produção real.

É possível gerar keystores utilizando métodos diferentes. Os keystores de amostra neste tópico foram gerados utilizando o `keytool`, a ferramenta de linha de comandos Java e o seguinte script. Você também pode utilizar o iKeyman, a ferramenta de gerenciamento de chaves da IBM, que é uma ferramenta de interface gráfica com o usuário para gerenciamento de keystores e chaves. Instalado com IBM WebSphere Application Server em *`install-dir`*`/WebSphere/AppServer/bin/ikeyman.bat`.

Criptografia SSL

- Keystore do cliente (clientsslkeys.jceks):
  - Chave privada do cliente
- Truststore do cliente (clientssltrusts.jceks):
  - Certificado auto-assinado do servidor com apenas uma chave pública
- Keystore do servidor (serversslkeys.jceks):
  - Chave privada do servidor
- Truststore do servidor (serverssltrusts.jceks):
  - Certificado auto-assinado do cliente com apenas uma chave pública

Os keystores de amostra também possuem as seguintes características.

Tabela 1. Características do Keystore do Cliente `clientsslkeys.jceks`

Campo	**Valor**
Nome do Arquivo	`C:\sampleks\clientsslkeys.jceks`
Storepass	senha
Tipo de Armazenamento	JCEK
Nome Distinto	CN=wasclient, O=IBM, C=US
Keypass	senha
Alias	wasclient

Tabela 2. Características do Truststore do Cliente `clientssltrusts.jceks`

Campo	**Valor**
Nome do Arquivo	`C:\sampleks\clientssltrusts.jceks`
Storepass	senha
Tipo de Armazenamento	JCEK
Arquivo de Certificado	wasserver.cert

Tabela 3. Características do Keystore do Servidor `serversslkeys.jceks`

Campo	**Valor**
Nome do Arquivo	`C:\sampleks\serversslkeys.jceks`
Storepass	senha
Tipo de Armazenamento	JCEK
Nome Distinto	CN=wasserver, O=IBM, C=US
Keypass	senha
Alias	wasserver

Tabela 4. Características do Truststore do Servidor `serverssltrusts.jceks`

Campo	**Valor**
Nome do Arquivo	`C:\sampleks\serverssltrusts.jceks`
Storepass	senha
Tipo de Armazenamento	JCEK
Arquivo de Certificado	wasclient.cert

Criando o Keystore do cliente

Usando o `keytool` Java, você pode gerar o keystore do cliente com o seguinte script.

```
REM  Gerar o keystore do cliente e a chave privada
keytool -genkey -v -alias wasclient -keypass password -keystore
clientsslkeys.jceks -storepass password -storetype jceks -dname
"CN=wasclient, O=IBM, C=US" -keyalg "RSA"
REM  Gerar o certificado auto-assinado do cliente
keytool -export -v -alias wasclient -file wasclient.cert -rfc
-keystore
clientsslkeys.jceks -storepass password -storetype jceks
```

Criando o Keystore do servidor

Usando o `keytool` Java, você pode gerar o keystore do servidor com o seguinte script.

```
REM  Gerar o keystore do servidor e a chave privada
keytool -genkey -v -alias wasserver -keypass password -keystore
serversslkeys.jceks -storepass password -storetype jceks -dname
"CN=wasserver, O=IBM, C=US" -keyalg "RSA"
REM  Gerar o certificado auto-assinado do servidor
keytool -export -v -alias wasserver -file wasserver.cert -rfc
-keystore
serversslkeys.jceks -storepass password -storetype jceks
```

Criando o Truststore do cliente

Usando o `keytool` Java, você pode gerar o truststore do cliente com o seguinte script.

```
REM  Importar o certificado do servidor para o truststore do cliente
keytool -import -v -noprompt -alias wasserver -file wasserver.cert -
keystore clientssltrusts.jceks -storepass password -storetype jceks
```

Criando o Truststore do servidor

Usando o `keytool` Java, você pode gerar o truststore do servidor com o seguinte script.

```
REM  Importar o certificado cliente para o truststore do servidor
keytool -import -v -noprompt -alias wasclient -file wasclient.cert -
keystore serverssltrusts.jceks -storepass password -storetype jceks
```

Gerando um Cliente de Teste com SSL Ativado

Use esta tarefa para gerar um cliente de teste para um serviço que permita o sigilo de dados usando a criptografia Secure Sockets Layer (SSL).

