IBM WebSphere Commerce

Manual de Segurança

Versão 54

IBM WebSphere Commerce

Manual de Segurança

Versão 54

Nota:
Antes de utilizar estas informações e o produto suportado por elas, leia as informações gerais nos “Avisos” na página 113.

Primeira Edição, Primeira Revisão (Maio de 2002).

Esta edição aplica-se à versão 5.4 do IBM WebSphere Commerce e a todos os releases e modificações subseqüentes até que seja indicado de outra forma em novas edições. Certifique-se de utilizar a edição correta para o nível do produto.

Solicite publicações através de um representante IBM ou filial IBM que atenda sua localidade. As publicações não são armazenadas no endereço fornecido a seguir.

A IBM agradece seus comentários. Você pode enviar seus comentários pelos seguintes métodos:

1. Eletronicamente, para um dos IDs de rede listados abaixo. Certifique-se de incluir seu endereço de rede completo se deseja receber resposta.

   ```
   Internet: torrcf@ca.ibm.com
   IBMLink: toribm(torrcf)
   ```

2. Por FAX, utilize os seguintes números:

   ```
   Estados Unidos e Canadá:  416-448-6161
   Outros países: (+1)-416-448-6161
   ```

3. Por correio para o seguinte endereço:

   Centro Industrial IBM Brasil
   Centro de Traduções
   Caixa Postal 71
   Campinas, SP - Brasil
   CEP: 13001-970

Quando o Cliente envia seus comentários à IBM, concede direitos não-exclusivos à IBM para usá-los ou distribuí-los da maneira que julgar conveniente sem que isso implique em qualquer compromisso ou obrigação para com o Cliente.

Índice

Prefácio

Este documento descreve os recursos de segurança do WebSphere Commerce 5.4 e como configurá-los.

Ele detalha questões e recursos de segurança do WebSphere Commerce como autenticação, autorização e políticas de controle de acesso. O objetivo deste documento é fornecer às pessoas responsáveis pela segurança em seu site (que, provavelmente, inclui um administrador do sistema ou um administrador do site do WebSphere Commerce) um documento abrangente com a possibilidade de proteger de forma confiável um site de produção do WebSphere Commerce.

O público-alvo para este documento é o responsável pela segurança ou o administrador de segurança para um site do WebSphere Commerce.

Note que muitas seções deste Manual vieram de outros documentos na biblioteca de informações do WebSphere Commerce 5.4 como a ajuda online do WebSphere Commerce 5.4, do *WebSphere Commerce 5.4 - Manual de Instalação* e do *WebSphere Commerce 5.4 - Manual do Programador*. Especificamente:

- As informações no Capítulo 3, "Autorização (Controle de Acesso)" na página 13 também estão documentadas no *WebSphere Commerce 5.4 - Manual de Controle de Acesso*.
- As informações no Capítulo 4, "Aprimorando a Segurança do Site" na página 39 e no Capítulo 6, "Gerenciamento de Sessões" na página 63 também estão documentadas na ajuda online do WebSphere Commerce 5.4. As informações emCapítulo 5, "Ativando a Segurança do WebSphere Application Server" na página 55 também estão documentadas no *WebSphere Commerce 5.4 - Manual de Instalação*.
- As informações em Parte 3, "Tarefas de Segurança do Administrador do Site" na página 69 também estão documentadas no *WebSphere Commerce 5.4 - Manual de Instalação*.
- As informações no Parte 4, "Tarefas de Segurança do Desenvolvedor do WebSphere Commerce" na página 87 também estão documentadas no *WebSphere Commerce 5.4 - Manual do Programador*.

Importante

Este documento abrange somente questões de segurança do WebSphere Commerce relacionadas à implementação de um site de e-commerce. As questões relacionadas ao sistema operacional não são abrangidas. Você deve consultar o fornecedor do sistema operacional para determinar as medidas adequadas que devem ser tomadas para proteger o sistema operacional.

Navegando por este Documento

Este documento está dividido nas seguintes partes:

- A Parte 1, "Modelo de Segurança do WebSphere Commerce" na página 1 discute o modelo de segurança do WebSphere Commerce e fornece uma visão geral conceitual da segurança do WebSphere Commerce. Ela será de interesse daqueles que desejam uma visão geral da segurança do WebSphere Commerce para planejar a segurança em um site do WebSphere Commerce.

- A Parte 2, “Tarefas de Segurança do Administrador do Site do WebSphere Commerce” na página 37 discute tarefas de administração do site do WebSphere Commerce relacionadas à segurança do site. Ela será de interesse daqueles que executam tarefas de administração de site relacionadas à segurança do site.
- A Parte 3, “Tarefas de Segurança do Administrador do Site” na página 69 discute tarefas de administração do sistema WebSphere Commerce relacionadas à segurança do sistema. Ela será de interesse daqueles que executam tarefas de administração do sistema e que estão relacionadas à segurança do sistema.
- A Parte 4, “Tarefas de Segurança do Desenvolvedor do WebSphere Commerce” na página 87 discute o controle de acesso do WebSphere Commerce do ponto de vista de um desenvolvedor. Esta parte será de interesse daqueles que desejam entender de conceitos de controle na implementação de políticas de controle de acesso em seu código.

Avaliação da Segurança Contínua

As linhas de produto do WebSphere Commerce são continuamente submetidas a análises de segurança de um grupo independente de Peritos em Segurança da IBM. Esses peritos executam análises de segurança do ponto de vista de um usuário que apenas têm acesso ao WebSphere Commerce através de um navegador aos usuários mais privilegiados que têm uma conta no mesmo sistema que o servidor WebSphere Commerce está executando. O feedback da análise dos peritos em segurança é utilizado para melhorar continuamente a segurança do WebSphere Commerce.

Melhorias de Segurança no WebSphere Commerce 5.4

A seguinte seção lista os aprimoramentos de segurança no WebSphere Commerce 5.4 relacionados ao WebSphere Commerce Suite 5.1. A maioria desses aprimoramentos foram feitas no release WebSphere Commerce Business Edition 5.1.Eles são geralmente aplicáveis ao:

- Administrador do site do WebSphere Commerce;
- Administrador do sistema;
- Desenvolvedor do WebSphere Commerce.

Observe que às vezes essas funções são alternadas.

Aprimoramentos para o Administrador do Site

A seguir são apresentados aprimoramentos de segurança do WebSphere Commerce 5.4 que geralmente são direcionados a um administrador do site:

Controle de acesso

- **Estrutura de controle de acesso** — Um aprimoramento importante é uma nova estrutura de controle de acesso que foi implementada no WebSphere Commerce 5.4. Essa nova estrutura utiliza as políticas de controle de acesso para determinar se um determinado usuário pode executar uma ação específica em um recurso determinado. A nova estrutura de controle de acesso fornece controle de acesso minucioso. Ela funciona em conjunto, mas não substitui o controle de acesso fornecido pelo WebSphere Application Server. A nova estrutura de controle de acesso está descrita em detalhes no Capítulo 11, “Controle de Acesso” na página 89.

  A nova estrutura de controle de acesso aprimora o controle de acesso anterior das seguintes maneiras:

Ela é expressiva...
Ela captura o propósito de uma grande variedade de políticas de acesso. A estrutura é genérica, portanto pode controlar uma gama de grupos de usuários, grupos de recursos, grupos de ações e grupos de relacionamentos.

Ela é hierárquica...
As políticas de controle de acesso pertencentes a uma organização também são aplicadas em suborganizações.

Ela é personalizável...
As políticas de controle de acesso são externas e não estão no código de aplicativo, portanto as alterações nas políticas podem ser feitas sem o código de recompilação.

Ela é compacta...
A nova estrutura é bem dimensionada. O número de políticas de controle de acesso aumenta com o número de processos de negócios e não com o número de objetos. A maioria das estruturas de agrupamento baseia-se em condições implícitas, então, contanto que as condições sejam satisfeitas, a política será aplicada.

- **Script entre sites** — Rejeite qualquer pedido de usuário que contenha atributos ou caracteres designados como não permitidos, utilizando o nó Proteção de Script Entre Sites do Gerenciador de Configuração do WebSphere Commerce. Está descrito em detalhes no Capítulo 4, "Aprimorando a Segurança do Site" na página 39.

Autenticação

- **Armazenamento de senha** — O WebSphere Commerce 5.4 criptografa e armazena um hash de senhas de uma via utilizando o esquema de hash SHA-1 no banco de dados do WebSphere Commerce, em vez de armazenar as próprias senhas. Isso assegura que as senhas do usuário não sejam decifradas por outra pessoa, incluindo o administrador do site ou do sistema.
- **Invalidação de Senha** — Solicite aos usuários que alterem suas senhas quando estiverem efetuando login no sistema pela primeira vez, utilizando o nó Invalidação de Senha do Gerenciador de Configuração do WebSphere Commerce. Está descrito em detalhes no Capítulo 4, "Aprimorando a Segurança do Site" na página 39.
- **Política de contas** — Configure uma política de contas para o site para definir as políticas relacionadas às contas em uso, utilizando a página Política de contas do WebSphere Commerce Administration Console. Está descrito em detalhes no Capítulo 4, "Aprimorando a Segurança do Site" na página 39.
- **Política de senhas** — Configure uma política de senha para o site para controlar as características de seleção de senha de um usuário utilizando a página Política de senhas do WebSphere Commerce Administration Console. Está descrito em detalhes no Capítulo 4, "Aprimorando a Segurança do Site" na página 39.
- **Política de bloqueio de contas** — Configure uma política de bloqueio de contas para o site para reduzir as chances de uma conta de usuário ficar comprometida utilizando a página Política de bloqueio de contas do WebSphere Commerce Administration Console. Está descrito em detalhes no Capítulo 4, "Aprimorando a Segurança do Site" na página 39.

Autorização

Comandos protegidos por senha — Solicite aos usuários que digitem suas senhas se estiverem executando pedidos que executam comandos designados, utilizando o nó Comandos Protegidos por Senha do Gerenciador de Configuração do WebSphere Commerce. Está descrito em detalhes no Capítulo 4, “Aprimorando a Segurança do Site” na página 39.

Dados criptografados

Ferramenta de atualização de banco de dados — Atualize dados criptografados, como senhas e informações do cartão de crédito bem como chave do comerciante em um banco de dados do WebSphere Commerce, utilizando o nó Ferramenta de Atualização de Banco de Dados do Gerenciador de Configuração do WebSphere Commerce. Está descrito em detalhes no Capítulo 4, “Aprimorando a Segurança do Site” na página 39.

Gerenciamento de sessões

Tempo limite de login — Efetue logoff para um usuário que está inativo por um período de tempo estendido e peça que ele efetue logon novamente no sistema, utilizando o nó Tempo Limite de Login. Esse aprimoramento é chamado através do Gerenciador de Configuração do WebSphere Commerce e está descrito em detalhes no Capítulo 4, “Aprimorando a Segurança do Site” na página 39.

Log de acesso

Log de acesso — identifica rapidamente qualquer ameaça de segurança contra o WebSphere Commerce ativando o log de acesso. Esse aprimoramento é chamado através do Gerenciador de Configuração do WebSphere Commerce e está descrito em detalhes no Capítulo 4, “Aprimorando a Segurança do Site” na página 39.

Aprimoramentos para o Administrador do Sistema

A seguir são apresentados aprimoramentos de segurança do WebSphere Commerce 5.4 que geralmente são direcionados a um administrador do site:

- Um aprimoramento de segurança importante é a habilidade de configurar as ferramentas administrativas do WebSphere Commerce para executar um número de porta não padrão (por exemplo, a porta 8000 como oposta à porta 443). Ao restringir o acesso a essa porta, você poderá limitar o acesso às ferramentas de administração para sua rede local ou intranet.
- A partir do WebSphere Commerce Administration Console, lance um programa de segurança que verifica e exclui arquivos temporários doWebSphere Commerce que podem conter exposições de segurança potenciais, utilizando a página Lançar verificação de segurança.

Aprimoramentos para o Programador do WebSphere Commerce

Um aprimoramento importante é uma nova estrutura de controle de acesso que foi implementada no WebSphere Commerce 5.4. Essa nova estrutura utiliza as políticas de controle de acesso para determinar se um determinado usuário pode executar uma ação específica em um recurso determinado. A nova estrutura de controle de acesso fornece controle de acesso minucioso. Ela funciona em conjunto, mas não substitui o controle de acesso fornecido pelo WebSphere Application Server. A nova estrutura de controle de acesso está descrita em detalhes no Capítulo 11, “Controle de Acesso” na página 89.

A nova estrutura de controle de acesso aprimora o controle de acesso anterior das seguintes maneiras:

Ela é expressiva...

Ela captura o propósito de uma grande variedade de políticas de acesso. A estrutura é genérica, portanto pode controlar uma gama de grupos de usuários, grupos de recursos, grupos de ações e grupos de relacionamentos.

Ela é hierárquica...

As políticas de controle de acesso pertencentes a uma organização também são aplicadas em suborganizações.

Ela é personalizável...

As políticas de controle de acesso são externas e não estão no código de aplicativo, portanto as alterações nas políticas podem ser feitas sem o código de recompilação.

Ela é compacta...

A nova estrutura é bem dimensionada. O número de políticas de controle de acesso aumenta com o número de processos de negócios e não com o número de objetos. A maioria das estruturas de agrupamento baseia-se em condições implícitas, então, contanto que as condições sejam satisfeitas, a política será aplicada.

Aprimoramentos de Segurança no WebSphere Commerce Suite 5.1 Pro Edition

Embora o Commerce Suite 5.1 representasse uma nova arquitetura de e-commerce e fosse uma nova escrita completa do Commerce Suite 4.1 baseado em C++, ele continha todos os recursos de segurança de versões anteriores do WebSphere Commerce Suite, mais os novos aprimoramentos de segurança incluídos. Esses aprimoramentos foram herdados pelo WebSphere Commerce 5.4.

O Commerce Suite 5.1 continuou com a proteção contra acesso não autorizado a recursos de administradores e compradores do WebSphere Commerce Suite que foram fornecidos em releases anteriores:

- Continuando o suporte para recursos de controle de acesso que asseguram que o usuário do WebSphere Commerce Suite seja autenticado ou esteja no modo SSL antes de obter acesso ou submeter informações sensíveis.
- Atribuindo comandos do WebSphere Commerce Suite a grupos de forma que somente o Administrador do Site ou Administradores do Nível de Armazenamento podem executar um comando específico, seguido pelo mesmo modelo do Commerce Suite 4.1.

Aprimoramentos de Segurança Gerais

Com a reescrita do Commerce Suite 5.1 em Java, uma série de problemas de segurança herdados, que importunam a escrita do software em C++, foram removidos. O Java não utiliza ponteiros, dessa forma eliminou o problema de estouro de buffer que é uma vulnerabilidade de segurança da maioria dos softwares baseados em C++. Por estar em conformidade com as especificações J2EE padrão na indústria, o WebSphere Commerce Suite utilizou uma forte verificação de tipos para garantir que o servidor não execute instruções enganosas especificadas por indivíduos desonestos.

O algoritmo DES Triplo (padrão de criptografia de dados) padrão na indústria foi utilizado para proteger informações sensíveis no sistema WebSphere Commerce

Suite. O pacote que contém o algoritmo DES Triplo é sinalizado digitalmente de forma que se ele tiver sido violado o servidor WebSphere Commerce Suite não poderá ser iniciado.

Gerenciamento de Sessões

O gerenciamento de sessões do WebSphere Commerce Suite foi completamente reescrito para segurança máxima, utilizando uma técnica exclusiva para garantir que cookies não sejam roubados. Com a utilização de um cookie de autenticação que somente flui através do SSL (secure sockets layer) e consiste em uma data e hora criptografadas, o design de gerenciamento de sessões reescrito protege contra pirataria de sessões.

Autenticação

As senhas do sistema e do aplicativo necessárias pelo servidor WebSphere Commerce Suite durante a execução foram seguramente criptografadas, utilizando-se uma chave de 12 bits especificada por um comerciante e armazenada nos arquivos de configuração do WebSphere Commerce Suite. As informações sensíveis que aparecem na caixa de entrada de URL dos usuários, foram criptografadas para proteger compradores contra divulgação não autorizada.

Log

O sistema de log do WebSphere Commerce Suite foi projetado com segurança como uma consideração importante para que as informações sensíveis, como senha e informações do cartão de crédito do comprador, não fossem registradas, por padrão, nos arquivos de log do WebSphere Commerce Suite.

Convenções Utilizadas neste Manual

Este manual utiliza as seguintes convenções de destaque:

- **Negrito** indica comandos ou controles da interface gráfica com o usuário (GUI) como os nomes de campos, ícones ou opções de menu.
- `Espaçamento fixo` indica exemplos de texto que devem ser digitados exatamente como o exibido, nomes de arquivo e caminhos e nomes de diretórios.
- *Itálico* é utilizado para dar ênfase às palavras. Itálico também indica nomes que devem ser substituídos pelos valores apropriados para seu sistema. Quando for exibido um dos nomes a seguir, substitua-o pelo valor do seu sistema, conforme descrito:

  host_name
  O nome completo do host da máquina do WebSphere Commerce Studio (por exemplo, `ibm.com` é o nome completo).

  Windows

  unidade
  A letra representando a unidade na qual você instalou o produto ou o componente que está sendo discutido (por exemplo, `C:`).

Este ícone representa uma dica ou informações adicionais que podem ajudá-lo a concluir uma tarefa.

Windows indica informações específicas ao WebSphere Commerce para Windows NT e Windows 2000.

AIX indica informações específicas ao WebSphere Commerce para AIX.

Solaris indica informações específicas ao WebSphere Commerce para o software Solaris™ Operating Environment.

400 indica informações específicas ao WebSphere Commerce para o IBM @server iSeries 400 (anteriormente chamado deAS/400)

Linux indica informações específicas ao WebSphere Commerce para Linux.

Professional indica informações específicas ao WebSphere Commerce Professional Edition.

Business indica informações específicas ao WebSphere Commerce Business Edition.

Onde Localizar mais Informações

Para obter informações sobre o produto WebSphere Commerce 5.4, consulte os seguintes sites da Web:

- Business `http://ibm.com/software/webservers/commerce/wc_be/lit-tech-general.html`
- Professional `http://www.ibm.com/software/webservers/commerce/wcs_pro/lit-tech-general.html`

Para obter mais informações relacionadas ao Commerce Studio, Professional Developer Edition 5.1 ou a releases anteriores do WebSphere Commerce Studio, consulte o seguinte site da Web:

`http://www.ibm.com/software/webservers/commerce/commercestudio/lit-tech-general.html`

Parte 1. Modelo de Segurança do WebSphere Commerce

Esta parte fornece uma visão geral conceitual da segurança do WebSphere Commerce.

Capítulo 1. Introdução ao Modelo de Segurança do WebSphere Commerce

Este capítulo descreve o modelo de segurança do WebSphere Commerce, bem como seus vários conceitos de segurança.

Visão Geral

As informações neste documento descrevem as noções de autenticação, autorização, políticas e confidencialidade:

O que é Autenticação?

Autenticação é o processo de verificar se os usuários ou aplicativos são quem eles afirmam ser. Em sistema WebSphere Commerce, a autenticação é requerida para todos os usuários e aplicativos que acessam o sistema, com exceção dos usuários convidados. O processo de autenticação do usuário é sempre executado sob o SSL. Isso assegura que um terceiro utilizando programas que rondam a rede não possam *bisbilhotar* na rede quando um usuário submete uma senha. As senhas nunca são decriptogradas durante o processo de autenticação, porque é a prática de segurança comum. Todas as senhas de usuários sofrem hash e são criptografadas utilizando uma chave de 128 bits, conhecida como *chave do comerciante*. A chave do comerciante é especificada durante a instalação e a configuração do sistema WebSphere Commerce.

O sistema WebSphere Commerce possui suas próprias senhas para propósitos de administração. Essas senhas devem ser alteradas periodicamente como parte de uma política de segurança em todo o site do WebSphere Commerce. Para obter detalhes sobre como alterar as senhas do sistema WebSphere Commerce 5.4, consulte o Capítulo 7, “Definindo e Alterando Senhas” na página 71.

O que é Autorização?

Autorização é o processo de determinar se um usuário pode executar uma operação específica em um recurso. A autorização é determinada das políticas de controle de acesso para recursos do WebSphere Commerce. Em um sistema WebSphere Commerce, o controle de acesso é necessário em duas áreas:

- Para proteger o Enterprise JavaBeans (EJB beans) do WebSphere Commerce contra acesso não autorizado. Esse processo é discutido no Capítulo 5, “Ativando a Segurança do WebSphere Application Server” na página 55.
- Para assegurar que somente partes autorizadas podem executar grupos diferentes de comandos do WebSphere Commerce. Esse processo é discutido no Capítulo 11, “Controle de Acesso” na página 89.

O que são Políticas de Controle de Acesso?

Supondo que você tenha terminado de definir as organizações e os usuários que participarão de seu site de e-commerce, você poderá agora gerenciar suas atividades através de um conjunto de políticas, um processo referido como *controle de acesso*.

Uma política de controle de acesso é uma regra que descreve qual usuário ou grupo de usuários está autorizado a executar atividades específicas em seu site.

Essas atividades podem variar de registro, gerenciamento de leilões, atualização de catálogo de produtos a concessão de aprovações em ordens, bem como a qualquer uma das centenas de outras atividades que são necessárias para operar e manter um site de e-commerce.

As políticas são o que concedem aos usuários o acesso ao seu site. A menos que eles estejam autorizados a executar suas responsabilidades através de uma ou mais políticas de controle de acesso, os usuários não têm acesso a nenhuma das funções de seu site.

O modelo de controle de acesso do WebSphere Commerce 5.4 baseia-se na aplicação de políticas de controle de acesso. As políticas de controle de acesso são aplicadas pelo Gerenciador de Políticas de controle de acesso. Em geral, quando um usuário tenta acessar um recurso que pode ser protegido, o gerenciador de políticas de controle de acesso primeiro determina quais políticas de controle de acesso são aplicáveis para esse usuário e, em seguida, com base nas políticas de controle de acesso aplicáveis, determina se o usuário pode executar a operação solicitada no recurso especificado.

O que é uma Trilha de Auditoria?

Em computação, uma *trilha de auditoria* é utilizada para consultar logs eletrônicos ou em papel que são utilizados para rastrear a atividade do computador. Por exemplo, um funcionário pode ter acesso a uma parte de uma rede corporativa, como contas a receber, mas pode não estar autorizado a acessar outras partes do sistema, como folha de pagamento. Se esse funcionário tentar acessar uma seção não autorizada digitando senhas, essa atividade inadequada será registrada na trilha de auditoria.

Em sistemas de e-commerce, as trilhas de auditoria são utilizadas para registrar a atividade de um cliente. Uma trilha de auditoria registra um contato inicial do cliente com o sistema, bem como ações subseqüentes, como pagamento e entrega do produto ou serviço. As empresas podem utilizar a trilha de auditoria para responder a quaisquer dúvidas ou reclamações. E também podem utilizar a trilha de auditoria para reconciliar contas, fornecer informações de análise e históricas para planejamento e orçamento futuros e fornecer um registro de vendas no caso de uma auditoria fiscal.

As trilhas de auditoria também podem ser utilizadas para investigar crimes de computador através do ciberespaço e da internet. Para expor um indivíduo que está conduzindo ataques maliciosos em um sistema, os investigadores podem seguir a trilha de auditoria deixada pelo criminoso. Às vezes, os criminosos no ciberespaço, sem saber, deixam para trás trilhas de auditoria em logs de atividade com seus provedores de serviços da internet ou, talvez, através de logs de salas de bate-papo.

O que é Confidencialidade?

Confidencialidade é o processo de proteger informações sensíveis de serem decifradas por destinatários involuntários. No sistema WebSphere Commerce, a confidencialidade é necessária quando informações sensíveis fluem do navegador do usuário para o servidor WebSphere Commerce, bem como do servidor WebSphere Commerce para o navegador do usuário. Conforme discutido no Capítulo 8, “Ativando o SSL para Produção com o IBM HTTP Server” na página 77, ou uso do SSL fornece confidencialidade para esse cenário.

A confidencialidade é também um requisito forte na área de gerenciamento de sessões. Como o protocolo HTTP (Hypertext Transfer Protocol) não tem informações de estado, um *cookie* é comumente utilizado para identificar continuamente o usuário ao servidor WebSphere Commerce. Se o cookie for roubado, então a conta do usuário ficará comprometida. Isso normalmente é conhecido como *pirataria de sessão*. O WebSphere Commerce impede que a pirataria de sessão utilize recursos exclusivos das especificações de cookie, conforme discutido no Capítulo 6, “Gerenciamento de Sessões” na página 63.

Capítulo 2. Autenticação

O WebSphere Commerce exibe a autenticação como o processo de verificar se os usuários ou aplicativos são o que eles dizem ser. Esta seção descreve os detalhes de vários aspectos da autenticação do WebSphere Commerce.

Modelo de Autenticação do WebSphere Commerce

O modelo de autenticação do WebSphere Commerce é baseado nos seguintes conceitos:

- Mecanismos de Desafio
- Mecanismos de Autenticação
- Registro de usuários

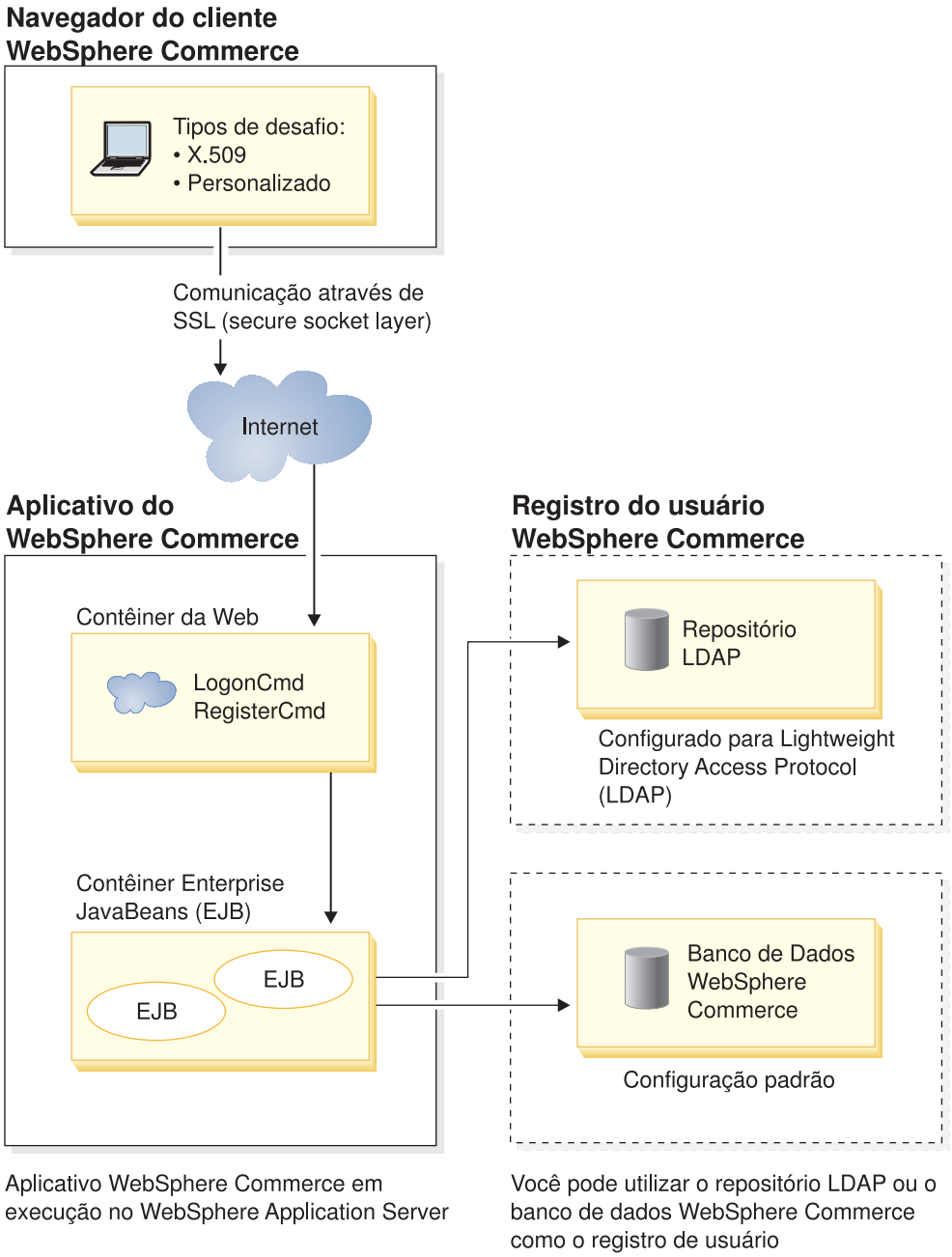


Figura 1. Modelo de segurança do WebSphere Commerce 5.4

Mecanismos de Desafio

Um mecanismo de desafio especifica como um servidor desafia e recupera dados de autenticação de um usuário. O WebSphere Commerce 5.4 suporta os seguintes métodos de autenticação ou de mecanismos de desafio:

Autenticação baseada em formulário ou personalizada
Esse mecanismo de autenticação permite um login específico do site através de uma página HTML ou formulário JSP.

Autenticação baseada em certificado (certificado X.509)
O mecanismo de desafio de certificado indica que o servidor Web seja

configurado para executar autenticação mútua através do SSL. O cliente precisa apresentar um certificado para estabelecer a conexão. Esse certificado é então mapeado para um registro do usuário.

Mecanismos de Autenticação

Um *mecanismo de autenticação* autentica um usuário verificando seus dados de autenticação junto com um registro de usuário associado. O WebSphere Commerce 5.4 emite um token de autenticação que está associado com um usuário em cada pedido subseqüente após o processo de autenticação. Estará encerrado quando o usuário efetua logoff ou fecha o navegador.

Validação de Certificado

Esse é o processo de verificar se o certificado do cliente X.509 é confiado pelo servidor da Web e se também está em conformidade com a política de certificados do servidor da Web. O WebSphere Commerce também verifica o certificado X.509 junto com o banco de dados do WebSphere Commerce. O servidor da Web executa o controle de acesso rústico no certificado, enquanto que o WebSphere Commerce executa um controle de acesso refinado no certificado.

Ligação LDAP

Esse é o processo de verificar as informações de desafio fornecidas como válidas, executando-se a operação de ligação LDAP para autenticar o usuário.

Ligação de Bancos de Dados

Esse é o processo de verificar se o id de usuário e senha fornecidos durante o processo de autenticação são válidos quando comparados com as informações de autenticação armazenadas no banco de dados do WebSphere Commerce.

Registro do Usuário

O registro do usuário é um repositório que contém informações do usuário e as informações de autenticação do usuário (por exemplo, a senha). As informações de autenticação fornecidas por um proprietário (ou seja, a representação de um usuário ou entidade do sistema em um registro do usuário) podem ser verificadas ou validadas pelo registro do usuário.

O WebSphere Commerce 5.4 suporta registros de usuário com base em dois domínios: registro do LDAP e o banco de dados do WebSphere Commerce.

O WebSphere Commerce 5.4 suporta os seguintes provedores LDAP:

- IBM SecureWay Directory Windows AIX Solaris Linux 400
- Netscape® Directory Server Windows AIX Solaris
- Windows 2000 Active Directory 2000

Credenciais

O servidor WebSphere Commerce 5.4 suporta mecanismos de autenticação com base em credenciais de validação, como certificados, tokens ou pares de ID do usuário e senha. As credenciais são verificadas junto a um registro de usuário que suporta tal esquema.

Token do WebSphere Commerce

O WebSphere Commerce utiliza um cookie de autenticação seguro para gerenciar os dados de autenticação. Um cookie de autenticação somente flui sobre o SSL e recebe uma marca de tempo para segurança máxima. Este cookie é utilizado para

autenticar o usuário dentro das conexões SSL sempre que um comando com distinção de maiúsculas e minúsculas for executado, por exemplo o`DoPaymentCmd`, que pede o número do cartão de crédito do usuário. Há um risco mínimo de que esse cookie seja roubado e utilizado por um usuário não autorizado.

Um segundo cookie que flui entre o navegador e o servidor dentro de conexões SSL ou não SSL é utilizado para verificação do usuário dentro de conexões não SSL.

WebSphere Application ServerToken LTPA

Um token LTPA é uma parte de dados que contém informações de usuário necessárias para determinar permissões de acesso para um recurso solicitado pelo usuário. Contém os dados de autenticação junto com a assinatura digital do servidor LTPA do WebSphere Application Server.

No caso do esquema LTPA (Lightweiht Third Party Authentication) do WebSphere Application Server, um diretório LDAP contendo as informações sobre os usuários é o registro do usuário ao qual a autenticação é executada. O servidor de recursos entra em contato com o Servidor de Segurança WebSphere Application Servere especifica que o LTPA seja o mecanismo de autenticação. Ele também fornece os dados de autenticação associados ao pedido. O Servidor de Segurança do WebSphere Application Server então valida os dados de autenticação junto ao servidor LTPA e retorna um token LTPA.

Sign-on Único

A filosofia por trás do sign-on único HTTP é preservar a autenticação do usuário através de vários pedidos HTTP. Seu objetivo é: evitar solicitar várias vezes ao usuário as credenciais de segurança de um determinado domínio de segurança que inclui:

- Servidores de WebSphere Application Server coperativos, mas distintos.
- Aplicativos cooperativos como os servidores LDAP, por exemplo IBM SecureWay Directory Server.

Em um cenário de sign-on único (SSO), um Cookie HTTP é utilizado para propagar informações de autenticação do usuário a servidores Web distintos livrando o usuário de digitar as informações de autenticação para cada nova sessão de cliente-servidor (assumindo autenticação básica).

Para obter as etapas para implementação de sign-on único com o WebSphere Commerce, consulte Capítulo 10, “Sign-on Único” na página 85.

Políticas de Autenticação

Uma política de autenticação é um conjunto de regras que são aplicadas ao processo de autenticação e à verificação de dados de autenticação pelo WebSphere Commerce. O WebSphere Commerce 5.4 suporta as política de contas, outras políticas relacionadas a autenticação e políticas de sessão conforme descritas nas seções a seguir.

Políticas de Contas

As seguintes seções descrevem políticas de contas disponíveis com o WebSphere Commerce:

Política de contas

A página Política de contas do WebSphere Commerce Administration Console permite configurar uma política de contas. Um critério de conta define os critérios relacionados à conta, como critérios de bloqueio de senha e de conta.

Depois que uma política de conta é criada, ela pode ser atribuída a um usuário. Observe que você não poderá excluir uma política de contas se ela estiver em uso (ou seja, um usuário estiver atribuído à ela).

Para obter informações sobre a criação de políticas de contas, consulte o "Configurando uma Política de Contas" na página 49.

Consulte também o tópico de referência ″Políticas de Autenticação Padrão″ na ajuda online do WebSphere Commerce.

Política de Bloqueio de Contas

A página Política de bloqueio de conta do WebSphere Commerce Administration Console permite configurar uma política de bloqueio de conta para diferentes funções do usuário dentro do WebSphere Commerce. A política de bloqueio de contas desativará uma conta de usuário, se ações maliciosas forem executadas nessa conta, para reduzir as chances que as ações comprometem a conta.

A política de bloqueio de contas aplica os seguintes itens:

- O limite de bloqueio de conta. Este é o número de tentativas de logon inválidas antes que a conta seja desativada.
- Adiamentos consecutivos de logins malsucedidos. Este é o período de tempo durante o qual o usuário não pode efetuar login, após duas tentativas falhas de login. O atraso é incrementado pelo valor de atraso do tempo configurado (por exemplo, 10 segundos) em cada falha de login consecutiva.

Para obter informações sobre a criação de políticas de bloqueio de contas, consulte o "Configurando uma Política de Bloqueio de Contas" na página 51.

Política de Senha

A página Política de senha do WebSphere Commerce Administration Console permite controlar uma seleção de senha do usuário para definir as características da senha a fim de garantir que ela atenda a política de segurança de seu site.

Este recurso define os atributos com os quais a senha deve estar de acordo. O critério de senha reforça as seguintes condições:

- Se o ID e a senha do usuário podem corresponder.
- Ocorrência máxima de caracteres consecutivos.
- Instâncias máximas de qualquer caracter.
- Tempo de vida máximo das senhas.
- Número máximo de caracteres alfanuméricos.
- Número máximo de caracteres numéricos.
- Comprimento máximo da senha.
- Se a senha anterior do usuário pode ser reutilizada.

Para obter informações sobre a criação de políticas de senhas, consulte o "Configurando uma Política de Senhas" na página 50.

Consulte também o tópico de referência ″Políticas de Autenticação Padrão″ na ajuda online do WebSphere Commerce.

Outras Políticas Relacionadas a Autenticação

As seguintes seções descrevem políticas relacionadas a autenticação disponíveis com o WebSphere Commerce:

Invalidação de Senha

Utilize o nó Invalidação de Senha do Gerenciador de Configuração para ativar ou desativar o recurso de invalidação de senha. Este recurso, quando ativado, requer que os usuários do WebSphere Commerce alterem sua senha se a senha do usuário tiver expirado. Nesse caso, o usuário é redirecionado para uma página em que é solicitado que ele altere sua senha. Os usuários não podem acessar nenhuma página segura no site até que tenham alterado sua senha.

Para obter informações sobre o nó Invalidação de Senha, consulte "Ativando a Invalidação de Senha" na página 43.

Comandos Protegidos por Senha

Utilize o nó Comandos Protegidos por Senha do Gerenciador de Configuração para ativar ou desativar o recurso de comandos protegidos por senha. Quando este recurso é ativado, o WebSphere Commerce requer que os usuários registrados que efetuaram logon no WebSphere Commerce digitem sua senha antes de continuar um pedido que executa comandos designados do WebSphere.

Cuidado: Quando você configura os comandos protegidos por senha, alguns dos comandos mostrados na lista de seleção de comandos podem ser executados por usuários genéricos ou convidados. A configuração de tais comandos como protegidos por senha restringirá os usuários genéricos e convidados de executá-los. Portanto, você deve ter cuidado ao configurar comandos a serem protegidos por senha.

Nota: O WebSphere Commerce exibirá somente os comandos que estão designados como `autenticados` ou definidos com o sinalizador `https` na tabela `URLREG` na lista de comandos disponíveis.

Para obter informações sobre a utilização do nó Comandos Protegidos por Senha, consulte "Ativando os Comandos Protegidos por Senha" na página 44.

Políticas de Sessão

No WebSphere Commerce 5.4 as políticas de sessão são incorporadas na política de tempo limite de login.

Com a política de tempo limite de login, o WebSphere Commerce efetuará logoff de um usuário que está inativo por um longo período de tempo e solicitará que ele efetue logon no sistema utilizando o nó Tempo Limite de Login. Esse aprimoramento é chamado através do Gerenciador de Configuração do WebSphere Commerce e está descrito em detalhes em "Ativando o Tempo Limite de Login" na página 42.

Capítulo 3. Autorização (Controle de Acesso)

O WebSphere Commerce exibe a autorização de authorization como o processo que verifica se os usuários ou aplicativos têm autoridade para acessar um recurso. Esta seção descreve os detalhes de vários aspectos do controle de acesso do WebSphere Commerce.

A autorização ou o controle de acesso, no WebSphere Commerce é executado utilizando-se políticas de controle de acesso. Uma política de controle de acesso é uma regra que descreve qual grupo de usuários pode executar um conjunto de ações em um conjunto de recursos. O WebSphere Commerce fornece um conjunto de políticas de controle de acesso padrão. Essas políticas de controle de acesso padrão são especificadas no formato XMT e designadas para aplicar muitos dos requisitos típicos de controle de acesso que um site de e-commerce precisa. Para entender o componente de controle de acesso do WebSphere Commerce, primeiro é necessário entender a hierarquia organizacional típica de um site de e-commerce.

Hierarquia Organizacional

Usuários e entidades organizacionais dentro do subsistema de membros do WebSphere Commerce são organizados em uma hierarquia. Geralmente, essa hierarquia emula uma hierarquia organizacional típica, com entradas para organizações e unidades organizacionais e entradas para usuários nos nós folha. A hierarquia inclui uma entidade organizacional artificial chamada de *organização raiz* na parte superior. Todas as outras entidades organizacionais e usuários são descendentes dessa organização raiz. Sob a organização raiz pode haver uma organização de venda e várias organizações de compra; todas essas organizações podem ter uma ou mais suborganizações sob elas. Os administradores de compra ou venda das organizações são os chefes e os responsáveis pela manutenção de suas organizações. No lado da organização de venda, cada sub-organização de venda pode ter uma ou mais lojas dentro dela. Os Administradores das Lojas são responsáveis pela manutenção das mesmas. O diagrama a seguir mostra a hierarquia organizacional de um site de e-commerce business-to-business.

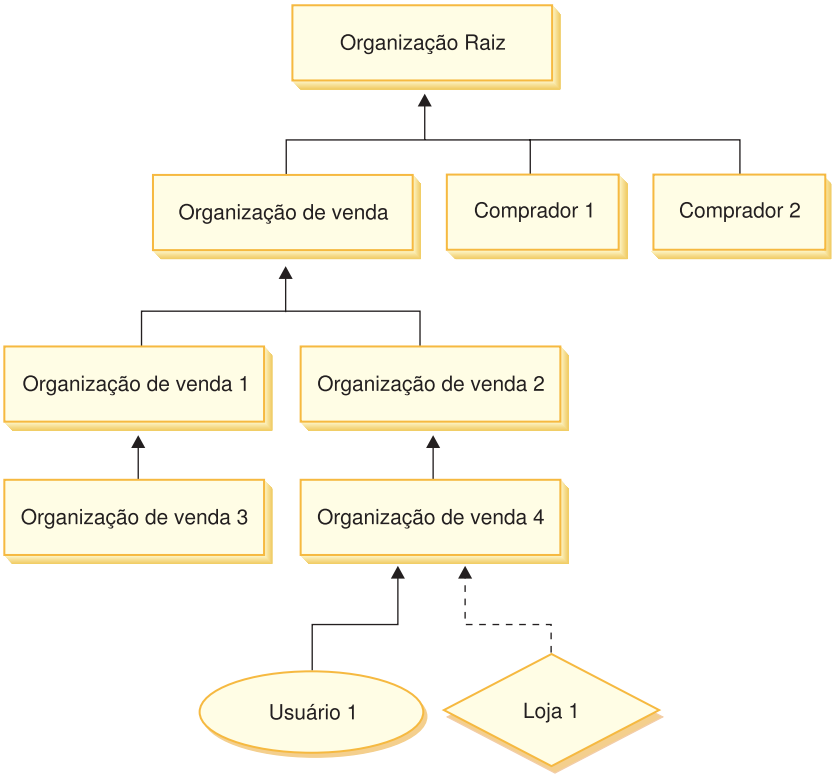


Figura 2. Hierarquia organizacional de um site de business-to-business

Organização Raiz

A organização raiz fica na parte superior da hierarquia organizacional. Um Administrador de site tem acesso de super usuário para executar qualquer operação dentro do WebSphere Commerce. O Administrador do Site instala, configura e mantém o WebSphere Commerce e seu software e hardware associados. Essa função normalmente controla o acesso e a autorização (ou seja, criando e atribuindo membros à função apropriada) e gerencia o site na Web. O Administrador do Site pode atribuir funções aos usuários e especificar as organizações para as quais o usuário exerce a função. O Administrador de Site deve atribuir uma senha a cada administrador para assegurar que apenas as partes autorizadas tenham acesso à informações confidenciais. Isso fornece uma forma de controlar as responsabilidades principais, como a atualização de um catálogo ou a aprovação de um RFQ (request for quotation - pedido de cotação).

Nota: É possível que um usuário exerça funções em uma organização diferente de sua organização pai.

Em um site do WebSphere Commerce, há uma organização de venda. Em um site de business-to-business, também há uma ou mais organizações de compra. O Administrador do Site pode definir as políticas de controle de acesso da organização de venda (que possui a loja), bem como as políticas de controle de acesso de cada organização que compra da loja. Em um site de business-to-consumer, não há organizações de compra. Os clientes de business-to-consumer são modelados como membros da organização padrão.