Antes de Iniciar

- Criar um Serviço
- Configurar uma Ferramenta de Montagem Conforme Descrito em “Configurando uma Ferramenta de Montagem com o IBM InfoSphere Information Server” na página 8
- Desativar o Serviço Não Seguro conforme Descrito em “Desativando um Serviço Não Seguro Usando o IBM InfoSphere Information Server Console” na página 9
- Exportar o Serviço para Criar um Arquivo Enterprise Archive (EAR) do Serviço conforme descrito em “Exportando um Serviço Usando o Console do WebSphere Application Server” na página 9
- Importar o Arquivo EAR de Serviço em uma Ferramenta de Montagem se Você Deseja Usar a Ferramenta para Ativar os Recursos de Segurança Conforme Descrito em “Importando um Arquivo EAR do Serviço Não Seguro para uma Ferramenta de Montagem” na página 10
- Incluir Confidencialidade no Serviço Conforme Descrito em “Incluindo Sigilo de Dados Usando a Criptografia SSL” na página 24
- Exportar o Arquivo EAR que Contém o Serviço Conforme Descrito em “Exportando um Arquivo EAR do Serviço Seguro de uma Ferramenta de Montagem” na página 29
- Reimplementar o Arquivo EAR de Serviço Conforme Descrito em “Reimplementando um Serviço Seguro com o Console do IBM WebSphere Application Server” na página 29

- Ativar o Serviço Protegido Conforme Descrito em "Ativando um Serviço Seguro Usando o IBM InfoSphere Information Server Console" na página 30

Sobre Esta Tarefa

Em uma parte desta tarefa, você criará um novo repertório SSL Java Secure Socket Extension (JSSE) usando o IBM WebSphere Application Server. Para criar este novo repertório, você precisará utilizar os keystores de amostra do "Gerando Keystores, Chaves e Certificados de Amostra" na página 36.

Procedimento

1. Efetue login no console administrativo do IBM WebSphere Application Server.
2. Na área de janela de navegação, expanda **Segurança** e clique em **SSL**.
3. Na janela Repertórios de Configuração SSL, clique em **Novo Repertório JSSE**.
4. Na guia **Configuração**:
   a. Digite um nome de alias para o repertório. Por exemplo, `WASClientSSL`.
   b. Não selecione a caixa de opção **Autenticação de Cliente**. O repertório SSL atua como um cliente SSL e não como um servidor, portanto não há um cliente para autenticação.
   c. Para o nível de segurança, selecione **ALTO**.
   d. Opcional: Selecione cifras na lista **Conjuntos de Criptografia** se deseja substituir as cifras predefinidas que criptografam o SSL de acordo com o nível de segurança selecionado.
   e. Opcional: Selecione a caixa de opção **Token Criptográfico**.
   f. Opcional: Selecione um provedor JSSE predefinido ou customizado.
   g. Selecione o protocolo **SSL**.
   h. Digite o local, o nome e a senha para o arquivo de chaves e selecione um formato. Utilize o arquivo de chaves localizado no tópico de referência de keystores de amostra.
   i. Digite o local, o nome e a senha para o arquivo de confiança e selecione um formato. Utilize o arquivo de confiança localizado no tópico de referência de keystores de amostra.
   j. Clique em **OK**.
5. Salve as alterações e reinicie o IBM WebSphere Application Server.
6. Na guia **Servidores** do IBM Rational Application Developer, clique com o botão direito do mouse em qualquer lugar dentro da janela e selecione **Novo** > **Servidor**.
7. Na página **Definir um Novo Servidor** da janela Novo Servidor, insira um nome para o host do servidor, selecione **IBM** > **WebSphere v6.1 Server** ou **WebSphere v7.0 Server** como o tipo de servidor e ambiente de tempo de execução do servidor. Se você seguiu a tarefa para configurar o IBM Rational Application Developer com IBM InfoSphere Information Server, o ambiente de tempo de execução correto será **Information Server WAS v6.1** ou **Information Server WAS v7.0**.
8. Clique em **Avançar** e certifique-se de que as informações na página seguinte estejam corretas, incluindo o nome do perfil e as informações sobre autenticação.
9. Clique em **Avançar**.
10. Na página **Incluir e Remover Projetos**, selecione o arquivo EAR seguro no campo **Projetos Disponíveis** e clique em **Incluir >** para incluí-lo na lista de projetos configurados.

11. Clique em **Avançar** e, em seguida, em **Concluir**.
12. Na guia **Servidores**, selecione o servidor criado e clique no ícone **Iniciar o servidor**.
13. Selecione **Arquivo** > **Novo** > **Projeto** > **Projeto da Web Dinâmico**.
14. Na janela Novo Projeto da Web Dinâmico, insira um nome de projeto (MyAppClient, por exemplo), selecione **Information Server WAS v6.1** ou **Information Server WAS v7.0** como o tempo de execução de destino, selecione **Incluir Projeto em um EAR** e insira um nome de projeto archive corporativo (EAR) (MyAppClient.ear, por exemplo) para o arquivo EAR que conterá o código do cliente.
15. Clique em **Concluir**.
16. Selecione **Arquivo** > **Novo** > **Outro**.
17. Na janela **Novo**, expanda **Serviços da Web**, selecione **Cliente de Serviço da Web** e clique em **Avançar**.
18. Na página **Serviços da Web** da janela Cliente de Serviço da Web, insira a URL do Web Services Description Language (WSDL) (http://localhost:9080/wisd/MyApp/MyService?wsdl, por exemplo) no campo **Definição de Serviço**.
19. Selecione **Cliente de Teste** como o nível de automação.
20. No painel Configuração, verifique estas configurações:

    Servidor
    Websphere v6.1 Server ou Websphere v7.0 Server

    Tempo de Execução do Serviço da Web
    IBM WebSphere JAX-RPC

    Projeto do Cliente
    MyAppClient

    Projeto EAR do Cliente
    MyAppClient.ear
21. Clique em **Concluir**.
22. Na página **Teste do Cliente de Serviço da Web**, selecione o recurso de teste **JSPs de Amostra do Serviço da Web** e o método que deseja testar. Utilize as configurações padrão para o restante desta página e clique em **Concluir**.
23. No **Explorer do Projeto** do IBM Rational Application Developer, expanda **Serviços da Web JSR-109** > **Clientes** e dê um clique duplo no cliente de teste gerado para editar o descritor de implementação. Reinicie o Rational Application Developer se o cliente de teste não estiver na pasta.
24. Clique na guia **Ligação WS** na janela Descritor de Implementação da Web e expanda a seção **Detalhes da Ligação do Nome Completo da Porta**.
25. No campo **Configuração SSL HTTPNome**, digite o nome do repertório SSL do cliente. Por exemplo, *name2Node01/WASClientSSL*.
26. Salve as alterações e reinicie o cliente de teste.
27. Opcional: Para testar seu serviço utilizando o cliente de teste, na guia **Cliente de Teste de Serviços da Web** que é aberta, selecione um método, digite qualquer número de entrada e clique em **Chamar**. A área de janela **Resultado** exibe o resultado.
28. Opcional: Para chamar o cliente de teste sem usar a ferramenta de montagem, use um navegador da Web e insira a URL `https://`*`hostname`*`:`*`WASSSLChannelPort`*`/`*`applicationName`*`/sample`*`serviceName`*`PortTypeProxy/TestClient.jsp` no campo do endereço.

hostname
O nome do servidor hospedando seu cliente de teste (host local, por exemplo).

WASSSLChannelPort
O número da porta utilizada pelo canal de transporte SSL (9443 é o padrão).

applicationName
O nome do cliente de teste.

serviceName
O nome do serviço que você deseja chamar.

Exemplo

Evite esses erros ao ativar o SSL utilizando o IBM WebSphere Application Server:

- Se você chamar um serviço SSL seguro utilizando HTTP em vez de HTTPS, a seguinte exceção será retornada:

  ```
  exceção: WSWS3499W: Novo local redirecionado:
  http://localhost:9080/wisd/MyApp/MyService
  ```

- Se você chamar um serviço SSL seguro utilizando um cliente de teste não configurado para SSL, a seguinte exceção será retornada:

  ```
  exceção: WSWS3713E: A conexão com o host remoto
  localhost falhou. Recebido o seguinte erro:
  Negociação encerrada pelo mecanismo SSL: FECHADO
  ```

- Se você chamar um serviço SSL seguro utilizando um cliente de teste que não esteja configurado adequadamente para SSL (o truststore do cliente não está configurado adequadamente), a seguinte exceção será retornada:

  ```
  exceção: com.ibm.wsspi.channel.framework.exception
  ChannelException:com.ibm.wsspi.channel.framework.exception.
  ChannelException: Nome do arquivo de confiança nulo inválido
  ```

Rastreando Mensagens SOAP

Rastreia as mensagens SOAP trocadas entre o cliente e o servidor para solucionar problemas com um serviço. Utilize a ferramenta Monitor do TCP/IP no IBM Rational Application Developer para rastrear mensagens SOAP.

Antes de Iniciar

- Criar um Serviço
- Configurar uma Ferramenta de Montagem Conforme Descrito em “Configurando uma Ferramenta de Montagem com o IBM InfoSphere Information Server” na página 8
- Desativar o Serviço Não Seguro conforme Descrito em “Desativando um Serviço Não Seguro Usando o IBM InfoSphere Information Server Console” na página 9
- Exportar o Serviço para Criar um Arquivo Enterprise Archive (EAR) do Serviço conforme descrito em “Exportando um Serviço Usando o Console do WebSphere Application Server” na página 9
- Importar o Arquivo EAR de Serviço em uma Ferramenta de Montagem se Você Deseja Usar a Ferramenta para Ativar os Recursos de Segurança Conforme Descrito em “Importando um Arquivo EAR do Serviço Não Seguro para uma Ferramenta de Montagem” na página 10
- Proteger um Serviço Conforme Descrito em “Protegendo um Serviço” na página 11

- Exportar o Arquivo EAR que Contém o Serviço Conforme Descrito em "Exportando um Arquivo EAR do Serviço Seguro de uma Ferramenta de Montagem" na página 29
- Reimplementar o Arquivo EAR de Serviço Conforme Descrito em "Reimplementando um Serviço Seguro com o Console do IBM WebSphere Application Server" na página 29
- Ativar o Serviço Protegido Conforme Descrito em "Ativando um Serviço Seguro Usando o IBM InfoSphere Information Server Console" na página 30