Organizações (vendedor)

Nos sites de business-to-business e de business-to-consumer, o Administrador do Site cria um vendedor no nível superior. Sob essa organização de venda, outras suborganizações ou unidades de organização podem ser criadas. Qualquer uma dessas entidades organizacionais pode possuir uma ou mais lojas. O Administrador do Site então define todas as políticas de controle de acesso especiais para uma organização de venda e atribui um Administrador do Vendedor para gerenciar essa organização. O Administrador do Vendedor registra usuários e atribui a eles funções diferentes para ajustar as necessidades de negócio da organização, de acordo com as políticas de controle de acesso pertencentes a essa organização.

As responsabilidades do Administrador do Vendedor são resumidas desta forma:

- Crie sub-organizações que possam possuir lojas. Opcionalmente, defina quais processos na organização requerem aprovação. Essa etapa é necessária somente em um site business-to-business.
- Atribua funções às sub-organizações.
- Crie usuários.
- Atribua funções a usuários.

Organizações (comprador)

Em um site de business-to-business, o Administrador do Site cria uma ou mais organizações de compra, dependendo das necessidades de negócio. O Administrador do Site então define todas as políticas de controle de acesso especiais para uma organização de compra e atribui um Administrador do Comprador para gerenciar a organização de compra. O Administrador do Comprador registra usuários e atribui a eles funções diferentes para ajustar as necessidades de negócio da organização, de acordo com as políticas de controle de acesso pertencentes a essa organização.

As responsabilidades do Administrador do comprador são resumidas desta forma:

- Criar e administrar sub-organizações dentro e uma organização compradora. Opcionalmente, defina quais processos na organização requerem aprovação. Essa etapa é necessária somente em um site business-to-business.
- Atribua funções às sub-organizações.
- Crie usuários.
- Atribua funções a usuários.

Nota: Observe que o Administrador do Site pode modificar e gerenciar as políticas de controle de acesso da organização de compra, se adequado. Para obter mais informações sobre as tarefas do Administrador do Site, consulte o "Administrador do Site" na página 16.

Funções

Conforme mencionado acima, o WebSphere Commerce fornece conjuntos de funções padrão. O Administrador do Site deve atribuir funções específicas a cada organização antes de atribuir usuários a essas funções. Uma organização somente pode exercer funções que foram atribuídas a sua organização pai. Da mesma maneira, um usuário somente pode exercer funções que foram atribuídas a sua organização pai.

Todas as funções no WebSphere Commerce são estendidas a uma organização. Por exemplo, um usuário exerce a função de Gerente de Produtos para a Organização

X. A organização pai deste usuário também deve ser atribuída à função Gerente de Produtos por si só. As políticas de controle de acesso poderiam então ser configuradas como para que este usuário possa somente executar as operações de gerenciamento de produto dentro do contexto da Organização X e suas suborganizções.

Nota: A atribuição de funções para usuários e organizações é feita na tabela MBRROLE.

As funções padrão fornecidas com o WebSphere Commerce podem ser agrupadas nas seguintes categorias:

- Operações de site;
- Desenvolvimento de site e conteúdo;
- Gerenciamento de marketing;
- Gerenciamento de produtos;
- Gerenciamento de vendas
- Gerenciamento de logística e operações;
- Gerenciamento organizacional.

Operações do Site

As seguintes funções de operações técnicas são suportadas peloWebSphere Commerce:

- Administrador do Site
- Administrador da Loja

Administrador do Site

O Administrador do Site instala, configura e mantém o WebSphere Commerce e o software e hardware associado. O Administrador responde a avisos, alertas e erros do sistema e diagnostica e soluciona problemas do sistema. Essa função normalmente controla o acesso e a autorização (criando e atribuindo membros à função apropriada), gerencia o site na Web, monitora o desempenho e gerencia tarefas de equilíbrio de carga. O Administrador do Site também pode ser responsável por estabelecer e manter diversas configurações do servidor para diferentes etapas do desenvolvimento: como teste, preparação e produção. Essa função também efetua backups críticos no sistema e resolve problemas de desempenho.

Administrador da Loja

O Administrador da Loja gerencia os ativos da loja, atualiza e publica as alterações nas informações de impostos, envio e da loja. O Administrador da Loja também pode gerenciar as políticas de controle de acesso para a organização. O Administrador da Loja, geralmente o líder da equipe de desenvolvimento da loja, é a única função da equipe com autoridade para publicar um archive da loja (o Administrador do Site também pode publicar um archive da loja). O Administrador da Loja geralmente tem conhecimento da Web e tem um conhecimento completo dos procedimentos de negócios da loja.

Desenvolvimento do Site e Conteúdo

O WebSphere Commerce suporta o site Desenvolvedor da Loja e a função de desenvolvimento de conteúdo.

Desenvolvedor da Loja

Os Desenvolvedores da Loja criam arquivos Java Server Pages e qualquer código personalizado necessário e podem modificar qualquer uma das funcionalidades padrão incluídas no WebSphere Commerce. Quando um archive de loja tiver sido criado, os Desenvolvedores de Loja terão autoridade para fazer alterações manualmente ou através do bloco de notas Perfil da Loja e dos blocos de notas Imposto e Envio. Eles não têm autoridade para publicar o archive da loja no WebSphere Commerce Server.

Logística e Operações

O WebSphere Commerce suporta as seguintes funções de gerenciamento de de logística e operações:

- Gerente de Logística
- Gerente de Operações
- Receptor
- Administrador de Devoluções
- Coletor

Gerente de Logística

Business O Gerente de Logística, às vezes chamado de Gerente de Envio, gerencia e negocia frete ou envio de grandes volumes das transportadoras para o warehouse e para clientes individuais. Essa função é responsável por assegurar que a companhia utiliza os melhores expedidores, com os melhores custos, para atender a estratégia de empresa. O envio é um aspecto importante do serviço do cliente e pode ser um fator de sucesso importante para os negócios online.

Gerente de Operações

B2C Essa função gerencia os pedidos que estão processando, garantindo que os pedidos sejam preenchidos adequadamente, que o pagamento seja recebido e que outros pedidos sejam enviados. O Gerente de Operações pode procurar por pedidos de clientes, exibir detalhes, gerenciar informações de pedidos e criar e editar devoluções.

Coletor

O Coletor coleta produtos de centros de distribuição e os empacota para envio aos clientes. O Coletor também gerencia listas de coleta e guias de envio que são utilizados para confirmar o envio de produtos durante o atendimento a pedidos.

Receptor

O Receptor recebe o estoque no centro de distribuição, rastreia registros de estoque esperados e recebimentos não esperados para produtos pedidos e recebe produtos devolvidos como um resultado de devoluções de clientes.

Administrador de Devoluções

O Administrador de Devoluções gerencia a disposição de produtos devolvidos.

- Lista de devoluções
- Lista de produtos devolvidos
- Disposições de produtos devolvidos

Gerenciamento de Produtos

As seguintes funções de gerencimento de produtos são suportadas pelo WebSphere Commerce:

- Comprador (Lado da Venda)

- Gerente de Categorias
- Gerente de Produtos ou Gerente de Propaganda

Comprador (Lado da Venda)
O comprador compra mercadorias para venda. Ele manipula relações com vendedores ou fornecedores e negocia para obter o produto desejado com condições favoráveis, para coisas como entrega e opções de pagamento. O comprador pode definir preços. O estoque é gerenciado pelo comprador para determinar as quantidades a serem compradas e garantir que o estoque seja adequadamente reabastecido.

Gerente de Categoria
O gerente de categoria gerencia a hierarquia de categorias, criando, modificando e excluindo categorias. A hierarquia de categorias organiza produtos ou serviços oferecidos pela loja. O Gerente de Categorias também gerencia produtos, registros de estoque esperado, informações sobre fornecedores, estoque e motivos de devolução.

Gerente de Produto/Gerente de Propaganda
O Gerente de Business Propaganda ou de B2C Produto rastreia compras do cliente, sugere descontos e determina a melhor forma de exibir preços e vender produtos na loja online

- Executa todas as tarefas do gerente de Categoria.
- Executa todas as tarefas do gerente de Marketing.

Gerenciamento de Vendas
As seguintes funções de gerencimento de produtos são suportadas pelo WebSphere Commerce:

- Gerentes de Vendas
- Representante de Conta
- Supervisor de Atendimento ao Cliente
- Representante de Atendimento ao Cliente

Gerente de Vendas
Os Gerentes de Vendas adquirem e mantêm clientes, atendem previsões de vendas, fornecem incentivos para aumento do negócio do cliente, contratam gerentes, definem condições de preços, trabalham com o gerente de produtos para estabelecer previsões de estoque e trabalham com o Gerente de Marketing para promoções.

Representante de Conta
Os Representantes de contas trabalham com contas individuais para construir relacionamentos e gerenciar questões de serviços do cliente. Eles podem ser autorizados a alterar o preço do contrato, a negociar contratos, perfis e a analisar a lucratividade por categoria de conta.

Supervisor do Atendimento ao Cliente
Essa função possui acesso a todas as tarefas de serviço do cliente. O Supervisor de Atendimento ao Cliente gerencia perguntas do cliente (como registro do cliente, pedidos, devoluções e leilões) e tem autoridade para concluir tarefas que não podem ser acessadas por um Representante de Serviço ao Cliente, como aprovar registros de devolução negados pelo sistema e contatar clientes com relação a exceções de pagamento (como falhas na autorização do cartão de crédito).

Representante de Atendimento ao Cliente

Independentemente dos negócios online serem bem projetados para oferecer ao cliente recursos de auto-serviço, existem alguns tipos de clientes ou ocasiões em que até o cliente mais experiente em web requer contato pessoal. A maioria dos negócios online fornece um e-mail, fax ou número de contato para o cliente obter serviço direto. É responsabilidade do representante de serviço ao cliente manipular todas as perguntas do cliente.

Gerenciamento de Marketing

O WebSphere Commerce suporta a função de gerenciamento de marketing do Gerente de Marketing.

Gerente de Marketing

O Gerente de Marketing comunica a estratégia de mercado e as mensagens da marca para os clientes. Essa função monitora, analisa e compreende o comportamento do cliente. Além disso, o gerente de marketing cria e modifica perfis de clientes para vendas direcionadas e cria e gerencia campanhas e promoções. O planejamento de eventos de campanhas pode ser manipulado por uma equipe composta pelo Comerciante, o Gerente de Marketing e o Gerente de Vendas.

Gerenciamento Organizacional

O WebSphere Commerce suporta as seguintes funções de gerenciamento organizacional:

- Administrador do Vendedor
- Administrador do Comprador
- Aprovador do Comprador

Administrador do Vendedor

O Administrador do Vendedor gerencia as informações para a organização de venda. Os administradores do vendedor criam e administram as suborganizações dentro da organização de venda e os vários usuários na organização de venda, incluindo a atribuição de funções de negócios adequadas.

Administrador do Comprador

O Administrador do Comprador gerencia as informações para a organização de compra. Eles criam e administram as suborganizações dentro da organização de compra e gerenciam os vários usuários, incluindo a aprovação de usuários como compradores. Outras funções no lado da compra, como aprovadores de comprador e administradores adicionais da organização de compra, podem ser criadas e gerenciadas.

Aprovador do Comprador

Um Aprovador do Comprador é um indivíduo na organização de compra que aprova pedidos feitos por compradores antes do pedido ser submetido para compra com o vendedor.

Política de Controle de Acesso

Uma política de controle de acesso autoriza um grupo de usuários a executar um conjunto de ações em um conjunto de recursos dentro do WebSphere Commerce. A menos que estejam autorizados a executar suas responsabilidades através de uma ou mais políticas de controle de acesso, os usuários não têm acesso a nenhuma das funções do sistema. Para compreender as políticas de controle de acesso, você precisa entender quatro conceitos principais: usuários, ações, recursos e

relacionamentos. Os usuários são as pessoas que utilizam o sistema. Os recursos são os objetos no sistema que precisam ser protegidos. Ações são as atividades que os usuários podem executar nos recursos. Os relacionamentos são condições opcionais que existem entre usuários e recursos.

Elementos de uma Política de Controle de Acesso

Uma política de controle de controle de acesso consiste em quatro elementos:

Grupo de Acesso
O grupo de usuários ao qual a política se aplica.

Grupo de Ações
Um grupo de ações executadas pelo usuário nos recursos.

Grupo de Recursos
Os recursos controlados pela política. Um grupo de recursos pode incluir objetos de negócios como `contrato` ou `pedido`, ou um conjunto de comandos relacionados como todos os comandos que os usuários de uma determinada função pode executar.

Relacionamento (opcional)
Cada tipo de recurso pode ter um conjunto de relacionamentos associadas a ele. Cada recurso pode ter um conjunto de usuários que preencham cada relacionamento. Por exemplo, uma política poderia especificar que somente o criador de um pedido pode modificá-lo. Neste caso, o relacionamento seria o `criador` e estaria entre o usuário e o recurso do pedido.

Conceitos da Política de Controle de Acesso

As políticas de controle de acesso concedem aos usuários o acesso ao seu site. A menos que eles estejam autorizados a executar suas responsabilidades através de uma ou mais políticas de controle de acesso, os usuários não têm acesso a nenhuma das funções de seu site.

Cada política de controle de acesso tem o seguinte formato:

```
AccessControlPolicy [AccessGroup,ActionGroup,ResourceGroup,Relationship]
```

Os elementos na política de controle de acesso especificam que o usuário que pertence a um grupo de acesso específico tem permissão para executar ações no grupo de ações especificado nos recursos que pertencem ao grupo de recursos especificado, desde que o usuário atenda a um relacionamento específico relativo ao recurso. O relacionamento é especificado somente quando necessário. Por exemplo, `[AllUsers,UpdateDoc,doc,creator ]` especifica que todos os usuários podem atualizar um documento, se eles forem os criadores do documento.

As seguintes seções descrevem informações conceituais e a terminologia associada ao controle de acesso.

Grupos de Membros

O subsistema Membros no WebSphere Commerce permite criar grupos de membros, os quais possuem usuários categorizados para várias razões de negócios. Os agrupamentos podem ser utilizados para vários fins, por exemplo, controle de acesso, aprovação, bem como marketing, como o cálculo de descontos e preços e exibição de produtos. Um grupo de membros do tipo Grupo de Acesso (-2) é para propostas de controle de acesso, enquanto que um grupo de membros do tipo Grupo de Usuários (-1) é para uso geral. Um grupo de membros está associado com tipos de grupo de membros na tabela MBRGRPUSG.

Grupos de acesso: Um grupo de membros do tipo Grupo de Acesso (-2) serve para agrupar usuários para fins de controle de acesso. Um grupo de acesso é um elemento de uma política de controle de acesso e está definido como um grupo de usuários definido especificamente para fins de controle de acesso. Os critérios para associação em um grupo de membros é normalmente baseado nas funções, na organização a qual o usuário pertence ou no status de registro do usuário. Por exemplo, o grupo de acesso chamado `Administradores do Comprador` é um grupo cujos usuários exercem funções de Administradores do Comprador.

O WebSphere Commerce inclui um número de funções padrão e correspondendo a cada função está um grupo de acesso padrão que implicitamente se refere aquela função.As funções podem ser utilizadas como atributos para incluir usuários em um grupo de acesso baseado no tipo de atividades que eles executam no site. Por exemplo, por padrão há uma função chamada Administrador do Vendedor e um grupo de acesso correspondente chamado `Administradores do Vendedor`. Um Administrador do Site utiliza o WebSphere Commerce Administration Console para criar, manter e excluir grupos de acesso para um site. Um Administrador do Comprador ou um Administrador do Vendedor utiliza o WebSphere Commerce Organization Administration Console para atribuir funções a usuários ou para explicitamente atribuir usuários a grupos de acesso. Os grupos de acesso podem ser implícitos, explícitos ou ambos.

Grupo de Acesso Implícito: Um grupo de acesso implícito é definido por um conjunto de critérios. Todos que satisfizerem os critérios serão um membro do grupo. Os critérios geralmente baseiam-se em funções, organização pai ou status de registro de um usuário. As condições implícitas que definem a associação em um grupo de membros estão na coluna `CONDIÇÕES` da tabela `MBRGRP`. A utilização de grupos de acesso implícito que especificam os atributos dos usuários facilita a autorização de acesso a usuários semelhantes sem ter que atribuir e retirar a atribuição de usuários individuais. Também elimina a necessidade de atualizar os membros de um grupo quando os atributos de um usuário são alterados. Um critério simples para um grupo de acesso é incluir todos que receberam uma função específica, independente de para qual organização o usuário exerce a função. Um critério mais complexo seria especificar que apenas usuários que exercem uma dentre um conjunto possível de funções para determinada organização pertenceria ao grupo de acesso.

Grupo de Acesso Explícito: É possível incluir ou remover explicitamente um usuário em um grupo de membros. Essas duas especificações explícitas podem ser feitas utilizando-se a tabela `MBRGRPMBR`. Um grupo de acesso explícito contém usuários atribuídos explicitamente que podem ou não compartilhar atributos comuns. Também permite excluir indivíduos que satisfaçam condições para inclusão em um grupo implicitamente definido, mas que você deseja excluir de qualquer forma.

Grupos de usuários: Um grupo de membros do tipo Grupo de Usuários (-1) é uma coleção de usuários definida pelo comerciante, que compartilha um interesse em comum. Os grupos de usuários são similares a clubes que são oferecidos por grandes lojas para seus clientes freqüentes ou preferidos. Fazer parte de um grupo de usuários pode autorizar aos clientes descontos ou outros bônus na compra de produtos. Por exemplo, se a pesquisa de mercado mostrar que clientes antigos compram repetidamente livros de viagem e bagagem, você pode atribuir a esses clientes um grupo de membros chamado `Clube de Viagem de Clientes Antigos`. Da mesma forma, você pode criar um grupo de usuários para premiar clientes freqüentes por seus negócios.

Ações

Geralmente, uma ação é uma operação executada em um recurso. Em políticas baseadas em funções para comandos controladores, a ação é `Execute` e o recurso é o comando sendo executado. Em políticas baseadas em funções para Exibições, a ação é o nome da exibição e o recurso é `com.ibm.commerce.commands.ViewCommand` . Para controle de acesso de nível de recurso, as ações geralmente mapeiam para comandos do WebSphere Commerce e o recurso é normalmente a interface remota de um EJB (Enterprise Java Bean) protegido. Por exemplo, o comando do controlador `com.ibm.commerce.order.commands.OrderCancelCmd` opera no recurso `com.ibm.commerce.order.objects.Order`. Por último, a ação `Exibir` é utilizada para ativar os recursos do bean de dados.

O WebSphere Commerce Administration Console pode ser utilizado por um Administrador de Site para associar as ações existentes com os grupos de ação, mas não para criar novas ações. Novas ações podem ser criadas definindo-as em um arquivo XML e, em seguida, carregando-as em um banco de dados. As ações são armazenadas na tabela `ACACTION`.

Grupos de Ação

Os grupos de ação são grupos de ações relacionadas. Um exemplo de um grupo de ação é o grupo `AccountManage` que inclui os seguintes comandos:

- `com.ibm.commerce.account.commands.AccountDeleteCmd`
- `com.ibm.commerce.account.commands.AccountSaveCmd`

Somente o Administrador do Site pode criar, atualizar e excluir grupos de ação.Isso pode ser feito a partir doWebSphere Commerce Administration Console e através do XML. Grupos de ações são armazenados na tabela `ACACTGRP`. Ações estão associadas com grupos de ação na tabela `ACACTACTGP`.

Categoria de Recursos

A categoria de recursos se refere a uma classe de recursos que precisam ser protegidos pelo controle de acesso. Os recursos devem implementar as informações da interface Protectable. As categorias de recursos são classes Java como pedido, RFQ e leilão. Os recursos são as instâncias dessas classes. Por exemplo, Auction1 criado pelo administrador de leilão A é um recurso; Auction2 criado pelo administrador de leilão B é outro recurso. Esses dois recursos pertencem à categoria de recursos: leilão.

Nota: Para obter mais informações sobre a interface Protectable, consulte o Manual do Programador do *IBM WebSphere Commerce*.

As categorias de recursos estão definidas na tabela `ACRESCGRY` e por conveniência são às vezes referidas como recursos. Um Administrador de Site pode associar categorias de recurso existentes com grupos de recurso, utilizando o WebSphere Commerce Administration Console. As novas categorias de recurso podem ser criadas utilizando o XML.

Recursos

Os recursos são quaisquer objetos no sistema que precisam ser protegidos. Por exemplo RFQs, leilões, usuários e pedidos são alguns dos recursos do WebSphere Commerce que precisam ser protegidos. Cada recurso tem um proprietário. A propriedade do recurso é utilizada para determinar quais políticas de controle de acesso aplicam-se a ele. As políticas de controle de acesso têm um proprietário, que é uma entidade organizacional. Uma política só é aplicada a recursos pertencentes à entidade organizacional que é proprietária da política. As políticas pertencentes a entidades organizacionais ascendentes também se aplicam ao recurso.

Recursos do Comando do Controlador: Para controle de acesso baseado em função para comandos do controlador, a política é estruturada de tal forma que a ação `Execute` está sendo executada no recurso de comandos do controlador. Essas políticas pretendem restringir a execução de comando controladores a usuários com uma função especificada. O grupo de acesso para essas políticas é geralmente aquele com uma única função, por exemplo, Gerenciadores de Produtos (aqueles com a função de Gerenciador de Produtos). Em seguida, o grupo de recursos seria o conjunto de comandos do controlador que um gerenciador de produtos pode executar.

Ao reforçar o controle de acesso baseado em função em um comando de controlador, o proprietário do comando deve ser determinado. Isto é feito chamando o método `getOwner()` no comando se tiver sido implementado. Geralmente este método não está implementado, então o WebSphere Commerce Runtime sempre o avaliará da seguinte maneira:

- Utilize a organização que possui a loja que está atualmente no contexto do comando.
- Se não houver nenhuma loja no contexto do comando, utilize a Organização Raiz como a proprietária.

Recursos do Bean de Dados: Nem todos os beans de dados requerem proteção. Dentro do aplicativo WebSphere Commerce existente, os beans de dados que requerem proteção já implementam o controle de acesso requerido. A dúvida sobre o que proteger aparece quando você cria novos beans de dados. Decidir quais recursos proteger vai depender de seu aplicativo. Um bean de dados deve ser protegido (diretamente ou indiretamente), se as informações a serem exibidas não forem suficientemente protegidas pelo controle de acesso baseado na função na exibição, que corresponde ao JSP (Java Server Page) que contém o bean de dados.

Se um bean de dados precisa ser protegido e pode existir por si só, deve ser diretamente protegido. Se a existência de um bean de dados depende da existência de um outro bean de dados, então ele deve delegar para outro bean de dados por motivo de proteção. Um exemplo de bean dados que deve ser diretamente protegido é o bean de dados `Order`. Um exemplo de bean de dados que deve ser indiretamente protegido é o bean de dados `OrderItem`, pois ele não pode existir sem o bean de dados `Order`. Consulte o *WebSphere Commerce 5.4 - Manual do Programador* para obter mais informações sobre como proteger o recurso do bean de dados.

Recursos de Dados: Os recursos de dados referem-se a objetos de negócios que podem ser manipulados, como leilões, pedidos, RFQs e usuários. Estes são normalmente protegidos no nível de bean corporativo, mas é possível proteger qualquer classe, desde que a interface Protectable seja implementada. Os recursos de dados são protegidos utilizando as verificações de controle de acesso do nível do recurso. A maneira comum de se fazer isso é retornar os recursos de dados no método `getResources()` de um controlador ou um comando de tarefa. Para obter mais informações, consulte o *WebSphere Commerce 5.4 - Manual do Programador*.

Grupos de Recursos

Um grupo de recursos identifica um conjunto de recursos relacionados. Um grupo de recursos pode incluir objetos de negócios, como um contrato ou um conjunto de comandos relacionados. No controle de acesso, os grupos de recursos especificam os recursos aos quais a política de controle de acesso autoriza o acesso.

Os grupos de recursos são definidos na tabela ACRESGRP. Os Administradores do Site podem gerenciar os grupos de recursos e associar os recursos com grupos de recursos utilizando o WebSphere Commerce Administration Console, ou o XML.

Grupos de Recursos Implícitos: Os grupos de recursos implícitos definem recursos que correspondem a um determinado conjunto de atributos. Um desses atributos deve ser o nome da classe do Java. Outros atributos podem incluir status, ID da loja, preço, etc. Por exemplo, você poderia criar um grupo de recursos implícito que inclua todos os pedidos que possuem status pendentes (ORDERS.STATUS=P). Os grupos de recursos implícitos geralmente são utilizados para agrupar recursos que serão utilizados em políticas de nível de recurso, quando os recursos compartilharem um atributo comum além do nome da classe Java.

Grupos de recursos implícitos são definidos utilizando-se a coluna CONDITIONS da tabela ACRESGRP. Grupos simples de recursos implícitos podem ser criados utilizando o WebSphere Commerce Administration Console. Progressivamente os grupos complexos podem ser criados utilizando o XML.

Grupos de Recursos Explícitos: Grupos de recursos explícitos são especificados pela associação de uma ou mais categorias de recursos a um grupo de recursos. Essa associação é feita na tabela ACRESGPRES . A inclusão de uma categoria de recursos em um grupo explicitamente, listando seu nome de classe Java permite agrupar recursos individuais que necessariamente podem não compartilhar atributos comuns.

Relacionamentos

Cada recurso pode ter algum tipo de relacionamento associado a ele e um conjunto de membros que realize cada relacionamento. Por exemplo, todos os recursos têm um relacionamento de *proprietário*, que é realizado pelo proprietário do recurso. Outros relacionamentos podem incluir recipientes de documentos e o criador de uma ordem. Esses relacionamentos de recursos são importantes na determinação de quem pode executar determinadas ações em uma instância específica de um recurso. Por exemplo, o criador de um documento pode não conseguir excluí-lo, mas talvez um auditor consiga. Similarmente, um revisor pode somente ler e aprovar um documento, mas não encaminhá-lo ou executar outras operações.

Os relacionamentos são armazenados na tabela ACRELATION, e são especificados opcionalmente em uma política de controle de acesso, utilizado a coluna ACRELATION_ID da tabela ACPOLICY. Ao avaliar uma política que requer o atendimento de um relacionamento entre o usuário e o recurso, o método fulfills(Membro Longo, Relacionamento de cadeia) no recurso será chamado para avaliá-la. Ao comparar esses relacionamentos para grupos de relacionamento, esses relacionamentos são referidos às vezes como relacionamentos simples.

Grupos de Relacionamentos: As políticas de controle de acesso podem especificar um usuário que deve cumprir um relacionamento específico com relação ao recurso que está sendo acessado ou elas podem especificar que um usuário deve cumprir as condições especificadas em um grupo de relacionamentos. Na maioria dos casos, um relacionamento é suficiente. No entanto, se mais relacionamentos complexos forem necessários, um grupo de relacionamento pode ser utilizado no lugar. Um grupo de relacionamento permite especificar vários relacionamentos e também uma cadeia de relacionamentos. Os dois são realizados utilizando uma construção de cadeia de relacionamento. Uma cadeia de relacionamento é uma construção que pode expressar um relacionamento simples (diretamente entre um usuário e o recurso), mas pode também ser utilizado para expressar uma série de relacionamentos entre o usuário e o recurso. Por exemplo, para expressar que o

usuário deve ter uma função em uma organização que possui um relacionamento (diferente do relacionamento de proprietário) com o recurso, ele deve utilizar o grupo de relacionamento. Neste exemplo, há um relacionamento de função entre o usuário e a organização, e um relacionamento entre a organização e o recurso.

Comparando relacionamentos e grupos de relacionamentos: Na maioria dos casos, a utilização de um relacionamento deve satisfazer os requisitos de controle de acesso para seu aplicativo desde que, de forma conceitual, a maioria dos relacionamentos sejam diretamente entre o usuário e o recurso. Por exemplo, a política declara que o usuário deve ser o criador do recurso. Se, porém, você precisar especificar vários relacionamentos, um grupo de relacionamento deve ser utilizado. Por exemplo, a política declara que o usuário deve ser o criador ou o remetente do recurso.

Os grupos de relacionamentos também são necessários para expressar uma cadeia de relacionamentos entre um usuário e o recurso. Em uma cadeia de relacionamentos, não há um relacionamento direto entre o usuário e o recurso por exemplo, um usuário pertence à organização compradora especificada por um pedido. Neste caso, o usuário tem um relacionamento filho com a organização, e esta organização tem um relacionamento de comprador com o pedido.

Cadeias de Relacionamentos: Cada grupo de relacionamento consiste de uma ou mais condições abertas RELATIONSHIP_CHAIN, agrupadas pelos elementos `andListCondition` ou `orListCondition`. Uma cadeia de relacionamento é uma série de um ou mais relacionamentos. O comprimento de uma cadeia de relacionamentos é determinado pelo número de relacionamentos que ela contém. Isso pode ser determinado examinando-se o número de entradas de `<parameter name= "X" value="Y"/>` na representação XML da cadeia de relacionamentos. A seguir está um exemplo de uma cadeia de relacionamento com um comprimento de um.

```
<openCondition name="RELATIONSHIP_CHAIN">
<parameter name="RELATIONSHIP"
value="aValue"/>
</openCondition>
```

Para cadeias de relacionamentos de comprimento um, o elemento `<parameter name="Relationship" value="something">` especifica um relacionamento direto entre o usuário e o recurso. O atributo do valor é a cadeia representando o relacionamento entre o usuário e o recurso. Isso também deve corresponder ao parâmetro de relacionamento do método `fulfills()` no recurso protectable.

Quando uma cadeia de relacionamento tem um comprimento de dois, ela é uma série de dois relacionamentos. O primeiro ,`<parameter name= "X" value="Y"/>`, elemento está entre o usuário e uma entidade organizacional. O último elemento ,`<parameter name= "X" value="Y"/>`, está entre a entidade organizacional e o recurso. A seguir está um exemplo de uma cadeia de relacionamentos com um comprimento de dois.

```
<openCondition name=RELATIONSHIP_CHAIN">
<parameter name="aValue1" value="aValue2"/>
<parameter name="RELATIONSHIP" value="aValue3"/>
</openCondition>
```

Os possíveis valores `aValue1` incluem `HIERARCHY` e `ROLE`. `HIERARCHY` especifica que há um relacionamento hierárquico entre o usuário e a entidade organizacional na hierarquia da associação. `ROLE` especifica que o usuário exerce a função na entidade organizacional.

Se o valor de aValue1 é HIERARCHY, os valores possíveis incluem filho, que retorna a entidade organizacional para a qual o usuário é um filho direto na hierarquia de membro. Se o valor de aValue1 é ROLE, valores possíveis incluem quaisquer entradas válidas na coluna NAME da tabela ROLE que retorna todas as entidades organizacionais para as quais o usuário atual exerce esta função.

A entrada aValue3 é uma cadeia representando o relacionamento entre uma ou mais entidades organizacionais recuperadas da avaliação do primeiro parâmetro e do recurso. Este valor corresponde ao parâmetro de relacionamento do método fulfills() no recurso protectable. Se mais que uma entidade organizacional for retornada pela avaliação do parâmetro aValue1 , esta parte do RELATIONSHIP_CHAIN é satisfeita se pelo menos uma destas entidades organizacionais satisfizerem o relacionamento especificado pelo parâmetro aValue2.

Nota: Um grupo de relacionamentos que consiste em uma única cadeia de relacionamento com um único elemento de parâmetro é funcionalmente equivalente a um relacionamento simples. Neste caso, é mais fácil utilizar o relacionamento em vez do grupo de relacionamentos na política.

Propriedade de Política e de Recurso

Todas as políticas pertencem a uma entidade organizacional. Todos os recursos de controle de acesso também têm um proprietário que é geralmente uma entidade organizacional; por exemplo, um pedido pertence à organização proprietária da loja onde o pedido foi feito. Usuários também podem possuir recursos; por exemplo, um usuário registrado possui as informações de seu registro de usuário. A propriedade de recursos e de políticas de controle de acesso é importante ao determinar quais políticas devem ser aplicadas a determinado recurso. Para determinado recurso, as políticas que pertencem à sua entidade organizacional e às entidades organizacionais ascendentes do proprietário são aplicadas.

Tipos de Políticas de Controle de Acesso

Existem dois tipos de políticas de controle de acesso:

- Políticas padrão
- Políticas modelo

Políticas padrão

As políticas padrão possuem um proprietário fixo. Por exemplo, se uma política normal pertencer à Organização Vendedora, ela se aplicará apenas aos recursos pertencentes à Organização Vendedora e a recursos pertencentes às entidades organizacionais descendentes, se existirem. Como a Organização Raiz é a organização ascendente de todas as outras organizações no WebSphere Commerce, qualquer política pertencente à Organização Raiz (ID de membro = -2001), por definição se aplica a todos os recursos do site. Assim, as políticas normais pertencentes à Organização Raiz são às vezes mencionadas como políticas de nível de site.

As políticas normais que não pertencem à Organização Raiz são mencionadas como políticas de nível organizacional, pois não se aplicam ao site inteiro, apenas aos recursos pertencentes ao proprietário da política ou a qualquer uma das entidades organizacionais descendentes dele. Um administrador de loja pode gerenciar as políticas para sua própria entidade organizacional e suas entidades organizacionais descendentes. Os administradores do site podem modificar todas as políticas.

Políticas Modelo

As políticas modelo têm um proprietário dinâmico. As políticas modelos se aplicam dinamicamente à entidade organizacional que possui o recurso e suas entidades organizacionais ascendentes. Por exemplo, se existirem 10 organizações sob a Organização Raiz e cada uma desejar assegurar que Administradores de Lojas possam modificar apenas os recursos pertencentes à Organização para a sua função. Existem duas formas de fazer isso:

1. Ter uma política modelo que se aplicará dinamicamente a qualquer uma das 10 organizações, dependendo do recurso que está sendo acessado. O critério para o grupo de acesso na política modelo também pode ser dinâmico. Por exemplo, se um usuário estiver tentando acessar um recurso pertencente à Organização 3, o proprietário da política modelo será alterado dinamicamente para a Organização 3, e o grupo de acesso também passará à Organização 3, ou seja, o usuário deve exercer a função de Administrador de Lojas para a Organização 3.
2. Ter 10 políticas, cada uma pertencente a uma das 10 organizações. O grupo de acesso para a Organização 1 especificaria que o usuário deve exercer a função de Administrador de Lojas para a Organização 1. O grupo de acesso para a Organização 2 especificaria que o usuário deve exercer a função de Administrador de Lojas para a Organização 2, e assim por diante.

A vantagem da primeira solução é existir apenas uma cópia física da política e 10 cópias lógicas. As políticas modelo podem ser gerenciadas por um administrador de site.

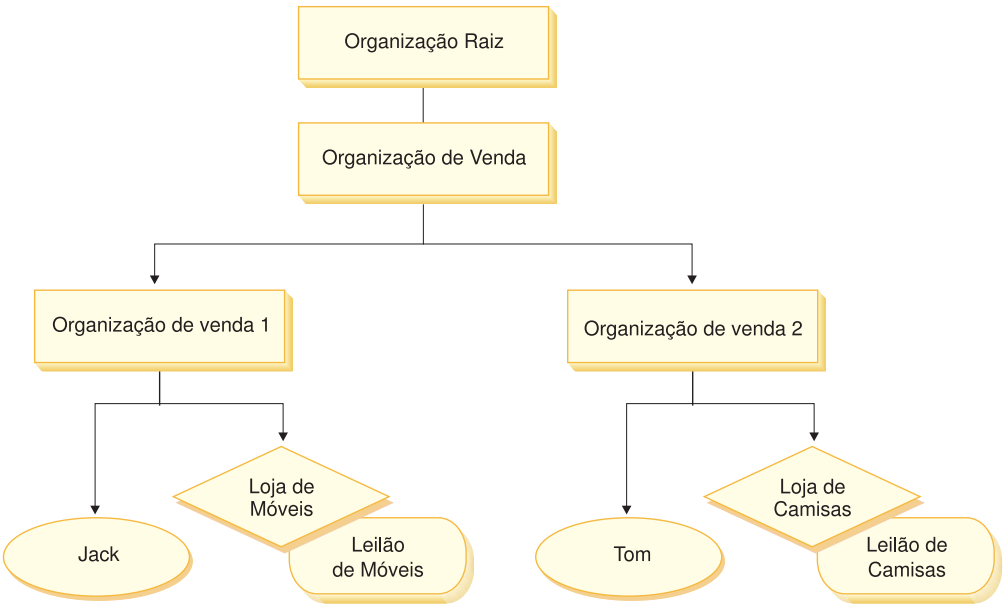
Substituindo Políticas Modelo: Outro recurso de políticas modelo é que elas podem ser substituídas para entidades organizacionais especificadas. Voltando ao exemplo acima, se uma 11a entidade organizacional for incluída no site do WebSphere Commerce, mas esta mais nova entidade organizacional não desejar que a política modelo seja aplicada a ela, existe um meio de especificá-la. Deve ser incluída uma entrada na tabela ACORGPOL, especificando o ID da política modelo e o ID de entidade organizacional da 11ª organização. Isso também pode ser feito através doWebSphere Commerce Administration Console, quando um Administrado de Lojas exclui ou atualiza uma política modelo, no contexto de organização privada.

Ao substituir uma política modelo para uma organização descendente de Organização Raiz,a política modelo ainda se aplicará ao nível de Organização Raiz. Se a política modelo está sendo substituída por uma política mais restritiva no nível de organização descendente, você deve substituir a política modelo no nível de Organização Raiz também. O único jeito de substituir uma política modelo para a Organização Raiz é através do banco de dados, executando o seguinte SQL:

```
insert into ACORGPOL (acpolicy_id, member_id) values ( (select acpolicy_id from
ACPOLICY where policyname = 'policyToOverride'), -2001)
```

Níveis de Controle de Acesso

Existem dois níveis amplos de controle acesso noWebSphere Commerce: nível de comando (também conhecido como baseado em função) e nível de recurso (também conhecido como baseado na instância).



Controle de Acesso Baseado na Função ou no Nível de Comando

O controle de acesso baseado na função ou nível de comando é controle de acesso inferior. Ele determina "quem faz o que". Com o controle de acesso baseado na função, é possível especificar que todos os usuários de uma função específica podem executar determinados tipos de comandos. Considere a política de controle de acesso, Vendedores podem executar comandos de vendedores. Nesta política, um dos comandos de vendedores é o comando `ModifyAuction`. Na figura acima, Jack e Tom são vendedores, então ambos podem modificar leilões.

O controle de acesso baseado em função é utilizado para os comandos e exibições do controlador. Esse tipo de controle de acesso não considera o recurso sobre o qual o comando agiria. Ele apenas determina se o usuário tem permissão para executar um comando ou exibição específica do controlador.

Esse nível de controle de acesso é obrigatório e é reforçado pelo Tempo de Execução. Todos os comandos do controlador devem ser protegidos pelo controle de acesso de nível de comando. Além disso, qualquer exibição que possa ser chamada diretamente ou que possa ser lançada por um redirecionador de outro comando (contrariamente a ser lançada pelo encaminhamento para a exibição) deve ser protegida pelo controle de acesso de nível de comando.

Controle de Acesso de Nível de Comando para Comandos do Controlador: Sempre que um comando do controlador for executado, uma política de controle de acesso deve existir para permitir que os usuários executem a ação `Execute` no recurso do comando. O recurso é o nome da interface do comando do controlador. O grupo de acesso é geralmente passado para uma única função. Por exemplo, você pode especificar que os usuários com a função Representante de Contas podem executar qualquer comando no grupo de recursos `AccountRepresentativesCmdResourceGroup`.

Controle de Acesso de Nível de Comando para Exibições: Quando uma exibição é chamada diretamente da URL ou quando é o resultado de um redirecionamento a partir de um comando, ela deve ter uma política de controle de acesso. Tal política deve ter o `nome da exibição` especificado como uma ação, na tabela

ACACTION. Essa ação deve ser associada a um grupo de ação, utilizando-se a tabela ACACTACTGP. Esse grupo de ação deve ser referenciado na política de nível de comando apropriada, na tabela ACPOLICY.

Controle de Acesso no Nível do Recurso ou Baseado na Instância

As políticas de controle de acesso no nível do recurso ou da instância fornecem controle de acesso gradual, determinando quem pode executar qual comando em quais recursos. O exemplo anterior de uma política de controle de acesso baseado na função, que permite que os Vendedores modifiquem os leilões, pode ser ajustado de foram adequada para que o controle de acesso no nível do recurso seja: Vendedores podem modificar leilões pertencentes à organização pela qual exercem a função. Em 28, Jack tem a função de vendedor para a Organização de Vendedor 1. Tom tem a função de vendedor para a Organização de Vendedor 2. Jack cria um leilão de móveis na loja de móveis. Tom cria um Leilão de Camisas na Loja de Camisas. Jack pode modificar o leilão de móveis, mas *não* o leilão de camisas. Tom pode modificar o leilão de camisas, mas *não* o leilão de móveis.

Para resumir, primeiro o sistema faz uma verificação de acesso no nível do comando. Se o usuário tiver permissão para executar um comando, uma política de controle de acesso no nível do recurso subseqüente será feita para determinar se o usuário pode acessar o recurso em questão.

O controle de acesso de nível de recurso se aplica a comandos e beans de dados.

Controle de Acesso de Nível de Recurso para Comandos: Após a conclusão da verificação do controle de acesso do nível do comando, se o acesso tiver sido concedido, a verificação de nível de recurso será feita em um dos dois casos a seguir:

- O comando implementa `getResources()` — esse método especifica as instâncias de recursos que devem ser verificadas com a ação atual; em que o comando agora é a ação. O WebSphere Commerce Runtime irá assegurar que o usuário atual tenha acesso a todos os recursos especificados pelo `getResources()`. Por padrão, `getResources()` retorna nulo, ou seja, não executa nenhuma verificação de nível de recurso.
- As chamadas de comando `checkIsAllowed(Object Resource, String Action)` — em casos em que o autor do comando não sabe quais recursos devem ser verificados ao mesmo tempo que getResources() é chamado pelo Runtime, o comando pode chamar esse método `checkIsAllowed()`, conforme necessário, para determinar se o par recurso e ação atual é autorizado. O leilão geralmente é o nome da interface do comando atual. Quando esse método for chamado, se o acesso for negado, uma exceção será emitida: `ECApplicationException( ECMessage._ERR_USER_AUTHORITY, ..)`

Controle de Acesso de Nível de Recurso para Beans de Dados: Conforme explicado acima, as exibições são protegidas por políticas de nível de comando, que geralmente são baseadas em funções. Por exemplo, a política de nível de comando pode determinar que um Administrador do Vendedor tenha acesso a uma exibição específica. Geralmente é necessário assegurar que os beans de dados no JSP estejam todos relacionados à organização para a qual o usuário exerce a função de Administrador do Vendedor. Isso é realizado tendo todos os beans de dados que precisam que a proteção (direta ou indiretamente), implemente a interface do Delegador. Estes beans de dados delegam para o bean de dados primário (independente) que por sua vez implementa interface Protectable. Um bean de dados primário delegaria para si mesmo e portanto implementaria ambas as interfaces. Então, sempre que um bean de dados for chamado utilizando o

método `activate()` do Gerenciador de Bean de Dados, o WebSphere Commerce Runtime irá assegurar que exista uma política que conceda ao usuário atual a autoridade para executar a ação `Display` no recurso de beans de dados.

Como o Controle de Acesso Impede Ações não Autorizadas

Esta seção explica como o controle de acesso baseado na política funciona para garantir que os usuários possam executar apenas ações às quais estão autorizados.

Verificando a Autorização antes de Executar uma Ação Iniciada pelo Usuário

O *Gerenciador de Políticas* é o componente de controle de acesso que determina se o usuário atual tem permissão ou não para executar a ação especificada no recurso especificado. As políticas de controle de acesso são especificadas no formato XML. Na instalação, as políticas padrão são carregadas automaticamente nas tabelas de bancos de dados adequadas. Quando o WebSphere Commerce Application Server é iniciado, as informações de controle de acesso são armazenadas em cache na memória para que o Gerenciador de Políticas verifique rapidamente uma autorização do usuário quando chamado para tal tarefa. Se as informações de controle de acesso forem alteradas no banco de dados através do WebSphere Commerce Administration Console, ou carregando os dados de políticas do XML, o armazenamento em cache do controle de acesso precisa ser atualizado. Isso pode ser feito atualizando o registro Controle de Acesso no WebSphere Commerce Administration Console. Reiniciando o WebSphere Commerce também resultará em uma atualização do cache.