Procedimento

1. Selecione **Janela** > **Mostrar Visualização** > **Outro**.
2. Na janela Mostrar Visualização, expanda **Depuração**, selecione **Monitor do TCP/IP** e clique em **OK**.
3. Clique com o botão direito do mouse na janela Monitor do TCP/IP e selecione **Propriedades**.
4. Clique em **Incluir** e digite ou selecione as seguintes informações na janela Novo Monitor:
   a. Digite um número de porta do monitoramento local não utilizado. Por exemplo, *13557*. O cliente enviará pedidos SOAP para esta porta.
   b. Digite o nome do computador host que está executando o servidor. Por exemplo, se o cliente e o servidor estiverem no mesmo computador, o nome do host será `localhost`.
   c. Digite o número da porta a ser monitorada, que é a porta pela qual o cliente enviaria pedidos se o monitoramento TCP/IP não estivesse ativado. Por exemplo, o número da porta padrão é `9080` para o IBM WebSphere Application Server.
   d. Selecione o tipo de monitoramento **HTTP** ou **TCP/IP**. **TCP/IP** mostra as mensagens HTTP completas, o que inclui os cabeçalhos HTTP e as mensagens SOAP. **HTTP** mostra apenas as mensagens SOAP.
   e. Clique em **OK**.
5. Na janela Preferências do Monitor do TCP/IP que é aberta, selecione o monitor e clique em **Iniciar** para começar o monitoramento.
6. No **Explorer do Projeto**, expanda **Serviços da Web JSR-109** > **Clientes**, clique com o botão direito do mouse no cliente de teste e selecione **Abrir**.
7. Selecione o método **getEndpoint()** e clique em **Chamar**. Copie a URL do terminal retornada.
8. Selecione o método **setEndpoint()**, cole a URL do terminal retornada anteriormente pelo método **getEndpoint()** e altere o número da porta para apontar para o número da porta do Monitor do TCP/IP. Clique em **Chamar**. Por exemplo, se o nome do host for host local e o número da porta local for 13557, o terminal será `http://localhost:13557/wisd/MyApp/MyService`.
9. Chame o serviço com o cliente de teste utilizando um dos seguintes métodos:
   - No **Cliente de Teste de Serviços da Web**, selecione um método definido no serviço, digite qualquer número de entrada e clique em **Chamar**.
   - Para chamar o cliente de teste sem usar a ferramenta de montagem, use um navegador da Web e insira a URL `https://`*`hostname`*`:`*`WASSSLChannelPort`*`/`*`applicationName`*`/sample`*`serviceName`*`PortTypeProxy/TestClient.jsp` no campo do endereço.

     hostname
     O nome do servidor hospedando seu cliente de teste (host local, por exemplo).

WASSSLChannelPort
O número da porta utilizada pelo canal de transporte SSL (9443 é o padrão).

applicationName
O nome do cliente de teste.

serviceName
O nome do serviço que você deseja chamar.

10. Depois de chamar o serviço, analise as mensagens HTTP e SOAP na janela Monitor do TCP/IP para solucionar os problemas ocorridos no serviço.

Comparação de Tecnologias de Segurança

Para escolher uma tecnologia de acordo com seus requisitos, você pode comparar as tecnologias de segurança utilizando dois parâmetros: grau de segurança oferecido e grau de dificuldade a ser configurado.

Geralmente, uma tecnologia é mais difícil para implementar quando é baseada em criptografia de chave pública, que requer a configuração de uma infraestrutura da chave pública (PKI). Esse é o caso de qualquer tipo de assinatura e criptografia digital. No entanto, essas tecnologias geralmente oferecem um nível melhor de segurança que outras tecnologias que possam exigir menos trabalho de infraestrutura.

Tabela 5. Métodos de Autenticação e Seus Níveis de Segurança

Método de autenticação	**Nível**	**Grau de segurança oferecido**	**Grau de dificuldade a ser configurado**	**Notas**
Autenticação básica HTTP	Transporte	baixo	baixo	O nome de usuário e a senha são enviados em texto claro (base64) na rede. Utilizado apenas em redes seguras (HTTPS ou intranet).
Autenticação de compilação HTTP (não suportada pelo IBM WebSphere Application Server)	Transporte	médio	médio	O nome de usuário e a senha são criptografados.
Token do nome do usuário	Mensagem	baixo	médio	O nome de usuário e a senha são enviados em texto claro na rede. Utilizado apenas em redes seguras (HTTPS, intranet ou Criptografia XML).

Tabela 5. Métodos de Autenticação e Seus Níveis de Segurança (continuação)

Método de autenticação	Nível	Grau de segurança oferecido	Grau de dificuldade a ser configurado	Notas
Token do certificado X.509	Mensagem	alto	médio	Requer uma PKI.
Token de bilhete Kerberos	Mensagem	alto	alto	Requer uma infraestrutura Kerberos.

Tabela 6. Método de Autorização e seu Nível de Segurança

Método de autorização	Nível	Grau de segurança oferecido	Grau de dificuldade a ser configurado	Notas
Restrições de segurança declarativa J2EE	Aplicativo	médio	médio	Não requer infraestrutura de segurança.