Quando um usuário tenta executar uma ação protegida de controle de acesso, uma verificação de controle de acesso será realizada para garantir que o usuário está autorizado. O Gerenciador de Políticas procura por todas as políticas de acesso que se aplicam à organização que possui o recurso. Em seguida verifica tais políticas para avaliar se o usuário está autorizado a executar a ação no recurso de destino. Se houver pelo menos uma política desse tipo, o Gerenciador de Políticas concederá acesso, caso contrário, o negará.

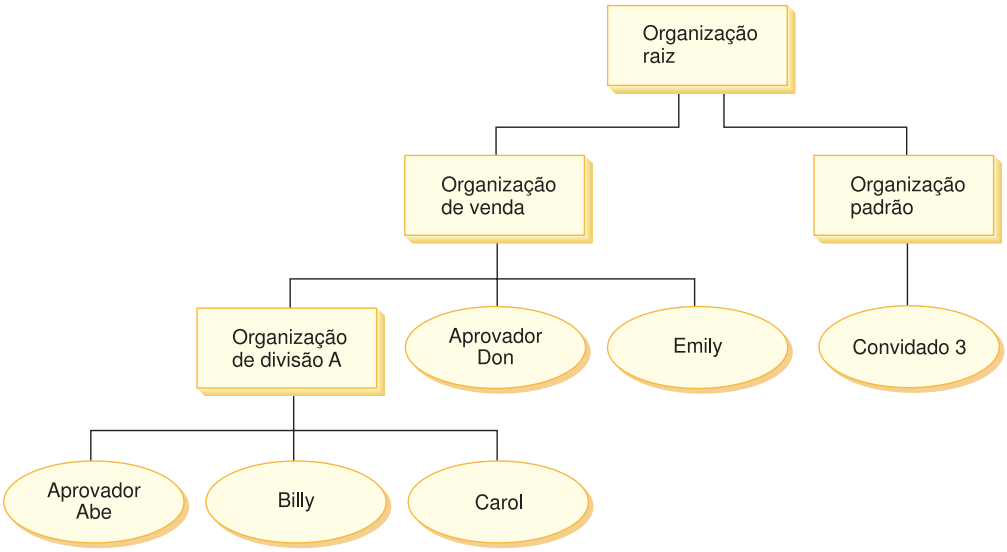
Utilizando o Controle de Acesso

Para obter mais informações sobre as tarefas tais como personalizar políticas de controle de acesso padrão, cenários e como utilizar os arquivos XML para personalizar as políticas de controle de acesso, consulte o site WebSphere Commerce - Manual de Controle de Acesso.

Avaliando as Políticas de Controle de Acesso

Esta seção pode ser utilizada como um guia para avaliar as políticas de controle de acesso. Nesta seção, você é apresentado a um cenário e guiado através de um exemplo de como avaliar um a política de controle de acesso normal e modelo. Cada seção começa com uma descrição de políticas relacionadas e cenários utilizando cada política. Para obter mais informações sobre políticas normais e modelos, consulte “Tipos de Políticas de Controle de Acesso” na página 26.

O seguinte diagrama exibe graficamente o cenário:



Hierarquia Organizacional

No diagrama, é possível ver as quatro organizações seguintes que estão no site:

- Organização Raiz
- Organização do Vendedor
- Organização Padrão
- Organização de Divisão A

Como você pode ver, a organização raiz é pai da Organização de vendedor e da organização padrão. A organização de vendedor é pai da organização de Divisão A

Usuários

No diagrama, Don e Emily estão registrados na Organização de Vendedores. Abe, Billy e Carol estão registrados na organização de Divisão A. O convidado 3 não está registrado, mas para fins de controle de acesso, pertence implicitamente à Organização Padrão.

Funções

Don tem a função de aprovador para a Organização de Vendedores. Abe tem a função de aprovador para a Organização de Divisão A.

Grupos de Acesso

Os seguintes grupos de acesso são utilizados neste cenário:

- Usuários registrados: Este grupo inclui implicitamente todos os usuários que estão registrados.
- Aprovadores para Vendedor: Este grupo inclui implicitamente todos os usuários que têm a função de aprovadores para a Organização de Vendedores.
- Aprovadores para a Divisão A: Este grupo inclui implicitamente todos os usuários que têm a função de aprovador para a organização de Divisão A.

Documentos

O objeto do documento é um recurso protegido. O proprietário de um documento é definido para ser a organização onde ele foi criado.

Requisitos de controle de acesso para atualizar documentos

A seguir estão os requisitos de controle de acesso para atualizar documentos:

1. Os usuários registrados podem atualizar um documento do qual são criadores.
2. Aprovadores para a Divisão A podem atualizar documentos pertencentes à Divisão A, mas não documentos pertencentes ao Vendedor. Aprovadores para a Organização de Vendedores podem atualizar documentos pertencentes às duas organizações, Divisão A e de Vendedores.

Avaliando Políticas Normais

Esta seção leva você pelas políticas normais e pelos cenários a fim de avaliá-los.

Políticas de controle de acesso relacionadas à atualização de documento

A seguir está o formato da política e as políticas de controle de acesso relacionados à atualização de documentos:

Formato da Política: `[Grupo de Acesso, Grupo de Ação, Grupo de Recurso, Relacionamento]`

Política 1:

```
[Usuários Registrados, Executar Grupo de Ação de Comando, Atualizar Documento
Grupo de Recurso, - ]
```

Esta é uma política normal baseada na função pertencente à Organização Raiz. Nesta política, os usuários registrados podem executar os comandos `Atualizar Documento`.

Política 2:

```
[Usuários Registrados, Atualizar Grupo de Ação de Documento, documento, criador ]
```

Esta é uma política normal baseada na função pertencente à Organização Raiz. Nesta política, os usuários registrados podem atualizar um documento se forem os criadores daquele documento.

Política 3:

```
[Aprovadores para Vendedor, Atualizar Grupo de Ação de Documento, documento, - ]
```

Esta é uma política normal de nível de recurso pertencente à Organização de Vendedores. Nesta política, os aprovadores para os Vendedores podem atualizar documentos que pertencem aos Vendedores.

Política 4:

```
[Aprovadores para Vendedor, Atualizar Grupo de Ação de Documento, documento, - ]
```

Esta é uma política normal baseada na função pertencente à Organização de Divisão A. Nesta política, os Aprovadores para a Divisão A podem atualizar documentos pertencentes à Divisão A.

Cenários

Cenário 1 : Billy tenta atualizar seu próprio documento: A seguir está a avaliação de controle de acesso para este cenário:

Comando - verificação de nível:

1. Não existe nenhum ID de loja especificado, então o proprietário do comando é definido como Organização Raiz. Assim, somente políticas pertencentes à Organização Raiz serão utilizadas para avaliar se o usuário tem acesso de nível de comando: políticas 1 e 2 pertencem à Organização Raiz.
2. A Política 1 concede acesso, desde que Billy seja um membro do grupo de acesso Usuários Registrados e esteja executando a ação `Executar` no recurso de comando `Atualizar Documento`.

Recurso - verificação de nível:

1. O comando `Atualizar Documento` especifica que o recurso de documento deve ser protegido. O documento de Billy pertence à Divisão A. Assim, somente as políticas pertencentes à Divisão A e suas organizações ascendentes se aplicarão: políticas 1, 2, 3 e 4.
2. A política 2 concede acesso desde que Billy seja um membro do grupo de acesso Usuários Registrados, esteja executando a ação de comando `Atualizar Documento` no recurso de documento e atenda o relacionamento de criador do documento.

Desde que Billy tenha passado pelas duas verificações de controle de acesso de nível de comando e de recurso, ele pode atualizar seu próprio documento.

Cenário 2: Don tenta atualizar o documento da Carol: A seguir está a avaliação de controle de acesso para este cenário:

Comando - verificação de nível:

1. Não existe nenhum ID de loja especificado, então o proprietário do comando é definido como Organização Raiz. Assim, somente políticas pertencentes à Organização Raiz serão utilizadas para avaliar se o usuário tem acesso de nível de comando: políticas 1 e 2 pertencem à Organização Raiz.
2. A Política 1 concede acesso, desde que Don seja um membro do grupo de acesso Usuários Registrados e esteja executando a ação `Executar` no recurso de comando `Atualizar Documento`.

Recurso - verificação de nível:

1. O comando `Atualizar Documento` especifica que o recurso de documento deve ser protegido. O documento de Carol pertence à Divisão A. Assim, somente as políticas pertencentes à Divisão A e suas organizações ascendentes se aplicarão: políticas 1, 2, 3 e 4.
2. A política 4 concede acesso desde que Don seja um membro do grupo de acesso Aprovadores para Vendedores, esteja executando a ação de comando `Atualizar Documento` no recurso de documento.

Desde que Don tenha passado pelas duas verificações de controle de acesso de nível de comando e de recurso, ele pode atualizar o documento da Carol.

Cenário 3: Abe tenta atualizar o documento de Emily: A seguir está a avaliação de controle de acesso para este cenário:

Comando - verificação de nível:

1. Não existe nenhum ID de loja especificado, então o proprietário do comando é definido como Organização Raiz. Assim, somente políticas pertencentes à Organização Raiz serão utilizadas para avaliar se o usuário tem acesso de nível de comando: políticas 1 e 2 pertencem à Organização Raiz.

2. A Política 1 concede acesso, desde que Abe seja um membro do grupo de acesso Usuários Registrados e esteja executando a ação `Executar` no recurso de comando `Atualizar Documento`.

Recurso - verificação de nível:

1. O comando `Atualizar Documento` especifica que o recurso de documento deve ser protegido. O documento da Emily pertence à Organização de Vendedores. Assim, somente as políticas pertencentes à Organização de Vendedores e suas organizações ascendentes se aplicarão: políticas 1, 2 e 3.
2. A política 3 NÃO concede acesso desde que Abe NÃO seja um membro dos Aprovadores do grupo de acesso de Vendedores.

Embora Abe tenha passado na verificação do nível de comando, mas falhou na verificação do controle de acesso no nível de recurso, ele não pode atualizar o documento de Emily.

Cenário 4:Convidado 3 tenta atualizar seu próprio documento: A seguir está a avaliação de controle de acesso para este cenário:

Comando - verificação de nível:

1. Não existe nenhum ID de loja especificado, então o proprietário do comando é definido como Organização Raiz. Assim, somente políticas pertencentes à Organização Raiz serão utilizadas para avaliar se o usuário tem acesso de nível de comando: políticas 1 e 2 pertencem à Organização Raiz.
2. A política 1 NÃO concede acesso, desde que o convidado 3 NÃO seja um membro do grupo de acesso `Usuários Registrados` .

Recurso - verificação de nível:

1. A verificação de nível de recurso NÃO foi executada pois a verificação do nível de comando falhou

Uma vez que o convidado 3 falhou na verificação do nível de comando, ele não pode atualizar seu próprio documento.

Avaliando Políticas Modelos

Este exemplo é baseado no cenário anterior.

Políticas de controle de acesso relacionadas à atualização de documento

Ao avaliar políticas modelos, as políticas de controle de acesso 1 e 2 utilizadas para avaliar políticas normais ainda se aplicam, porém, as políticas normais 3 e 4 são substituídas pela política modelo 5. Para obter mais informações sobre políticas 1 e 2 consulte "Avaliando Políticas Normais" na página 32.

Política 5:

```
[Aprovadores para Organização, Atualizar Grupo de Ação de Documento, documento, - ]
```

Esta política é uma política modelo de nível de recurso. Os aprovadores para a organização que possui o documento podem atualizar os documentos.

Também precisamos de um novo grupo de acesso com parâmetros para ser utilizado por esta política modelo. O seguinte grupo de acesso foi incluído neste cenário:

- Aprovadores para Organização: Este grupo inclui implicitamente todos os usuários que possuem a função de aprovador para a organização ? . (o

parâmetro ? será alterado dinamicamente para o proprietário da política, à medida que a política modelo for aplicada no tempo de execução).

Cenários

Os seguintes cenários utilizam políticas 1, 2, e 5 somente.

Cenário 1: Don tenta atualizar o documento da Carol: A seguir está a avaliação de controle de acesso para este cenário:

Comando - verificação de nível:

1. Não existe nenhum ID de loja especificado, então o proprietário do comando é definido como Organização Raiz. Assim, somente políticas pertencentes à Organização Raiz serão utilizadas para avaliar se o usuário tem acesso de nível de comando: políticas 1 e 2 pertencem à Organização Raiz. Durante a avaliação da política, as políticas modelos alteram dinamicamente a propriedade para a organização que possui o recurso e subseqüentemente aqueles ascendentes da organização, então a política 5 também se aplicará.
2. A Política 1 concede acesso, desde que Don seja um membro do grupo de acesso Usuários Registrados e esteja executando a ação `Executar` no recurso de comando `Atualizar Documento`.

Recurso - verificação de nível:

1. O comando `Atualizar Documento` especifica que o recurso de documento deve ser protegido. O documento de Carol pertence à Divisão A. Assim, somente as políticas pertencentes à Divisão A e suas organizações ascendentes se aplicarão: políticas 1 e 2. Durante a avaliação da política, as políticas modelos alteram dinamicamente a propriedade para a organização que possui o recurso e subseqüentemente aqueles ascendentes da organização, então a política 5 também se aplicará.
2. A política modelo 5 é aplicada primeiro à organização que possui o recurso: Divisão A. Neste momento, a política 5 se comporta essencialmente como a política 5a:

   ```
   [Aprovadores para Divisão A, Atualizar Grupo de Ação de Documento,
   documento, - ] normal política de nível de recurso pertencente à Divisão A.
   ```

3. A política 5a NÃO concede acesso desde que Don NÃO seja um membro do grupo de acesso Aprovadores para a Divisão A.
4. A política modelo 5 será depois aplicada à organização pai da Divisão A: Organização de Vendedores. Neste momento, a política 5 se comporta essencialmente como a política 5b:

   ```
    [Aprovadores para Vendedor, Atualizar Grupo de Ação de Documento,
   documento, - ]normal política de nível de recurso pertencente aos Vendedores.
   ```

5. A política 5b concede acesso desde que Don seja um membro do grupo de acesso Aprovadores para Vendedores, esteja executando a ação de comando `Atualizar Documento` no recurso de documento.

Desde que Don tenha passado pelas duas verificações de controle de acesso de nível de comando e de recurso, ele pode atualizar o documento da Carol.

Cenário 2: Abe tenta atualizar documento de Emily: A seguir está a avaliação de controle de acesso para este cenário:

Comando - verificação de nível:

1. Não existe nenhum ID de loja especificado, então o proprietário do comando é definido como Organização Raiz. Assim, somente políticas pertencentes à Organização Raiz serão utilizadas para avaliar se o usuário tem acesso de nível

de comando: políticas 1 e 2 pertencem à Organização Raiz.Durante a avaliação da política, as políticas modelos alteram dinamicamente a propriedade para a organização que possui o recurso e subseqüentemente aqueles ascendentes da organização, então a política 5 também se aplicará.

2. A Política 1 concede acesso, desde que Abe seja um membro do grupo de acesso Usuários Registrados e esteja executando a ação `Executar` no recurso de comando `Atualizar Documento`.

Recurso - verificação de nível:

1. O comando `Atualizar Documento` especifica que o recurso de documento deve ser protegido. O documento da Emily pertence à Organização de Vendedores. Assim, somente as políticas pertencentes aos Vendedores e suas organizações ascendentes se aplicarão: políticas 1 e 2. Durante a avaliação da política, as políticas modelos alteram dinamicamente a propriedade para a organização que possui o recurso e subseqüentemente aqueles ascendentes da organização, então a política 5 também se aplicará.
2. A política modelo 5 é aplicada primeiro à organização que possui o recurso: Organização de Vendedores. Neste momento, a política 5 se comporta essencialmente como a política 5a:

   ```
   [Aprovadores para Vendedor, Atualizar Grupo de Ação de Documento,
   documento, - ]política normal de nível de recurso pertencente aos Vendedores.
   ```

3. A política 5a NÃO concede acesso desde que Abe NÃO seja um membro do grupo de acesso Aprovadores para os Vendedores.
4. A política modelo 5 será depois aplicada à organização pai da organização de vendedores: Organização raiz. Neste momento, a política 5 se comporta essencialmente como a política 5b:

   ```
   [Aprovadores para Raiz, Atualizar Grupo de Ação de Documento,
   documento, - ] política normal de nível de recurso pertencente à Raiz
   ```

5. A política 5b NÃO concede acesso desde que Abe NÃO seja um membro do grupo de acesso Aprovadores para Raiz.
6. A organização raiz não possui uma organização pai, assim a política modelo 5 foi completamente avaliada.

Embora Abe tenha passado na verificação do nível de comando, mas falhou na verificação do controle de acesso no nível de recurso, ele não pode atualizar o documento de Emily.

Parte 2. Tarefas de Segurança do Administrador do Site do WebSphere Commerce

Essa parte descreve as tarefas de segurança que geralmente podem ser executadas pelo administrador do site do WebSphere Commerce.

Capítulo 4. Aprimorando a Segurança do Site

Para aprimorar a segurança do seu site doWebSphere Commerce, você pode ativar qualquer um dos seguintes recursos no Gerenciador de Configuração do WebSphere Commerce:

- Efetue logoff como um usuário que está inativo por um período estendido e solicite que ele efetue logon no sistema novamente, utilizando o nó Tempo Limite de Login. Para obter detalhes, consulte "Ativando o Tempo Limite de Login" na página 42.
- Solicite aos usuários que alterem suas senhas quando estiverem efetuando login no sistema pela primeira vez, utilizando o nó Invalidação de Senha. Para obter detalhes, consulte "Ativando a Invalidação de Senha" na página 43.
- Solicite aos usuários que digitem suas senhas se estiverem executando pedidos que executam comandos designados, utilizando o nó Comandos Protegidos por Senha. Para obter detalhes, consulte "Ativando os Comandos Protegidos por Senha" na página 44.
- Atualize dados criptografados, como senhas e informações do cartão de crédito, bem como a chave do comerciante em um banco de dados WebSphere Commerce, utilizando o nó Ferramenta de Atualização do Banco de Dados. Para obter detalhes, consulte "Atualizando os Dados Criptografados" na página 45.
- Rejeite qualquer pedido de usuário que contenha atributos ou caracteres designados como não permitidos, utilizando o nó Proteção de Script Entre Sites. Para obter detalhes, consulte "Ativando a Proteção de Script Entre Sites" na página 46.
- Identifique rapidamente todas as ameaças de segurança contra o WebSphere Commerce ativando o log de acesso. Para obter detalhes, consulte "Ativando o Log de Acesso" na página 48.

Além disso, é possível ativar os seguintes recursos do drop down Segurança no WebSphere Commerce Administration Console:

- Configure uma política de contas para o site para definir as políticas relacionadas às contas em uso, utilizando a página Política de contas. Para obter detalhes, consulte "Configurando uma Política de Contas" na página 49.
- Configure uma política de senha para que seu site controle as características de seleção de senha de um usuário utilizando a página Política de senhas (somente se os usuários estiverem autenticados junto ao banco de dados do WebSphere Commerce). Para obter detalhes, consulte "Configurando uma Política de Senhas" na página 50.
- Configure uma política de bloqueio de contas para que seu site reduza as chances de uma conta de usuário ficar comprometida, utilizando a página Política de bloqueio de contas (somente se os usuários estiverem autenticados junto ao banco de dados do WebSphere Commerce). Para obter detalhes, consulte "Configurando uma Política de Bloqueio de Contas" na página 51.
- Lance um programa de segurança que verifica e exclui arquivos temporários doWebSphere Commerce que podem conter exposições de segurança potenciais utilizando a página Lançar verificação de segurança. Para obter detalhes, consulte "Lançando uma Verificação de Segurança" na página 52.

Para obter mais informações sobre conceitos relacionados, consulte os seguintes tópicos na ajuda online do WebSphere Commerce:

- Gerenciador de Configuração
- Arquivo de configuração do WebSphere Commerce
- Administration Console
- Segurança

Para obter informações sobre tarefas relacionadas, consulte os seguintes tópicos na ajuda online do WebSphere Commerce.

- Lançar o Gerenciador de Configuração
- Abrir o Administration Console

Exibições de Segurança

Antes de utilizar determinados recursos de segurança do WebSphere Commerce, você será solicitado a definir as exibições associadas de sua loja antes que possa utilizar esse recurso. As informações a seguir descrevem como definir as exibições para:

- Tempo limite de login (consulte "Tempo Limite de Login")
- Invalidação de senha (consulte "Invalidação de Senha" na página 41)
- Comandos protegidos por senha (consulte "Comandos Protegidos por Senha" na página 41)
- Proteção de script entre sites (consulte "Proteção de Scripts entre Sites" na página 42)

Para obter informações gerais sobre a criação de exibições e o desenvolvimento da fachada da loja, consulte o *Manual do Desenvolvedor da Loja*.

Tempo Limite de Login

Para utilizar o recurso de segurança de tempo limite de login, você precisa definir as exibições LoginTimeoutErrorView e ReLogonFormView para sua loja.

LoginTimeoutErrorView

Se as informações de tempo limite de login estiverem incorretas, o WebSphere Commerce redirecionará o navegador do usuário para essa exibição. Se isso ocorrer, provavelmente será porque uma pessoa violou o cookie.

Tabela 1. Atributos de LoginTimeoutErrorView

ECConstants.EC_LOGIN_TIMEOUT_ ERROR_MSGCODE	
	1 O tempo de expiração está definido com valor errado.
	2 O tempo de logon está definido com o valor errado.
	3 Tempo de expiração ou logon definido com o valor errado.

ReLogonFormView

Essa exibição é exibida para usuários após a sessão ter expirado. Ela precisa fornecer ao usuário um formulário de entrada do ID de logon e senha do usuário. O botão submeter chamará o comando Logon. Também deve haver um botão Cancelar para redirecionar o usuário para outra página, na maioria dos casos, a página da fachada da loja.

Não existem atributos para ReLogonFormView.

Tabela 2. Atributos de formulário de ReLogonFormView

ECUserConstants.EC_UREG_LOGONID	O id de logon do usuário.
ECUserConstants.EC_UREG_LOGON PASSWORD	A senha de logon do usuário.

Tabela 2. Atributos de formulário de ReLogonFormView (continuação)

ECUserConstants.EC_RELOGIN_URL	A URL que será exibida se as credenciais fornecidas forem inválidas. Na maioria dos casos, será o nome dessa exibição.
ECConstants.EC_STORE_ID	O identificador da loja.
ECConstants.EC_URL	A URL que é exibida quando as credenciais inseridas pertencem a um usuário diferente. Na maioria dos casos, deve ser uma home page da loja ou a mesma URL que foi utilizada em uma página de logon da loja.

Invalidação de Senha

Para utilizar o recurso de segurança de invalidação de senha, você precisa definir a exibição ChangePassword para sua loja.

ChangePassword

Essa exibição será exibida se uma senha de usuário tiver expirado. Ela deve fornecer ao usuário um formulário de entrada da senha atual (expirada) e da nova senha. O botão Submeter chama o comando ResetPassword. Também deve haver um botão Cancelar que redireciona o usuário para outra página, na maioria dos casos, a página da fachada da loja.

Tabela 3. Atributos de ChangePassword

ECConstants.EC_PASSWORD_EXPIRED_ FLAG	**1**	A senha do usuário expirou. Esse atributo é necessário para distinguir essa exibição da exibição utilizada para o recurso de alteração de senha, pois elas são iguais. A exibição para a alteração de senha poderá ser chamada por um usuário e a JSP (JavaServer Pages) atribuída a essa exibição deverá ser o mesma para ambos os casos. A JSP deve procurar esse atributo para decidir o que exibir.
	null	O atributo não está em uma URL . Esse é o comportamento normal de alteração de senha.
ECUserConstants.EC_UREG_LOGONID	O id de logon do usuário atual.	
ECConstants.EC_LOGIN_RETURN_URL	A URL à qual o navegador é redirecionado após uma alteração de senha bem-sucedida. Essa URL será transmitida para um comando de ação com o nome ECConstants.EC_URL.	

Tabela 4. Atributos de formulário de ChangePassword

ECUserConstants.EC_UREG_LOGONID	O ID de logon do usuário. O ID de logon atual foi passado para a exibição.
ECUserConstants.EC_UREG_LOGON PASSWORDOLD	A senha antiga.
ECUserConstants.EC_UREG_LOGON PASSWORD	A nova senha.
ECUserConstants.EC_UREG_LOGON PASSWORDVERIFY	A verificação da nova senha.
ECConstants.EC_URL	A URL na qual os usuários são redirecionados após uma alteração de senha bem-sucedida. O valor foi passado para a exibição.
ECUserConstants.EC_RELOGIN_URL	A URL na qual o navegador foi redirecionado se a alteração de senha não tiver sido bem-sucedida.

Comandos Protegidos por Senha

Para utilizar o recurso de segurança de comandos protegidos por senha, você precisa definir as exibições PasswordReEnterErrorView e PasswordReEnterFormView para sua loja.

PasswordReEnterErrorView

Essa exibição é utilizada nos seguintes cenários:

- Um usuário não fornece a senha correta e é efetuado logoff.
- A autenticação falhou.

Em ambos os casos, o usuário deve ter uma forma de continuar para a outra página através de um link na página atual.

Tabela 5. Atributos de PasswordReEnterErrorView

ECConstants.EC_PASSWORD_REREQUEST_ MSGCODE		
	0	Ocorreu um problema ao tentar autenticar o usuário.
	null	O atributo não está em uma URL . O usuário falhou ao fornecer a senha e foi efetuado logoff.

PasswordReEnterFormView

Essa exibição é exibida quando o usuário tenta executar um comando protegido por senha. Ela deve fornecer ao usuário um formulário de entrada de senha. Devem haver dois campos de entrada para a senha.

Tabela 6. Atributos de PasswordReEnterFormView

ECConstants.EC_PASSWORD_REREQUEST_ URL	A URL está em execução utilizando o botão Submeter do formulário.
ECConstants.EC_PASSWORD_REREQUEST_ MSGCODE	O código de mensagem especificando a mensagem que é mostrada ao usuário:
1	As senhas que foram digitadas não correspondem.
2	A senha não foi digitada.
3	Uma senha incorreta foi digitada.

AÇÃO: A URL é transmitida como um parâmetro chamado:

Tabela 7. Atributos de formulário de PasswordReEnterFormView

ECConstants.EC_PASSWORD_REREQUEST_ PASSWORD1	A primeira senha.
ECConstants.EC_PASSWORD_REREQUEST_ PASSWORD2	A segunda senha.

Proteção de Scripts entre Sites

Para utilizar o recurso de segurança de script entre sites, você precisa definir as exibições ProhibitedAttrsErrorView, ProhibitedCharacterErrorView e ProhibCharEncodingErrorView para sua loja.

ProhibitedAttrsErrorView
Essa exibição é mostrada ao usuário quando o pedido não é processado, porque ele continha atributos proibidos.

ProhibitedCharacterErrorView
Essa exibição é mostrada ao usuário quando o pedido não é processado, porque ele continha caracteres proibidos.

ProhibCharEncodingErrorView
Igual à exibição ProhibitedCharacterErrorView acima.

Ativando o Tempo Limite de Login

Nota: Para utilizar o recurso de segurança de tempo limite de login para uma loja, você precisa definir as exibições LoginTimeoutErrorView e ReLogonFormView para a loja conforme descrito em "Tempo Limite de Login" na página 40.

Utilize o nó Tempo Limite de Login do Gerenciador de Configuração para ativar ou desativar o recurso de tempo limite de login. Quando este recurso for ativado, um usuário do WebSphere Commerce que estiver inativo por um período de tempo estendido tem sua sessão encerrada no sistema e é solicitado que ele inicie a sessão novamente. Se depois o usuário iniciar a sessão com êxito, o WebSphere

Commerce executará o pedido original feito pelo usuário. Se o logon do usuário falhar, o pedido original será descartado e o usuário permanecerá com logoff no sistema.

Note que para as ferramentas do WebSphere Commerce (como o Console de Administração, o WebSphere Commerce Accelerator, Store Services e assim por diante), o recurso de tempo limite de login não apresenta uma página de novo login ao usuário. Em vez disso, ele fecha a janela do navegador e fica por conta do usuário efetuar logon novamente na ferramenta. Portanto, no caso de ferramentas, o pedido original que o usuário submete não é processado.

Para ativar este recurso:

1. Lance o Gerenciador de Configuração e vá para o nó de Tempo Limite de Login para a sua instância como segue: **WebSphere Commerce >** *host_name* **> Lista de Instâncias >** *instance_name* **> Propriedades da Instância > Tempo Limite de Login**
2. Para ativar o recurso de tempo limite de login, clique na caixa de opção **Ativar**.
3. Digite o valor de tempo limite de login, em segundos, no campo Valor.
4. Para aplicar suas alterações no Gerenciador de Configuração, clique em **Aplicar**.
5. Depois de atualizar com êxito a configuração de sua instância, você receberá uma mensagem indicando uma atualização com êxito.
6. No WebSphere Application Server Administration Console, pare e, em seguida, reinicie a instância do WebSphere Commerce Server.

Observe que o valor do tempo limite de login é armazenado no arquivo *instance*.xml em milissegundos, enquanto o valor no Gerenciador de Configuração é inserido em segundos.

Ativando a Invalidação de Senha

Nota: Para utilizar o recurso de segurança de invalidação de senha, você precisa definir a exibição ChangePassword para sua loja conforme descrito em "Invalidação de Senha" na página 41.

Utilize o nó Invalidação de Senha do Gerenciador de Configuração para ativar ou desativar o recurso de invalidação de senha. A invalidação de senha, quando ativada, requer que os usuários do WebSphere Commerce alterem suas senhas, se a senha do usuário tiver expirado. Nesse caso, o usuário será redirecionado para uma página onde será solicitada a alteração de sua senha. Os usuários não podem acessar nenhuma página segura no site até que tenham alterado sua senha. Para ativar este recurso:

1. Lance o Gerenciador de Configuração e vá para o nó de Invalidação de Senha para sua instância da seguinte maneira: **WebSphere Commerce >** *host_name* **> Lista de Instâncias >** *instance_name* **> Propriedades da Instância > Invalidação da Senha**
2. Para ativar o recurso de invalidação de senha, clique na caixa de opções **Ativar**.
3. Para aplicar suas alterações no Gerenciador de Configuração, clique em **Aplicar**.
4. Depois de atualizar com êxito a configuração de sua instância, você receberá uma mensagem indicando uma atualização com êxito.
5. No WebSphere Application Server Administration Console, pare e, em seguida, reinicie a instância doWebSphere Commerce Server.

Ativando os Comandos Protegidos por Senha

Nota: Para utilizar o recurso de segurança de comandos protegidos por senha, você precisa definir as exibições PasswordReEnterErrorView e PasswordReEnterFormView para sua loja conforme descrito em "Comandos Protegidos por Senha" na página 41.

Utilize o nó Comandos Protegidos por Senha do Gerenciador de Configuração para ativar ou desativar o recurso de comandos protegidos por senha. Quando este recurso é ativado, o WebSphere Commerce requer que os usuários registrados que efetuaram logon no WebSphere Commerce digitem sua senha antes de continuar um pedido que executa comandos designados do WebSphere.

Cuidado: Ao configurar comandos protegidos por senha, alguns dos comandos mostrados na lista de seleção de comandos podem ser executados por usuários genéricos ou convidados. A configuração de tais comandos como protegidos por senha restringirá os usuários genéricos e convidados de executá-los. Portanto, você deve ter cuidado ao configurar comandos a serem protegidos por senha.

Para ativar este recurso:

1. Lance o Gerenciador de Configuração e vá para o nó de Comandos Protegidos por Senha para sua instância da seguinte maneira: **WebSphere Commerce>** *host_name* **> Lista de Instâncias >** *instance_name* **> Propriedades da Instância > Comandos Protegidos por Senha**
2. Na guia Geral:
   a. Para ativar o recurso de comandos protegidos por senha, clique em **Ativar**.
   b. Digite o número de repetições no campo Repetições. (O número padrão de repetições é 3).
3. Na guia Avançado:
   a. Selecione um comando do WebSphere Commerce que deseja proteger a partir da lista na janela Lista de Comandos Protegidos por Senha e clique em **Incluir**. O comando selecionado é listado na janela Lista Atual Protegida por Senha.
   b. Se desejar desativar a proteção por senha para qualquer comandoWebSphere Commerce, selecione o comando na janela Lista Atual de Comandos Protegidos por Senha e clique em **Remover**.
4. Para aplicar suas alterações no Gerenciador de Configuração, clique em **Aplicar**.
5. Depois de atualizar com êxito a configuração de sua instância, você receberá uma mensagem indicando uma atualização com êxito.
6. No WebSphere Application Server Administration Console, pare e, em seguida, reinicie a instância WebSphere Commerce Server.

Nota: O WebSphere Commerce exibirá somente os comandos que são designados como `autenticados` ou definidos com o sinalizador `https` na tabela `URLREG` na lista de comandos disponíveis.

Atualizando os Dados Criptografados

Utilize a Ferramenta de Atualização do Banco de Dados disponível no nó Banco de Dados do Gerenciador de Configuração para atualizar todos os dados criptografados (por exemplo, senhas ou números de cartões de crédito), bem como a chave do comerciante em um banco de dados do WebSphere Commerce para uma determinada instância. Para utilizar a ferramenta:

1. Lance o Gerenciador de Configuração e vá para a sua entrada de banco de dados específica, da seguinte maneira: **WebSphere Commerce>** *host_name* **> Lista de Instâncias >** *instance_name* **> Propriedades da Instância > Banco de Dados >** *database_name*
2. Clique com o botão direito do mouse em *database_name* e selecione **Executar Ferramenta de Atualização de Banco de Dados**
   - Selecione **Atualizar todos os bancos de dados para essa instância** para migrar dados criptografados para todos os bancos de dados da instância selecionada.

     400 Como o iSeries suporta uma única configuração de banco de dados, esta opção não se aplica ao iSeries.
   - Selecione **Atualizar banco de dados selecionado** para migrar os dados criptografados para um banco de dados específico, selecionando o banco de dados na lista drop down (padrão).
3. Selecione uma ação que você deseja executar na caixa Item de Ação e preencha as informações necessárias no campo Parâmetro:

Ações	Parâmetros	Ação Necessária
Alterar Chave do Comerciante	Chave do Comerciante Antiga	Digite sua chave de comerciante antiga que utilizou quando criou a instância atual do WebSphere Commerce.
	Nova Chave do Comerciante	Insira sua nova chave do comerciante. É o número hexadecimal de 16 dígitos para o Gerenciador de Configuração criptografar novamente os dados atualmente criptografados. A Chave do Comerciante deve ter pelo menos um caracter alfanumérico (a até f) e pelo menos um caracter numérico (0 até 9). Qualquer caracter alfanumérico deve ser digitado com letras minúsculas e você não pode digitar o mesmo caracter mais que quatro vezes seguidas.

4. Clique em **OK** para executar a ferramenta de atualização do banco de dados no banco de dados selecionado do WebSphere Commerce ou em todos os bancos de dados do WebSphere Commerce.
5. Depois de atualizar com êxito a configuração de sua instância, você receberá uma mensagem indicando uma atualização com êxito.
6. No WebSphere Application Server Administration Console, pare e, em seguida, reinicie a instância do WebSphere Commerce Server.

Ativando a Proteção de Script Entre Sites

Nota: Para utilizar o recurso de segurança de script entre sites para uma loja, é necessário definir as exibições `ProhibitedAttrsErrorView`, `ProhibitedCharacterErrorView` e `ProhibCharEncodingErrorView` para a loja conforme descrito em "Proteção de Scripts entre Sites" na página 42.

Utilize o nó de Proteção de Script Entre Sites do Gerenciador de Configuração para ativar ou desativar a proteção de script entre sites para a sua instâncias. Quando ativada, a proteção de script entre sites rejeita quaisquer pedidos do usuário que contenham atributos ou cadeias que estejam designados como não permitidos. Você pode especificar os atributos e cadeias não permitidos neste nó do Gerenciador de Configuração. E também pode excluir comandos de proteção de script entre sites permitindo que os valores de atributos especificados para esse comando específico contenham cadeias proibidas. A proteção de script entre sites fica desativada por padrão.

Aviso: A proteção de script entre sites é um recurso restritivo no qual a execução dos comandos será restrita com base na configuração. O recurso não verifica quais atributos ou cadeias foram definidas como proibidas, portanto quando você os configurar, certifique-se de que os atributos proibidos não sejam aqueles utilizados pelos comandos. Também certifique-se de que as cadeias proibidas não sejam os valores normalmente transmitidos aos comandos. Tome bastante cuidado ao configurar esse recurso.

Para ativar este recurso:

1. Lance o Gerenciador de Configuração e vá para o nó de Proteção de Script Entre Sites para a sua instância da seguinte forma: **WebSphere Commerce>** *host_name* **> Lista de Instâncias >** *instance_name* **> Propriedades da Instância > Proteção de Script Entre Sites**
2. Utilize a guia Geral para ativar o recurso de proteção cruzada de script do site, da seguinte forma:
   a. Clique em **Ativar**.
   b. Para incluir atributos que deseja rejeitar para os comandosWebSphere Commerce, clique com o botão direito na tabela Atributos Proibidos e selecione **Incluir linha**. Digite o atributo que você deseja rejeitar. Você só pode especificar um atributo por linha.
   c. Para remover atributos da tabela Atributos Proibidos, destaque e clique com o botão direito do mouse na linha que contém o atributo na tabela e selecione **Excluir linha**.
   d. Para incluir cadeias que deseja rejeitar para os comandos do WebSphere Commerce, clique no botão direito na tabela Caracteres Proibidos e selecione **Incluir linha**. Inclua a cadeia que você deseja rejeitar. Você só pode especificar uma cadeia por linha.
   e. Para remover caracteres da tabela Caracteres Proibidos, destaque e clique com o botão direito do mouse na linha que contém o caracter na tabela Caracteres Proibidos e selecione **Excluir linha**.

   Nota: As seguintes cadeias são especificadas por padrão nos campos de caracteres proibidos. Essas cadeias são mais comumente utilizadas como tags de script em ataques maliciosos a scripts entre sites:
   - `<SCRIPT`
   - `&lt;SCRIPT`

- <% e <%

.

3. Utilize a guia Avançado para excluir os comandos do WebSphere Commerce da proteção de script entre sites permitindo que os valores dos atributos especificado para esse comando específico contenha cadeias proibidas como segue:
   a. Selecione os comandos na caixa Lista de Comandos.
   b. Digite uma lista de atributos, separados por vírgulas, para os quais os caracteres proibidos são permitidos na janela Lista de Atributos Excluídos e clique em **Incluir**.
   c. Para remover um comando juntamente com seus atributos, selecione o comando na janela Lista de Comandos Excluídos e clique em **Remover**.

   Você também pode remover atributos específicos de um comando, selecionando o atributo e clicando em **Remover**.
4. Para aplicar suas alterações no Gerenciador de Configuração, clique em **Aplicar**.
5. Depois de atualizar com êxito a configuração de sua instância, você receberá uma mensagem indicando uma atualização com êxito.
6. No WebSphere Application Server Administration Console, pare e, em seguida, reinicie a instância do WebSphere Commerce Server.

Notas:

1. Quando os comandos forem excluídos da proteção de script entre sites, os valores de atributos especificados serão codificados através da codificação de símbolos em HTML. Por exemplo, o comando `cmd1?user=<Thomas>` é codificado como `ascmd1?user=&#60;Thomas&#62;`
2. Quando você especifica a cadeia nos campos de caracteres proibidos, saiba que:
   - Uma determinada seqüência de caracteres pode fazer com que a cadeia seja convertida para um único caracter em conformidade com os padrões de codificação da URL. Por exemplo, a cadeia `<%bb` será convertida em uma cadeia `<X` em que *X* é um único caractere que tem um valor de representação hexadecimal HEX 'bb' (decimal 187). Nesse caso, a cadeia `<%bb` não será capturada pela proteção de script entre sites, se tiver passado em uma URL.
   - Uma determinada seqüência de caracteres pode fazer com que a conversão da cadeia falhe, se eles não estiverem em conformidade com os padrões de codificação da URL. Por exemplo, a cadeia `<%gg` fará com que a conversão falhe, pois HEX 'gg' não é uma representação válida de valor hexadecimal. Nesse caso, a cadeia `<%gg` provocará uma exceção, resultando em nenhuma resposta ao pedido de URL que contém tal cadeia, independente da proteção de script entre sites estar ativada.

Exemplo: Considere os seguintes exemplos:

- Cadeias proibidas: `<SCRIPT`, `<%`

  Atributos proibidos: `mycomment`, `description`

Comando	Status
cmd1?description=Available...	rejeitado
cmd2?userid=Thomas...	aceito
cmd3?mycomment=<SCRIPT>...	rejeitado
cmd4?password=<%...%>...	rejeitado

- Se quiser permitir que o atributo `text` do comando `cmd1` contenha cadeias proibidas (`<SCRIPT`, `<%`) e não para outros atributos, por exemplo o atributo `txt`, você poderá excluir `cmd1` e especificar `text` como o atributo excluído.

Comando	Status
cmd1?text=<SCRIPT>...	aceito
cmd1?text=<%...%>...	aceito
cmd1?txt=<SCRIPT>...	rejeitado
cmd1?txt=<%..%>...	rejeitado

Ativando o Log de Acesso

Quando ativado, o recurso de log de acesso registra todos os pedidos recebidos pelo servidor WebSphere Commerce ou apenas os pedidos que resultaram em violações de acesso. Exemplos de violações de acesso são falha de autenticação, autoridade insuficiente para executar um comando ou redefinição de uma senha que não segue as regras de senha de seu site. Quando ativado, o log de acesso permite que um administrador WebSphere Commerce identifique rapidamente as ameaças de segurança no sistema WebSphere Commerce.

Quando ocorre um evento de falha de autenticação ou de autorização, as seguintes informações são registradas nas tabelas do banco de dados do arquivo de log de acesso, `ACCLOGMAIN` e `ACCLOGSUB`:

- Nome do Host do cliente
- ID do thread que está executando o comando;
- ID do usuário do cliente;
- Hora em que ocorreu o evento;
- Comando que foi executado;
- Loja para qual o comando foi executado;
- Recurso no qual a operação foi executada;
- Resultado da verificação de controle de acesso.

Para ativar o log de acesso, faça o seguinte:

1. Lance o Gerenciador de Configuração.
2. Selecione o **Nome do Host** > **Instância** > **Instance_List** e então abra a pasta **Componentes**.
3. Selecione **AccessLoggingEventListener**.
4. No painel Geral, ative a caixa de opção **Ativar Componente**.
5. Selecione o painel Avançado e ative **Iniciar**.
6. Clique em **Aplicar**.
7. Saia do Gerenciador de Configuração.
8. Reinicie o WebSphere Application Server.

Para alterar o tamanho do arquivo de log ou especificar se todos os pedidos foram registrados ou não, você precisa editar manualmente o arquivo *instance*`.xml` para a instância WebSphere Commerce localizada no subdiretório de instâncias do WebSphere Commerce:

1. Abra o arquivo *instance*`.xml` file para a instância em um editor.
2. Localize o seguinte nó, que está localizado no nó `<LogSystem>/<activitylog>`:

```
<accessLogging cacheSize="aa" logAllRequests="bbbbb" />
```

em que:

- *aa* é um valor inteiro especificando o número máximo de entradas que serão registradas na memória antes das entradas serem gravadas no banco de dados. Geralmente, um número mais alto resultará em melhor desempenho com relação ao registro de acesso. O valor padrão é 32.
- *bbbbb* é `true` ou `false`. Um valor `true` significa que todos os pedidos recebidos estão registrados. Um valor `false` significa que somente as violações de acesso estão registradas. Para evitar registro excessivo ou desnecessário, um valor `false` é recomendado. Utilize `true` somente quando você suspeitar de problemas de autenticação ou contravenção de segurança em seu site. O valor padrão é `false`.

3. Quando tiver concluído as atualizações, salve o arquivo *instance*`.xml` para sua instância do WebSphere Commerce.
4. Reinicie o WebSphere Application Server.