As restrições de segurança declarativa J2EE são fáceis de configurar (apenas exigem alterações nos descritores de implementação J2EE) e, ao mesmo tempo, oferecem um bom nível de controle de acesso. Geralmente, são o ponto inicial para serviços de segurança.

Tabela 7. Método de Sigilo e seu Nível de Segurança

Método de sigilo	Nível	Grau de segurança oferecido	Grau de dificuldade a ser configurado	Notas
SSL	Transporte	médio	médio	Requer uma PKI. O sigilo é fornecido de ponto de rede para ponto de rede.

O SSL e o Transport Layer Security (TLS) oferecem recursos de segurança adicionais em relação à criptografia, incluindo autenticação, proteção de dados e suporte para token criptográfico para conexões HTTP seguras.

A criptografia é uma operação intensiva de cálculos que pode afetar o desempenho. Também aumenta a sobrecarga de gerenciamento e de administração. Portanto, deve ser utilizada com a devida consideração de sua aplicabilidade.

Tabela 8. Método de Integridade Digital e Seu Nível de Segurança

Método de integridade de dados	Nível	Grau de segurança oferecido	Grau de dificuldade a ser configurado	Notas
Assinatura Digital XML	Mensagem	alto	médio	Requer uma PKI

A assinatura digital é uma operação intensiva de cálculos que pode gerar penalidades do desempenho. Também aumenta a sobrecarga de gerenciamento e de administração. Portanto, deve ser utilizada com a devida consideração de sua aplicabilidade.

Tecnologias e Ligações de Segurança

Nem todas as tecnologias de segurança estão disponíveis para todas as ligações.

Para algumas ligações, apenas um subconjunto da lista completa de tecnologias de segurança pode estar disponível (ou aplicável). Por exemplo, nenhuma das tecnologias de segurança dos serviços da Web é aplicável para a ligação EJB. A tabela a seguir resume as tecnologias de segurança disponíveis por ligação.

Tabela 9. Tecnologias e Ligações de Segurança

	Tecnologia de Segurança	**EJB**	**SOAP sobre HTTP**	**SOAP sobre JMS**	**Texto sobre JMS**
Autenticação	JAAS/EJB	Disponíveis			
Autenticação	Básico HTTP		Disponíveis		
Autenticação	Compilação HTTP		Não suportada pelo IBM WebSphere Application Server 6.0 e posteriores		
Autenticação	Token do nome de usuário de segurança dos serviços da Web		Disponíveis	Disponíveis	
Autenticação	Outra segurança dos serviços da Web (Kerberos, X509, LTPA, SAML)		Disponíveis	Disponíveis	
Autorização	J2EE	Disponíveis	Disponíveis	Disponíveis	Disponíveis
Sigilo dos Dados	HTTPS e SSL	Disponíveis	Disponíveis	Disponíveis	Disponíveis

Acessibilidade do Produto

É possível obter informações sobre o status de acessibilidade dos produtos IBM.

Os módulos do produto e as interfaces com o usuário do IBM InfoSphere Information Server não são totalmente acessíveis. O programa de instalação instala os seguintes módulos e componentes do produto:

- IBM InfoSphere Business Glossary
- IBM InfoSphere Business Glossary Anywhere
- IBM InfoSphere DataStage
- IBM InfoSphere FastTrack
- IBM InfoSphere Information Analyzer
- IBM InfoSphere Information Services Director
- IBM InfoSphere Metadata Workbench
- IBM InfoSphere QualityStage

Para obter informações sobre o status de acessibilidade de produtos IBM, consulte as informações de acessibilidade de produtos IBM, em http://www.ibm.com/able/product_accessibility/index.html.

Documentação Acessível

A documentação acessível para produtos InfoSphere Information Server é fornecida em um centro de informações. O Centro de Informações apresenta a documentação no formato XHTML 1.0, o qual é visível na maioria dos navegadores da Web. O XHTML permite que as preferências de exibição no navegador sejam configuradas. Ele também permite que leitores de tela e outras tecnologias assistidas sejam utilizadas para acessar a documentação.

IBM e Acessibilidade

Consulte o IBM Human Ability and Accessibility Center para obter informações adicionais sobre o compromisso que a IBM possui com relação à acessibilidade.

Acessando a Documentação do Produto

A documentação é fornecida em uma variedade de locais e formatos, incluindo a ajuda que é aberta diretamente das interfaces do cliente do produto, em um centro de informações que abrange o conjunto e nos manuais de arquivo PDF.

O centro de informações é instalado como um serviço comum com o IBM InfoSphere Information Server. O centro de informações contém ajuda para a maioria das interfaces do produto, bem como a documentação completa para todos os módulos do produto no conjunto. É possível abrir o centro de informações a partir do produto instalado ou de um navegador da Web.

Acessando o centro de informações

Você pode usar os seguintes métodos para abrir o centro de informações instalado.

- Clique no link **Ajuda** na parte superior direita da interface do cliente.