No seguinte exemplo, o log de acesso mantém 3 entradas na memória antes de registrar entradas nas tabelas de banco de dados. Além disso, ele registra todos os pedidos recebidos no WebSphere Commerce server:

```
<accessLogging cacheSize="3" logAllRequests="true" />
```

Configurando uma Política de Contas

A página Política de Contas do WebSphere Commerce Administration Console permite configurar uma política de contas. Esta página lista todas as políticas de conta existentes incluindo as predefinidas fornecidas com o WebSphere Commerce por padrão. Um critério de conta define os critérios relacionados à conta, como critérios de bloqueio de senha e de conta. Nesta página é possível:

- Criar uma nova política de conta, clicando em **Novo.**
- Alterar as características de uma política de conta existente selecionando a política na lista e clicando em **Alterar**.
- Excluir uma política de conta existente selecionando a política na lista e clicando em **Excluir**.

Para criar uma nova política de contas:

1. Abra o Administration Console.
2. No menu drop down Segurança do Administration Console, clique em **Política de Contas**.
3. Na página Política de Contas, clique em **Novo** para criar uma nova política de contas.
4. Digite o nome da política de contas no campo Nome (por exemplo, `my_account_policy`).
5. No menu Política de senhas, selecione uma política de senhas preexistente.
6. No menu Política de bloqueio de contas, selecione uma política de bloqueio de contas preexistente.
7. Clique em **OK**.

Depois que uma política de conta é criada, ela pode ser atribuída a um usuário. Observe que você não pode excluir uma política de contas, se ela estiver em uso (ou seja, um usuário estiver atribuído à política de contas).

Consulte também o tópico de referências ″Políticas de Autenticação Padrão″ na ajuda online do WebSphere Commerce.

Configurando uma Política de Senhas

A página Política de Senhas do WebSphere Commerce Administration Console permite controlar uma seleção de senha do usuário para definir as características da senha a fim de garantir que ela atenda à política de segurança de seu site. Esta página lista todas as políticas de senhas existentes incluindo as predefinidas fornecidas com o WebSphere Commerce por padrão.

Uma política de senhas define os atributos com os quais a senha deve estar de acordo. O critério de senha reforça as seguintes condições:

- Se o ID e a senha do usuário podem corresponder.
- Ocorrência máxima de caracteres consecutivos.
- Instâncias máximas de qualquer caracter.
- Tempo de vida máximo das senhas.
- Número mínimo de caracteres alfanuméricos.
- Número mínimo de caracteres numéricos.
- Comprimento mínimo da senha.
- Se a senha anterior do usuário pode ser reutilizada.
- Você pode criar uma nova política de senhas, clicando em **Novo.**
- Você pode alterar as características de uma política de senhas existente selecionando a política na lista e clicando em **Alterar**.
- Você pode excluir uma política existente selecionando a política de senha na lista e clicando em **Excluir**.

Para criar uma nova política de senha:

1. Abra o Administration Console.
2. No menu drop down Segurança do Administration Console, clique em **Política de Senhas**.
3. Na página Política de Senhas, clique em **Novo** para criar uma nova política de senhas.
4. Digite um nome para a política de senhas no campo Nome (por exemplo, `my_password_policy`).
5. Atualize o seguinte conforme necessário para modificar todos os valores a partir do valor padrão para compradores:
   - **O ID do usuário e senha podem coincidir?** Define se o ID do usuário e senha podem ser idênticos ou não. Selecione `Sim` ou `Não` na lista.
   - **Máximo de tipos de caracteres consecutivos**. Define a ocorrência máxima de caracteres consecutivos em uma senha. O valor mínimo é 2 caracteres consecutivos. Por exemplo, com um valor 2, um usuário não pode digitar uma senha como `aaabc`.
   - **Máximo de instâncias de qualquer caracter.** Define o número máximo de vezes que o mesmo caracter pode aparecer em uma senha. O valor mínimo é 1 instância de um caracter. Por exemplo, com um valor 2, um usuário não pode digitar uma senha como `abcaabc`.
   - **Tempo de vida máximo das senhas.** Define o período de tempo, em dias, que uma senha pode existir. O valor mínimo é 1 dia. Após esse período de tempo, o usuário será solicitado a alterar sua senha.

- **Número mínimo de caracteres alfabéticos**. Define o número mínimo de caracteres alfabéticos que precisam estar em uma senha. O valor mínimo é 10 caracteres alfabéticos.
- **Número mínimo de caracteres numéricos**. Define o número mínimo de caracteres numéricos que precisam estar em uma senha. O valor mínimo é 0 caracteres numéricos.
- **Comprimento mínimo de senha**. Define o menor comprimento de uma senha, em caracteres. O valor mínimo é 1 caracter.
- **A senha pode ser reutilizada?** Define se uma senha anterior do usuário pode ser reutilizada. Selecione `sim` ou `não` na lista.

6. Clique em **OK**.

Notas:

1. Você não pode excluir uma política de senhas se ela estiver em uso (ou seja, um usuário estiver atribuído à política de senhas).
2. As políticas de senha serão aplicadas somente se os usuários estiverem autenticados no banco de dados do WebSphere Commerce.

Consulte também o tópico de referências ″Políticas de Autenticação Padrão″ na ajuda online do WebSphere Commerce.

Configurando uma Política de Bloqueio de Contas

A página Política de Bloqueio de Contas do WebSphere Commerce Administration Console permite configurar uma política de bloqueio de contas para funções do usuário diferentes dentro do WebSphere Commerce. Esta página lista todas as políticas de bloqueio de conta existentes incluindo as predefinidas fornecidas com o WebSphere Commerce por padrão. Uma política de bloqueio de contas desativará uma conta de usuário, se ações maldosas forem executadas nessa conta, para reduzir as chances dessa ações que comprometem a conta.

Uma política de bloqueio de contas reforçam os seguintes itens:

- O limite de bloqueio de conta. Este é o número de tentativas de logon inválidas antes que a conta seja desativada.
- Adiamentos consecutivos de logins malsucedidos. Este é o período de tempo durante o qual o usuário não pode efetuar login, após duas tentativas falhas de login. O atraso é incrementado pelo valor de atraso do tempo configurado (por exemplo, 10 segundos) em cada falha de login consecutiva.

Para definir uma política de bloqueio de contas:

1. Abra o Administration Console.
2. No menu drop down Segurança do Administration Console, clique em **Política de bloqueio de contas**.
3. A página Política de Bloqueio de Contas lista todas as políticas de bloqueio de contas existentes. Nesta página é possível:
   - Criar uma nova política clicando em **Novo.**
   - Alterar as características de uma política existente selecionando a política na lista e clicando em **Alterar**.
   - Excluir uma política existente selecionando a política na lista e clicando em **Excluir**.

Para uma nova política de bloqueio de contas, na página Política de Bloqueio de Contas:

1. Digite o nome da política de bloqueio de contas no campo Nome (por exemplo, `my_policy`).
2. Digite um limite de bloqueio de contas no campo Limite de bloqueio de contas. Por exemplo, digite 6 (para seis tentativas).
3. Digite o atraso de login consecutivo malsucedido em segundos no campo Tempo de espera. Por exemplo, digite 10 (para dez segundos).
4. Clique em **OK**.

Notas:

1. Você não pode excluir uma política de bloqueio de conta, se ela estiver em uso (ou seja, um usuário será atribuído à política de bloqueio de conta).
2. As políticas de senha serão aplicadas somente se os usuários estiverem autenticados no banco de dados do WebSphere Commerce.

Lançando uma Verificação de Segurança

400 Esse recurso não é aplicável noWebSphere Commerce for iSeries.

A página Lançar Verificação de Segurança do WebSphere Commerce Administration Console permite lançar manualmente um programa de segurança que verifica e exclui arquivos WebSphere Commerce temporários que possam conter exposições de segurança potenciais. Normalmente o programa de verificação de segurança é executado como um job programado e, por padrão, é definido para ser executado uma vez por mês.

Para chamar o programa de verificação de segurança:

1. Abra o Administration Console.
2. No menu drop down Segurança do Administration Console, clique em **Verificador de Segurança**.
3. Na página Lançar Verificação de Segurança, clique em **Lançar**.

Os resultados da verificação de segurança, incluindo todas as ações executadas pelo programa são gravados na janela de log Verificação de segurança e no arquivo `sec_check.log` no subdiretório de log:

NT *unidade*:\WebSphere\Commerce\instances*instance_name*\log

2000 *unidade*:\Arquivos de Programas\WebSphere\Commerce\instances*instance_name*\log

AIX /usr/lpp/Commerce/instances/*instance_name*/log

Solaris /opt/WebSphere/Commerce/instances/*instance_name*/log

Linux /opt/WebSphere/Commerce/instances/*instance_name*/log

Windows Em plataformas não Windows, as permissões de arquivos são automaticamente definidas pelo WebSphere Commerce para que os arquivos sensíveis não possam ser acessados por usuários não autorizados. Em plataformas Windows, é necessário definir as permissões manualmente como segue. Esse procedimento assegura que somente o grupo Administradores tenha o direito de `leitura/gravação/execução` nos arquivos sensíveis:

1. No Windows Explorer, clique no botão direito na pasta *unidade*:\WebSphere.

2. Clique em **Propriedades** e **Segurança**. Por padrão, o grupo ″Todos″ tem a permissão **todos** para essa pasta.
3. Clique em **Incluir**.
4. Uma janela é exibida (Selecione usuários, computadores...). Nessa janela, selecione o grupo **Administradores**.

   Nota: Isso pode parecer um pouco ambíguo aqui, porque você poderá ver Administrador como um usuário, mas precisará incluir o grupo Administradores e não o usuário Administrador.

   Clique em **Incluir** e, em seguida, em **OK**.
5. Na guia Segurança, o Grupo Administradores foi incluído. Você precisa remover ″Todos″. Selecione **Todos** e desmarque a caixa que informa ″Permitir permissão que pode ser herdada....″
6. Clique em **Remover** na janela Segurança que é exibida.

Campo de Encrypt PDI do Gerenciador de Configuração

Ao configurar sua instância do WebSphere Commerce, recomenda-se selecionar a caixa de opção PDI Encrypt. Ative essa caixa de opção para especificar as informações nas tabelas ORDPAYINFO e ORDPAYMTHD devem ser criptografadas. Selecionando a caixa de opção, as informações de pagamento são armazenadas no banco de dados do WebSphere Commerce em formato criptografado.

Capítulo 5. Ativando a Segurança do WebSphere Application Server

Este capítulo descreve como ativar segurança para o WebSphere Application Server. Ativar a segurança do WebSphere Application Server evita que todos os componentes do Enterprise JavaBean sejam expostos a chamadas remotas realizadas por qualquer pessoa.

Nota: Windows AIX Solaris Linux Ao ativar a segurança do WebSphere Application Server é altamente recomendado que sua máquina atenda aos seguintes requisitos:

- Um mínimo de memória da máquina de 1 GB.
- Um tamanho de heap mínimo de 384 MB, para o aplicativo WebSphere Commerce.

Antes de Iniciar

Antes de começar a ativar a segurança, será necessário saber como o WebSphere Application Server no qual você está ativando segurança valida IDs do usuário. O WebSphere Application Server pode utilizar o LDAP ou o registro de usuários do sistema operacional como registro de usuários do WebSphere Application Server.

Windows AIX Solaris Linux Para obter informações sobre os últimos eFixes requeridos para executar a segurança do WebSphere Application Server, consulte o documento README do WebSphere Commerce 5.4 mais recente disponível do site da Web do WebSphere Commerce em:

Business `http://www.ibm.com/software/webservers/commerce/wc_be/lit-tech-general.html`

Professional `http://www.ibm.com/software/webservers/commerce/wc_pe/lit-tech-general.html`

Ativando a Segurança com um Registro de Usuário LDAP

Windows Para ativar a segurança do WebSphere Application Server quando estiver utilizando o LDAP como registro de usuário do WebSphere Application Server, efetue login no sistema como um usuário com autoridade administrativa e execute as seguintes etapas.

400 Para ativar a segurança do WebSphere Application Server quando estiver utilizando o LDAP como o registro de usuário do WebSphere Application Server, efetue login no sistema e execute as seguintes etapas.

AIX Solaris Linux Para ativar a segurança do WebSphere Application Server quando estiver utilizando o LDAP como registro de usuário do WebSphere Application Server, efetue login no sistema como `wasuser` e execute as seguintes etapas.

1. Inicie o Servidor WebSphere Application Server Administration e abra o Console do Administrador do WebSphere Application Server.
2. No Console, modifique as definições da segurança global conforme segue:

a. No menu Console, selecione **Centro de Segurança**.
b. Na guia Geral, selecione **Ativar Segurança**.
c. Na guia **Autenticação**, selecione LTPA (Lightweight Third Party Authentication). Preencha as definições de LTPA e desmarque a caixa de opção **Ativar Sign-on Único** se não quiser utilizar esta funcionalidade. Preencha a guia **Definições de LDAP** como a seguir, dependendo do tipo de servidor de diretório que você está utilizando:

Windows AIX Solaris Linux 400

Tabela 8. Usuários SecureWay

Nome do Campo	Definição	Valores de Exemplo	Notas
ID do Servidor de Segurança	ID do Usuário	*user_ID*	• Este não deve ser o administrador LDAP. • Não utilize um usuário especificado como cn=xxx. • Assegure que a classe do objeto deste usuário seja combatível com a classe do objeto especificada no campo Filtro do Usuário da janela Propriedades Avançados do LDAP.
Senha do Servidor de Segurança	Senha do Usuário	*password*	
Tipo de Diretório	Tipo de servidor LDAP	SecureWay	
Host	Nome do host do servidor LDAP	*hostname.domain.com*	
Porta	Porta que o servidor LDAP está utilizando		Este campo não é necessário
Nome Distinto Base	Nome distinto sob o qual a pesquisa ocorre	o=ibm,c=us	
Nome Distinto de Vinculação	Nome distinto para vincular ao diretório durante a pesquisa		Este campo não é necessário
Senha de Vinculação	Senha para o Nome Distinto de Vinculação		Este campo não é necessário

Windows

Tabela 9. Usuários do Netscape

Nome do Campo	Definição	Valores de Exemplo	Notas
ID do Servidor de Segurança	ID do Usuário	*user_ID*	• Este não deve ser o administrador LDAP. • Não utilize um usuário especificado como cn=xxx. • Assegure que a classe do objeto deste usuário seja combatível com a classe do objeto especificada no campo Filtro do Usuário da janela Propriedades Avançados do LDAP.
Senha do Servidor de Segurança	Senha do Usuário	*password*	
Tipo de Diretório	Tipo de servidor LDAP	Netscape	
Host	Nome do host do servidor LDAP	*hostname.domain.com*	
Porta	Porta que o servidor LDAP está utilizando		Este campo não é necessário
Nome Distinto Base	Nome distinto sob o qual a pesquisa ocorre	o=ibm	
Nome Distinto de Vinculação	Nome distinto para vincular ao diretório durante a pesquisa		Este campo não é necessário
Senha de Vinculação	Senha para o Nome Distinto de Vinculação		Este campo não é necessário

Windows

Tabela 10. Usuários Domino

Nome do Campo	Definição	Valores de Exemplo	Notas
ID do Servidor de Segurança	Nome Abreviado/ID de Usuário	*user_ID*	Certifique-se de que a classe do objeto deste usuário seja combatível com a classe do objeto especificada no campo Filtro do Usuário da janela Propriedades Avançados do LDAP.

Tabela 10. Usuários Domino (continuação)

Nome do Campo	Definição	Valores de Exemplo	Notas
Senha do Servidor de Segurança	Senha do Usuário	*password*	
Tipo de Diretório	Tipo de servidor LDAP	Domino 5.0	
Host	Nome do host do servidor LDAP	*hostname.domain.com*	
Porta	Porta que o servidor LDAP está utilizando		Este campo não é necessário
Nome Distinto Base	Nome distinto sob o qual a pesquisa ocorre		Este campo não é necessário
Nome Distinto de Vinculação	Nome distinto para vincular ao diretório durante a pesquisa		Este campo não é necessário
Senha de Vinculação	Senha para o Nome Distinto de Vinculação		Este campo não é necessário

Windows

Tabela 11. Usuários do Active Directory

Nome do Campo	Definição	Valores de Exemplo	Notas
ID do Servidor de Segurança	sAMAccountName	*user_ID*	• Nome de Logon do Usuário de qualquer usuário comum. • Não utilize um usuário especificado como cn=xxx. • Assegure que a classe do objeto deste usuário seja combatível com a classe do objeto especificada no campo Filtro do Usuário da janela Propriedades Avançados do LDAP.
Senha do Servidor de Segurança	Senha do Usuário	*password*	
Tipo de Diretório	Tipo de servidor LDAP	Active Directory	
Host	Nome do host do servidor LDAP	*hostname.domain.com*	
Porta	Porta que o servidor LDAP está utilizando		Este campo não é necessário

Tabela 11. Usuários do Active Directory (continuação)

Nome do Campo	Definição	Valores de Exemplo	Notas
Nome Distinto Base	Nome distinto sob o qual a pesquisa ocorre	CN=users, DC=domain1, DC=domain2, DC=com	
Nome Distinto de Vinculação	Nome distinto para vincular ao diretório durante a pesquisa	CN=*user_ID*, CN=users, DC=domain1, DC=domain2, DC=com	O valor *user_ID* é o Nome de Exibição. Este não é necessariamente o mesmo Nome de Logon do Usuário.
Senha de Vinculação	Senha para o Nome Distinto de Vinculação	*bind_password*	Esta deve ser a mesma Senha do Servidor de Segurança.

d. Windows 400 Reinicie o WebSphere Application Server Administration Server, e em seguida abra novamente o WebSphere Application Server Administrator's Console.

e. Na guia **Mapeamento de Função**, selecione o servidor de aplicativos WCS e clique no botão **Editar Mapeamentos...**.

1) Selecione a Função WCSSecurity e clique no botão **Selecionar...**.

2) Marque a caixa de opção Selecionar usuários/grupos e inclua o ID do usuário que foi digitado na etapa 2c na página 56.

f. Clique em **Concluir**.

3. Feche o console administrativo, pare e reinicie o servidor WebSphere Application Server Administration. A partir de agora, quando você abrir o Administration Console do WebSphere Application Server, serão solicitados o ID e a senha do Servidor de Segurança.
4. Abra o Gerenciador de Configuração do WebSphere Commerce e selecione **Instâncias** > *instance_name* > **Propriedades da Instância** > **Segurança** e clique na caixa de opção **Ativar**. Será solicitado que você digite o nome e a senha do usuário informados na etapa 2c na página 56. Clique em **Aplicar** em seguida saia do Gerenciador de Configuração.
5. Pare e reinicie o servidor de administração do WebSphere Application Server.

Ativando a Segurança com um Registro de Usuário do Sistema Operacional

Windows 400 Para ativar a segurança do WebSphere Application Server quando estiver utilizando a validação do usuário do sistema operacional como o registro de usuário do WebSphere Application Server, efetue login como um usuário com autoridade administrativa e execute as etapas a seguir.

AIX Solaris Linux Para utilizar o sistema operacional como um registro de usuário, o WebSphere Application Server precisa ser executado como root. Execute o WebSphere Application Server como root e execute as seguintes etapas.

1. AIX Solaris Linux Efetue login como root
2. AIX Solaris Linux Inicie o WebSphere Application Server e lance o WebSphere Application Server Administration Console enquanto estiver com a sessão iniciada como root:

```
export DISPLAY=fully_qualififed_host_name:0.0
cd WAS_HOME/bin
./startupServer.sh &
./adminclient.sh remote_WAS_host_name  port
```

em que *fully_qualififed_host_name* é o nome do computador que você estiver utilizando para acessar o WebSphere Application Server Administration Console, *remote_WAS_host_name* é o nome do host completo do WebSphere Application Server, e porta é a porta pela qual você está acessando o WebSphere Application Server (a porta padrão é 2222).

3. No WebSphere Application Server Administration Console modifique as definições da segurança global conforme segue:
   a. No menu Console, selecione **Centro de Segurança**.
   b. Na guia Geral, selecione a caixa de opção **Ativar Segurança**.
4. Selecione a guia **Autenticação** e selecione o botão de opção **Sistema Operacional Local**
5. Digite o ID do servidor de segurança no campo **ID do Servidor de Segurança**. Digite o nome do usuário como a seguir:

Nome do Campo	Valores de Exemplo	Notas
ID do Usuário	*user_ID*	Windows O ID do usuário com privilégios administrativos do sistema operacional com o qual foi efetuado login. Se a máquina pertencer a um domínio, utilize o ID do usuário completo. Por exemplo: DomainXYZ\user_id. Certifique-se de que esta conta exista no servidor do domínio e que seja um membro do grupo do Administrador. AIX Solaris Linux Um ID do usuário que é root ou tem autoridade root. 400 O Id de usuário no iSeries deve ter a autoridade *SECOFR.
Senha do Servidor de Segurança	*password*	Esta é a senha pertencente ao usuário com privilégios administrativos do sistema operacional com a qual foi efetuado login.

6. Windows 400 Reinicie o WebSphere Application Server Administration Server, e em seguida abra novamente o WebSphere Application Server Administrator's Console.
7. Na guia **Mapeamento de Função**, selecione o aplicativo corporativo do WC e clique no botão **Editar Mapeamentos...**.
   a. Selecione WCSecurityRole e clique no botão **Selecionar...**.
   b. Selecione a caixa de opção Selecionar usuários/grupos, digite o ID do usuário que foi utilizado na etapa 5 no campo Pesquisa e clique em

Pesquisar. Selecione esse usuário na lista Usuários/Grupos Disponíveis e clique em **Incluir** para incluí-lo na lista Usuários/Grupos Selecionados. Em seguida, clique em **OK** em cada painel até sair do Centro de Segurança.

8. Abra o WebSphere Commerce Gerenciador de Configuração e selecione **Lista de Instâncias → *instance_name* → Propriedades da Instância→ Segurança** e selecione a caixa de opção **Ativar Segurança**. Selecione **Registro de Usuário do Sistema Operacional** para o modo de autenticação e digite o nome do usuário e a senha digitados na etapa 5 na página 60. Clique em **Aplicar** e saia do Gerenciador de Configuração.
9. Pare e reinicie o servidor de administração do WebSphere Application Server. A partir de agora, quando você abrir o WebSphere Application Server Administration Console, serão solicitados o ID e a senha do Servidor de Segurança.