  Nota: No IBM InfoSphere FastTrack e no IBM InfoSphere Information Server Manager, o item de Ajuda principal abre um sistema de ajuda local. Escolha **Ajuda > Abrir Info Center** para abrir o centro de informações de conjunto completo.
- Pressione a tecla F1. A tecla F1 geralmente é aberta no tópico que descreve o contexto atual da interface do cliente.

  Nota: A tecla F1 não funciona em clientes da Web.
- Use um navegador da Web para acessar o centro de informações instalado, mesmo quando não estiver conectado ao produto. Insira o seguinte endereço em um navegador da Web: http://host_name:port_number/infocenter/topic/com.ibm.swg.im.iis.productization.iisinfsv.home.doc/ic-homepage.html. O host_name é o nome do computador da camada de serviços no qual o centro de informações está instalado e port_number é o número da porta para o InfoSphere Information Server. O número de porta padrão é 9080. Por exemplo, em um computador Microsoft® Windows® Server denominado iisdocs2, o endereço da Web está no seguinte formato: http://iisdocs2:9080/infocenter/topic/com.ibm.swg.im.iis.productization.iisinfsv.nav.doc/dochome/iisinfsrv_home.html.

Um subconjunto do centro de informações, atualizado periodicamente, está disponível no Web site da IBM no endereço http://publib.boulder.ibm.com/infocenter/iisinfsv/v8r7/index.jsp.

Obtendo a Documentação em PDF e em Cópia Impressa

- Um subconjunto dos manuais em formato PDF está disponível através do instalador do software e mídia de distribuição do InfoSphere Information Server. Os outros manuais em formato PDF estão disponíveis on-line e podem ser acessados a partir do seguinte documento de suporte: https://www.ibm.com/support/docview.wss?uid=swg27008803&wv=1.
- Você também pode solicitar publicações do IBM no formato de cópia impressa on-line ou por meio do representante IBM local. Para solicitar publicações on-line, acesse o Centro de Publicações da IBM em http://www.ibm.com/e-business/linkweb/publications/servlet/pbi.wss.

Fornecendo feedback sobre a documentação

É possível enviar seus comentários sobre a documentação das seguintes maneiras:

- Formulário de comentários do leitor on-line: www.ibm.com/software/data/rcf/
- E-mail: comments@us.ibm.com

Links para Web Sites Não IBM

Este centro de informações pode fornecer links ou referências a recursos e Web sites não IBM.

A IBM não faz representações, não oferece garantias ou outros comprometimentos quanto a quaisquer Web sites não IBM ou recursos de terceiros (incluindo qualquer Web site da Lenovo) que possam ser referidos, acessados ou vinculados a qualquer site da IBM. Um link para um Web site não IBM não significa que a IBM endossa o conteúdo ou o uso de tal Web site ou de seu proprietário. Além disso, a IBM não faz parte de, e nem é responsável por, quaisquer transações entre o cliente e terceiros, mesmo que ele tome conhecimento dessas partes (ou utilize um link para tais partes) de um site IBM. Portanto, você reconhece e concorda que a IBM não é responsável pela disponibilidade desses sites ou recursos externos, e não é responsável por qualquer conteúdo, serviços, produtos ou outros materiais disponíveis nesses sites ou recursos.

Quando o cliente acessa um Web site não IBM, mesmo um que possa conter o logotipo IBM, entenda que ele é independente da IBM e que a IBM não controla o conteúdo nesse Web site. É responsabilidade do cliente tomar precauções para se proteger contra vírus, worms, Cavalos de Troia e outros programas potencialmente destrutíveis, e proteger suas informações da maneira que julgar apropriada.

Avisos e Marcas Registradas

Essas informações foram desenvolvidas para produtos e serviços oferecidos nos Estados Unidos.

Avisos

A IBM pode não oferecer, em outros países, os produtos, serviços ou recursos discutidos nesta publicação. Consulte seu representante IBM local para obter informações sobre os produtos e serviços disponíveis atualmente em sua área. Qualquer referência a um produto, programa ou serviço IBM não tem o propósito de declarar ou implicar que apenas esse produto, programa ou serviço possa ser utilizado. Qualquer produto, programa ou serviço funcionalmente equivalente que não infrinja qualquer direito de propriedade intelectual da IBM poderá ser utilizado no lugar. Entretanto, é de responsabilidade do usuário avaliar e verificar a operação de qualquer produto, programa ou serviço não-IBM.

A IBM pode possuir patentes ou solicitações de patentes pendentes relativas a assuntos tratados nesta publicação. O fornecimento desta publicação não garante ao Cliente nenhum direito sobre tais patentes. Pedidos de licença devem ser enviados, por escrito, para:

Gerência de Relações Comerciais e Industriais da IBM Brasil
Av. Pasteur, 138-146
Botafogo
Rio de Janeiro, RJ
CEP: 22290-240

Para pedidos de licenças com relação a informações sobre DBCS (Conjunto de Caracteres de Byte Duplo), entre em contato com o Departamento de Propriedade Intelectual da IBM em seu país ou envie pedidos, por escrito, para:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

O parágrafo a seguir não se aplica ao Reino Unido ou qualquer outro país em que tais disposições não estejam de acordo com a legislação local: A INTERNATIONAL BUSINESS MACHINES CORPORATION FORNECE ESTA PUBLICAÇÃO "NO ESTADO EM QUE SE ENCONTRA", SEM GARANTIA DE NENHUM TIPO, SEJA EXPRESSA OU IMPLÍCITA, INCLUINDO, MAS A ELAS NÃO SE LIMITANDO, AS GARANTIAS IMPLÍCITAS DE NÃO-INFRAÇÃO, COMERCIALIZAÇÃO OU ADEQUAÇÃO A UM DETERMINADO PROPÓSITO. Alguns países não permitem a exclusão de garantias expressas ou implícitas em certas transações; portanto, esta disposição pode não se aplicar ao Cliente.

Estas informações podem conter imprecisões técnicas ou erros tipográficos. Periodicamente são feitas alterações nas informações aqui contidas; tais alterações serão incorporadas em futuras edições desta publicação. A IBM pode, a qualquer momento, aperfeiçoar e/ou alterar os produtos e/ou programas descritos nesta publicação, sem aviso prévio.

Referências nestas informações a Web sites que não sejam da IBM são fornecidas apenas por conveniência e não representam de forma alguma um endosso a estes Web sites. Os materiais contidos nesses Web sites não fazem parte dos materiais desse produto IBM e a utilização desses Web sites é de inteira responsabilidade do Cliente.

A IBM pode utilizar ou distribuir quaisquer informações fornecidas da forma que julgar apropriada sem incorrer em qualquer obrigação para com o Cliente.

Licenciados deste programa que desejam obter informações sobre este assunto com objetivo de permitir: (i) a troca de informações entre programas criados independentemente e outros programas (incluindo este) e (ii) a utilização mútua das informações trocadas, devem entrar em contato com:

Av. Pasteur, 138-146
Botafogo
Rio de Janeiro, RJ
CEP: 22290-240

Tais informações podem estar disponíveis, sujeitas a termos e condições apropriadas, incluindo em alguns casos, o pagamento de um imposto.

O programa licenciado descrito neste documento e todos os materiais licenciados disponíveis para ele são fornecidos pela IBM sob os termos do Contrato com o Cliente IBM, Contrato de Licença Internacional de Programas IBM ou qualquer contrato equivalente entre a IBM e o Cliente.

Os dados de desempenho aqui contidos foram determinados em um ambiente controlado. Portanto, os resultados obtidos em outros ambientes operacionais podem variar significativamente. Algumas medidas podem ter sido tomadas em sistemas em nível de desenvolvimento e não há garantia de que estas medidas serão as mesmas em sistemas disponíveis em geral. Além disso, algumas medidas podem ter sido estimadas por meio de extrapolação. Os resultados reais podem variar. Os usuários deste documento devem verificar os dados aplicáveis para seu ambiente específico.

As informações relativas a produtos não-IBM foram obtidas dos fornecedores dos respectivos produtos, de seus anúncios publicados ou de outras fontes publicamente disponíveis. A IBM não testou estes produtos e não pode confirmar a precisão do desempenho, da compatibilidade ou de qualquer outra reivindicação relacionada a produtos não-IBM. Perguntas sobre a capacidade de produtos não-IBM devem ser endereçadas aos fornecedores dos respectivos produtos.

Todas as declarações em relação à estratégia ou intenção futuras da IBM estão sujeitas a alteração ou suspensão sem aviso prévio e representam somente metas e objetivos.

Estas informações são destinadas apenas para finalidades de planejamento. As informações nessa publicação estão sujeitas a alterações antes que os produtos descritos se tornem disponíveis.

Essas informações contêm exemplos de dados e relatórios utilizados em operações diárias de negócios. Para ilustrá-las da maneira mais completa possível, os exemplos incluem os nomes de indivíduos, empresas, marcas e produtos. Todos

esses nomes são fictícios e qualquer semelhança com os nomes e endereços utilizados por uma empresa real é mera coincidência.

LICENÇA DE COPYRIGHT:

Essas informações contêm programas aplicativos de amostra no idioma de origem, que ilustram técnicas de programação em diversas plataformas operacionais. O Cliente poderá copiar, modificar e distribuir esses programas de amostra em qualquer forma sem pagamento a IBM, por propósitos de desenvolvimento, utilização, marketing ou distribuição dos programas de aplicativos em conformidade com a interface de programação de aplicativos para a plataforma operacional para a qual os programas de amostra são escritos. Esses exemplos não foram totalmente testados sob todas as condições. A IBM, portanto, não garante ou expressa confiabilidade, capacidade de manutenção ou funcionamento desses programas. Os programas de amostra são fornecidos "NO ESTADO EM QUE SE ENCONTRAM", sem garantia de nenhum tipo. A IBM não deve ser responsabilizada por nenhum dano decorrente do uso dos programas de amostra.

Cada cópia ou parte desses programas de amostra ou qualquer trabalho derivado deve incluir um aviso de copyright com os dizeres:

© (o nome da sua empresa) (ano). Partes deste código são derivados do IBM Corp. Sample Programs. © Copyright IBM Corp. _digite o ano ou os anos_. Todos os Direitos Reservados.

Se estas informações estiverem sendo exibidas em cópia eletrônica, as fotografias e ilustrações coloridas podem não aparecer.

Marcas Registradas

IBM, o logotipo IBM e ibm.com são marcas registrads da International Business Machines Corp., registradas em várias jurisdições, no mundo inteiro. Outros nomes de produtos e serviços podem ser marcas registradas da IBM ou de outras empresas. Uma lista atual de marcas registradas IBM está disponível na Web, em www.ibm.com/legal/copytrade.shtml.

Os termos a seguir são marcas ou marcas registradas de outras empresas:

Adobe é uma marca registrada da Adobe Systems Incorporated nos Estados Unidos e/ou em outros países.

IT Infrastructure Library é uma marca registrada da Central Computer and Telecommunications Agency, a qual está agora vinculada ao Office of Government Commerce.

Intel, o logotipo Intel, Intel Inside, o logotipo Intel Inside, Intel Centrino, o logotipo Intel Centrino, Celeron, Intel Xeon, Intel SpeedStep, Itanium e Pentium são marcas ou marcas registradas da Intel Corporation ou suas subsidiárias nos Estados Unidos e/ou em outros países.

Linux é uma marca registrada da Linus Torvalds nos Estados Unidos e/ou em outros países.

Microsoft, Windows, Windows NT e o logotipo Windows são marcas registradas da Microsoft Corporation nos Estados Unidos e/ou em outros países.

ITIL é uma marca registrada e uma marca registrada da comunidade do Departamento de Comércio do Governo e está registrada no U.S. Patent and Trademark Office

UNIX é uma marca registrada do The Open Group nos Estados Unidos e em outros países.

Cell Broadband Engine é uma marca registrada da Sony Computer Entertainment, Inc. nos Estados Unidos e/ou em outros países e é utilizada sob licença a partir deste ponto.

Java e todas as marcas registradas e logotipos baseados em Java são marcas ou marcas registradas da Oracle e/ou afiliadas.

O United States Postal Service possui as seguintes marcas registradas: CASS, CASS Certified, DPV, LACS^{Link}, ZIP, ZIP + 4, ZIP Code, Post Office, Postal Service, USPS e United States Postal Service. IBM Corporation é um licenciado não exclusivo da DPV e LACS^{Link} do United States Postal Service.

Outros nomes de empresas, produtos ou serviços podem ser marcas registradas ou marcas de serviço de terceiros.

Entrando em Contato com a IBM

É possível entrar em contato com a IBM para obter suporte ao cliente, serviços de suporte a software, informações de produtos e informações gerais. Também é possível fornecer feedback à IBM sobre os produtos e a documentação.

A tabela a seguir lista os recursos para suporte ao cliente, serviços de software, treinamento e informações sobre produtos e soluções.

Tabela 10. Recursos IBM

Recurso	Descrição e local
Portal de Suporte IBM	Você pode customizar as informações de suporte escolhendo os produtos e os tópicos que interessam a você em www.ibm.com/support/entry/portal/Software/Information_Management/InfoSphere_Information_Server
Serviços de Software	É possível localizar as informações sobre o software, TI e serviços de consultoria de negócios, no site de soluções em www.ibm.com/businesssolutions/
Minha IBM	Você pode gerenciar links para Web sites IBM e informações que atendam às suas necessidades específicas de suporte técnico criando uma conta no site Minha IBM em www.ibm.com/account/
Treinamento e Certificação	É possível aprender sobre os serviços de educação e treinamento técnico projetados para pessoas, empresas e organizações públicas para adquirir, manter e otimizar suas habilidades de TI em http://www.ibm.com/software/sw-training/
Representantes IBM	É possível entrar em contato com um representante IBM para aprender sobre as soluções em www.ibm.com/connect/ibm/us/en/

Fornecendo feedback

A tabela a seguir descreve como fornecer feedback para a IBM sobre produtos e documentação de produtos.

Tabela 11. Fornecendo Feedback à IBM

Tipo de Feedback	Ação
Feedback do Produto	É possível fornecer feedback geral do produto através da Pesquisa de Consumabilidade em www.ibm.com/software/data/info/consumability-survey

Tabela 11. Fornecendo Feedback à IBM (continuação)

Tipo de Feedback	Ação
Feedback da Documentação	Para comentar sobre o centro de informações, clique no link Feedback na parte superior direita de qualquer tópico no centro de informações. Também é possível enviar comentários sobre os manuais de arquivo PDF, o centro de informações ou qualquer outra documentação das seguintes maneiras: • Formulário de comentários do leitor on-line: www.ibm.com/software/data/rcf/ • E-mail: comments@us.ibm.com

Índice Remissivo

K

L

M

P

R

S

T

V

W

Impresso no Brasil

S517-0025-00