Desativando a Segurança do WebSphere Commerce

O WebSphere Commerce Business Edition permite desativar a segurança EJB. Para desativar a segurança de EJB do WebSphere Commerce, proceda da seguinte maneira:

1. Inicie o WebSphere Application Server Administration Console.
2. Clique em **Console → Centro de Segurança...** e desmarque a caixa de opção **Ativar Segurança** na guia **Geral**.
3. Abra o Gerenciador de Configuração do WebSphere Commerce e selecione **Lista de Instâncias → *instance_name* → Propriedades da Instância → Segurança** e limpe a caixa de opção **Ativar Segurança**.
4. Saia do WebSphere Application Server Administration Console.
5. Pare e reinicie o servidor de administração do WebSphere Application Server.

Opções de Implementação de Segurança do WebSphere Commerce

O WebSphere Commerce suporta várias configurações de implementação de segurança.A tabela a seguir ilustra as opções de implementação de segurança disponíveis.

Tabela 12. Cenários de segurança de uma única máquina

A segurança do WebSphere Application Server está ativada.	• Utilize o sistema operacional como o registro do WebSphere Application Server. • Utilize o banco de dados como o registro do WebSphere Commerce.
	• Utilize o LDAP como o registro do WebSphere Application Server. • Utilize o LDAP como o registro do WebSphere Commerce.
	• Utilize o LDAP como o registro do WebSphere Application Server.

Tabela 12. Cenários de segurança de uma única máquina (continuação)

A segurança do WebSphere Application Server está desativada e o site de seu WebSphere Commerce está localizado atrás de um firewall.	• Um registro do WebSphere Application Server não é requerido. • Utilize o banco de dados como o registro do WebSphere Commerce.
	• Um registro do WebSphere Application Server não é requerido. • Utilize o LDAP como o registro do WebSphere Commerce.

Tabela 13. Cenários de segurança de várias máquinas

A segurança do WebSphere Application Server está ativada. O LDAP está sempre implementado.	• Utilize o LDAP como o registro do WebSphere Application Server. • Utilize o LDAP como o registro do WebSphere Commerce.
	• Utilize o LDAP como o registro do WebSphere Application Server. • Utilize um banco de dados como o registro do WebSphere Commerce. • Será necessário configurar o LDAP e colocar uma entrada administrativa no registro do LDAP.
A segurança do WebSphere Application Server está desativada e o site de seu WebSphere Commerce está localizado atrás de um firewall.	• Utilize um banco de dados como o registro do WebSphere Commerce. • Um registro do WebSphere Application Server não é requerido. • Sign-on único não é suportado.
	• Utilize o LDAP como o registro do WebSphere Application Server. • Um registro do WebSphere Application Server não é requerido.

Nota: Se você operar o site do WebSphere Commerce de trás de um firewall, será possível desativar a segurança do WebSphere Application Server. Você deve desativar a segurança do WebSphere Application Server apenas se tiver certeza de que nenhum aplicativo mal intencionado esteja em execução atrás do firewall.

Capítulo 6. Gerenciamento de Sessões

Os navegadores da Web e sites de e-commerce utilizam HTTP para comunicação. Como o HTTP é um protocolo sem informações de estado (o que significa que cada comando é executado independentemente sem qualquer conhecimento dos comandos que vêm antes dele), deve haver uma maneira de gerenciar sessões entre o lado do navegador e o lado do servidor.

O WebSphere Commerce suporta dois tipos de sessão de gerenciamento: baseado em cookie e regravação de URL. O administrador pode escolher suportar somente o gerenciamento de sessões baseadas em cookie ou ambos os tipos. Se o WebSphere Commerce suportar apenas o tipo baseado em cookie, os navegadores dos compradores deverão aceitar cookies. Se baseado em cookie e regravação de URL forem selecionados, o WebSphere Commerce tentará primeiro utilizar cookies para gerenciar sessões; se o navegador do comprador estiver definido para não aceitar cookies, então será utilizada a regravação de URL.

Gerenciamento de Sessões Baseadas em Cookie

Quando um gerenciamento de sessões baseadas em cookie é utilizado, uma mensagem (cookie) contendo as informações do usuário é enviada ao navegador pelo servidor Web. Esse cookie é enviado de volta ao servidor quando o usuário tenta acessar determinadas páginas. Ao enviar de volta o cookie, o servidor consegue identificar o usuário e recupera a sessão do usuário do banco de dados de sessão, mantendo, dessa forma, a sessão do usuário. Uma sessão baseada em cookie termina quando o usuário efetua logoff ou fecha o navegador. O gerenciamento de sessões baseadas em cookie é seguro e apresenta benefícios de desempenho. O gerenciamento de sessão baseado em cookie é seguro porque utiliza uma tag de identificação que flui somente sobre o SSL. O gerenciamento de sessão baseada em cookie oferece benefícios de desempenho significativo porque o mecanismo de armazenamento em cache do WebSphere Commerce suporta somente sessões baseadas em cookie e não em regravação URL. O gerenciamento de sessões baseadas em cookie é recomendado para sessões do comprador.

Se você não estiver utilizando regravação de URL e quiser certificar-se de que os usuários têm cookies ativados em seus navegadores, marque **Teste de aceitação de cookie** na página Gerenciamento de Sessão do Gerenciador de Configuração. Isso informa ao comprador que seu navegador não suporta cookies ou se o cookie estiver desligado, será necessário um navegador que suporte cookies para navegar no site do WebSphere Commerce.

Por razões de segurança, o gerenciamento de sessões baseadas em cookie utiliza dois tipos de cookies:

- Um cookie de sessão não seguro

  Utilizado para gerenciar dados de sessão. Ele contém o ID de sessão, o idioma negociado, a loja atual e a moeda preferida dos compradores quando o cookie é construído. Esse cookie pode fluir entre o navegador e o servidor sob a conexão SSL ou não SSL. Existem dois tipos de cookies de sessão não seguros:

  – Um cookie de seção do WebSphere Application Server baseia-se no padrão de sessão HTTP de servlet. Os cookies do WebSphere Application Server persistem na memória ou banco de dados em uma implementação de nós múltiplos. Para obter mais informações, pesquise por ″gerenciamento de

sessão" no WebSphere Application Server InfoCenter disponível em http://www.ibm.com/software/webservers/appserv/infocenter.html.

– Um cookie de sessão do WebSphere Commerce é interno ao WebSphere Commerce e não persiste no banco de dados.

Para selecionar qual tipo de cookie utilizar, selecione WCS ou WAS para o parâmetro **Gerenciador de sessão de cookie** na página Gerenciamento de Sessão do Gerenciador de Configuração.

- Um cookie de autenticação seguro

  Utilizado para gerenciar dados de autenticação. O cookie de autenticação flui através do SSL e a hora é autenticada para segurança máxima. Esse é o cookie utilizado para autenticar o usuário sempre que um comando com distinção de maiúsculas e minúsculas for executado, por exemplo, DoPaymentCmd que pede o número do cartão de crédito do usuário. Há um risco mínimo de que esse cookie seja roubado e utilizado por um usuário não autorizado. Os cookies do código de autenticação são sempre gerados pelo WebSphere Commerce quando o gerenciamento de sessões baseadas e cookie está em uso.

Tanto os cookies de sessão como os de código de autenticação são requeridos para exibir páginas de segurança.

Para erros de cookie, CookieErrorView é chamado nas seguintes circunstâncias:

- O usuário efetuou login de outro local com o mesmo ID de Logon.
- O cookie foi danificado, violado ou ambos.
- Se a aceitação do cookie for definida para "true" e o navegador do usuário não suportar cookies.

Utilizando Cookies para Gerenciamento de Sessão

Para utilizar os cookies no WebSphere Commerce, faça o seguinte:

1. Abra o Gerenciador de Configuração.
2. Selecione a **Instância**, em seguida abra a pasta **Gerenciamento de Sessão**.
3. Selecione os valores de sessão adequados.
   - Teste de aceitação de cookies

     Selecione esta caixa de opção para verificar se o navegador do cliente aceita cookies para um site que suporta apenas cookies.
   - Gerenciador de sessão de cookies

     Selecione se você deseja que o WebSphere Commerce ou o WebSphere Application Server gerencie seus cookies. O padrão é WebSphere Commerce.
     – Um cookie de sessão do WebSphere Application Server baseia-se no padrão de sessão HTTP de servlet. Os cookies do WebSphere Application Server persistem na memória ou no banco de dados em uma implementação de nós múltiplos. Para obter mais informações, pesquise por "gerenciamento de sessão" no WebSphere Application Server InfoCenter disponível em http://www.ibm.com/software/webservers/appserv/infocenter.html.
     – Um cookie de sessão do WebSphere Commerce é interno ao WebSphere Commerce e não persiste no banco de dados.
4. Clique na guia **Avançado**. Selecione os valores de sessão adequados.
   - Caminho do cookie

Normalmente, este campo não deve ser alterado. Especifica o caminho para o cookie, que é o subconjunto de URLs para o qual um cookie deve ser enviado.

- Duração do cookie

  Este campo não deve ser alterado. O padrão é que um cookie deve expirar quando o navegador é fechado.

- Domínio do cookie

  Normalmente, este campo não deve ser alterado. Especifica um padrão de restrição de domínio. Um domínio especifica os servidores que devem ver um cookie. Por padrão, o cookie é retornado somente ao WebSphere Commerce Server que o emitiu. Por padrão, os cookies são retornados somente ao host que os salvou. A especificação de um padrão de nome de domínio substitui isso. O padrão deve iniciar com um ponto e conter pelo menos dois pontos. Um padrão corresponde somente a uma entrada além do ponto inicial. Por exemplo, `".ibm.com"` é válido e corresponde a `a.ibm.com` e a `b.ibm.com`, mas não a `www.a.ibm.com`. Para obter detalhes sobre padrões de domínio, consulte a Especificação de Cookie do Netscape e o RFC 2109.

5. Clique em **Aplicar**.
6. Feche o Gerenciador de Configuração.
7. No WebSphere Application Server Administration Console, pare e, em seguida, reinicie a instância.

Regravação de URL

Com a regravação de URL, todos os links retornados ao navegador ou redirecionados têm o ID de sessão anexados a ele. Quando o usuário clica nesses links, o formulário de regravação da URL é enviado ao servidor como parte do pedido do cliente. O mecanismo de servlet reconhece o ID de sessão na URL e o salva para obter o objeto adequado para esse usuário. Para utilizar a regravação de URL, os arquivos HTML (arquivos com extensão `.html` ou `.htm`) não podem ser utilizados para links. Para utilizar a regravação de URL, os arquivos JSP devem ser utilizados para fins de exibição. Uma sessão com regravação de URL expira quando o comprador efetua logoff.

Nota: O armazenamento em cache do WebSphere Commerce e a regravação de URL não podem operar juntos. Com a regravação de URL ativada, é necessário desativar o componente de armazenamento em cache do the WebSphere Commerce.

Utilizando Gerenciamento de Sessões de Regravação de URL

Para especificar como as sessões devem ser gerenciadas, faça o seguinte:

1. Abra o Gerenciador de Configuração.
2. Selecione a **Instância**, em seguida abra a pasta **Gerenciamento de Sessão**.
3. Selecione os valores de sessão adequados.

   Ative a regravação de URL. Selecione esta caixa de opções para utilizar a regravação de URL no gerenciamento de sessões.

   Gerenciador de sessão de cookies. Selecione o WebSphere Application Server.
4. Clique em **Aplicar**.
5. Feche o Gerenciador de Configuração.
6. No WebSphere Application Server Administration Console, pare e, em seguida reinicie a instância.

Gravando Modelos JSP para Regravação de URL

Se você quiser utilizar a regravação de URL para manter um estado de sessão, não inclua links em partes do aplicativo da Web nos arquivos HTML simples. Essa restrição é necessária, porque a codificação de URL não pode ser utilizada em arquivos HTML simples. Para manter o estado utilizando a regravação de URL, cada página que o usuário solicitar durante a sessão deve ter código que possa ser entendido pelo interpretador Java. Se você tiver tais arquivos HTML simples no aplicativo da Web e partes do site que o usuário poderá acessar durante a sessão, converta-os para arquivos JSP. Isso gerará um impacto no escritor de aplicativos, porque, ao contrário de manter sessões com cookies, manter sessões com regravação de URL requer que cada modelo JSP no aplicativo utilize codificação de URL para cada atributo `HREF` nas tags `<A>`. A sessão será perdida se um ou mais modelos JSP em um aplicativo não chamar os métodos `encodeURL(String url)` ou encode `RedirectURL(String url)`.

Gravando Links

Com a regravação de URL, todos os links retornados ao navegador ou redirecionados devem ter o ID de sessão anexados a ele. Por exemplo, esse link em uma página da Web:

```
<a href="store/catalog">
```

é regravado como

```
<a href="store/catalog;$jsessionid$DA32242SSGE2">
```

Quando o usuário clica nesse link, o formulário de regravação da URL é enviado ao servidor como parte do pedido do cliente. O Mecanismo de Servlet reconhece `;$jsessionid$DA32242SSGE2` como o ID de sessão e o salva para obter o objeto `HttpSession` adequado para esse usuário.

O seguinte exemplo mostra como o código Java pode ser incorporado em um arquivo JSP:

```
<%
response.encodeURL ("/store/catalog");
%>
```

Para regravar as URLs que você está retornando ao navegador, chame o método `encodeURL()` no modelo JSP antes de enviar a URL ao fluxo de saída. Por exemplo, se um modelo JSP que não utiliza regravação de URL tiver:

```
out.println("<a href=\"/store/catalog\">catalog</a>")"
```

substitua-o por:

```
out.println("<a href=\"");
out.println(response.encodeURL ("/store/catalog"));
out.println("\">catalog</a>");
```

Para regravar as URLs que você está redirecionando, chame o método `encodeRedirctURL()`. Por exemplo, se o modelo JSP tiver:

```
response.sendRedirect (response.encodeRedirectURL ("http://myhost/store/catalog"));
```

Os métodos `encodeURL()` e `encodeRedirectURL()` fazem parte do objeto `HttpServletResponse`. Em ambos os casos, essas chamadas verificam se a regravação de URL foi configurada antes da codificação da URL. Se não tiver sido configurada, ela retornará a URL original.

Gravando Formulários: Para gravar formulários para submissão, chame `response.encodeURL("Logon");` na tag `ACTION` do modelo de formulário. Por exemplo,

```
String strLoginPost = response.encodeURL("Logon");
<FORM NAME="Logon" METHOD="post" ACTION= <%= strLoginPost %> >
...
</FORM>
```

Gravando a primeira página: A página de entrada, normalmente a home page, não pode conter quadros. Se você quiser utilizar quadros na loja, poderá fazer com que uma página sem quadro com um link para a loja atue como a página de entrada da loja. No entanto, se a loja não utilizar quadros e um cliente tentar acessar essas páginas com quadros sem primeiro passar pela página de entrada, sua sessão poderá ser perdida. Os clientes também podem perder sua sessão se utilizarem o botão **Voltar** (somente com quadros) para retornar à página de entrada e atualizá-la. A atualização da página de entrada fornece a eles um novo ID de sessão. Um link para voltar à página de entrada como uma alternativa ao botão **Voltar** é necessário para ajudar a evitar esse tipo de perda de sessão.

Parte 3. Tarefas de Segurança do Administrador do Site

Essa parte descreve as tarefas de segurança que geralmente podem ser executadas por um administrador do sistema em seu site, não necessariamente o administrador do site do WebSphere Commerce.

Capítulo 7. Definindo e Alterando Senhas

A maioria dos componentes do WebSphere Commerce utiliza IDs de usuário e senhas que são validadas pelo sistema operacional. Para obter informações sobre como alterar essas senhas, consulte a documentação do sistema operacional. Este capítulo inclui como definir e alterar senhas dos componentes do WebSphere Commerce que não validam IDs do usuário e senhas através do sistema operacional.

Referência Rápida para IDs do Usuário, Senhas e Endereços da Web

A administração no ambiente do WebSphere Commerce exige uma variedade de IDs do usuário. Estes IDs do usuário, junto com suas autoridades, estão descritas na lista abaixo. Para os IDs do usuário do WebSphere Commerce, são identificadas as senhas padrão.

Windows **ID do Usuário do Windows**

Seu ID do usuário Windows *deve* ter autoridade de Administrador. Se você estiver utilizando o DB2, ele necessita que o ID do usuário e senha sigam estas regras:

- Não podem ter mais de 8 caracteres de comprimento.
- Podem conter somente os caracteres de A até Z, de a até z, de 0 a 9, @, #, $, e _.
- Não podem começar com um caractere de sublinhado (_).
- O ID do usuário não pode ser nenhum dos seguintes, em letras maiúsculas,minúsculas ou uma combinação de ambas: USERS, ADMINS, GUESTS, PUBLIC, LOCAL.
- O ID do usuário não pode começar com nenhuma dessas opções: letra maiúscula, minúscula ou ambas: IBM, SQL, SYS.
- O ID do usuário não pode ser igual a nenhum nome de serviço do Windows.
- O ID do usuário deve ser definido na máquina local e pertencer ao grupo do Administrador Local.
- O ID do usuário deve ter o direito de usuário avançado para *Atuar como parte do sistema operacional*.

Você pode executar a instalação sem o direito de usuário avançado *Atuar como parte do sistema operacional*, porém, o programa de instalação do DB2 não poderá validar a conta especificada para o Servidor de Administração. É recomendável que qualquer conta de usuário utilizada para instalar o DB2 tenha este direito de usuário avançado.

Importante

Se seu ID de usuário do Windows *não* tiver autoridade Administrador, tiver mais de 8 caracteres ou não estiver definido na máquina local, você será notificado do problema e não poderá prosseguir com a instalação.

Se você estiver utilizando o DB2, você utilizará este ID de usuário como o nome de usuário do banco de dados DB2 (ID de logon do usuário do banco de dados).

Se você precisar criar um ID do usuário que atenda aos critérios acima, poderá encontrar informações sobre a criação de um ID do usuário do Windows na ajuda online do Windows.

Perfis de usuário iSeries 400

Dois perfis de usuário iSeries são utilizados e consultados freqüentemente quando você instala e configura o WebSphere Commerce:

- Um perfil de usuário que você cria e utiliza para instalar o WebSphere Commerce e acessar o Gerenciador de Configuração. Para instalar e configurar o WebSphere Commerce, você deve utilizar um perfil de usuário USRCLS(*SECOFR) do iSeries, ou utilizar o perfil de usuário QSECOFR. Se você precisar criar um perfil de usuário, consulte o *WebSphere Commerce 5.4 - Manual de Instalação* para iSeries.
- Um perfil de usuário que é criado pelo Gerenciador de Configuração quando você cria uma instância WebSphere Commerce. Este perfil de usuário também é conhecido como "perfil de usuário de instância." Um perfil de usuário de USRCLS(*USER) é criado pelo Gerenciador de Configuração toda vez que você cria uma instância WebSphere Commerce. Se você precisar criar um perfil de usuário, consulte o *WebSphere Commerce 5.4 - Manual de Instalação* para iSeries.

ID do usuário do Gerenciador de Configuração

A interface gráfica do Gerenciador de Configuração permite modificar a maneira como o WebSphere Commerce é configurado. O ID do usuário e senha padrão do Gerenciador de Configuração são `webadmin` e `webibm`.

Windows AIX Solaris Linux Você pode acessar o Gerenciador de Configuração na máquina do WebSphere Commerce ou em qualquer máquina que esteja na mesma rede que o WebSphere Commerce.

400 Para o iSeries, você pode acessar Gerenciador de Configuração a partir de qualquer máquina Windows que está na mesma rede como seu servidor iSeries.

IBM HTTP Server ID do usuário Windows AIX Solaris Linux

Se estiver utilizando o IBM HTTP Server, você pode acessar a home page do servidor Web abrindo seu navegador Web e digitando o seguinte endereço da Web:

`http://host_name`

Se tiver personalizado o servidor Web, pode ser requerido digitar o nome da primeira página do servidor Web após o nome do host.

Instance Administrator do WebSphere Commerce

O ID do usuário e senha do Instance Administrator aplicam-se às seguintes ferramentas do WebSphere Commerce:

- WebSphere Commerce Accelerator. Para acessar o WebSphere Commerce Accelerator a partir de uma máquina executando um sistema operacional Windows, abra seu navegador Internet Explorer, e digite o seguinte endereço na Web:

  `https://host_name:8000/accelerator`
- WebSphere Commerce Administration Console. Para acessar o WebSphere Commerce Administration Console a partir de uma máquina

remota executando um sistema operacional Windows, abra seu navegador do Internet Explorer Web e digite o seguinte endereço da Web:

`https://nome_do_host:8000/adminconsole`

- Store Services. Você pode acessar a página Store Services abrindo o navegador da Web e digitando o seguinte endereço:

  `https://nome_do_host:8000/storeservices`

O ID do usuário padrão do Instance Administrator é `wcsadmin` e a senha padrão é `wcsadmin`.

Nota: O ID do usuário `wcsadmin` nunca deve ser removido e sempre deve ter autoridade de administrador da instância.

O WebSphere Commerce requer que o ID do usuário e senha sigam as seguintes regras:

- A senha deve possuir pelo menos 8 caracteres de comprimento.
- A senha deve incluir pelo menos 1 dígito numérico.
- A senha não deve conter mais que 4 ocorrências de um caractere.
- A senha não irá repetir o mesmo caractere mais de três vezes.

Administrador do Payment Manager

Ao instalar o Payment Manager, o ID de Administrador do WebSphere Commerce, `wcsadmin`, é atribuído automaticamente com a função de Administrador do Payment Manager. Siga as instruções no *WebSphere Commerce 5.4 - Manual de Instalação* para mudar a Payment Manager Realm Class para WCSRealm se ainda não o tiver feito.

A função de Administrador do Payment Manager permite quem um ID do usuário controle e administre o Payment Manager.

Notas: 400

- Não exclua ou renomeie o ID do usuário de logon `wcsadmin`, e não altere a função `wcsadmin` pré-atribuída do Payment Manager, pois as funções do WebSphere Commerce relacionadas à integração do Payment Manager não irão funcionar.
- Se você atribuir uma função do Payment Manager a um administrador do WebSphere Commerce e, depois, quiser excluir ou renomear o ID do usuário de logon desse administrador, deve remover a função de administrador do Payment Manager antes de excluir ou renomear o ID do usuário.

Importante

O Payment Manager atribuiu previamente a função de Administrador do Payment Manager a dois outros IDs de administração:

- `ncadmin`
- `admin`

Para evitar que um usuário obtenha inadvertidamente esta função de Administrador do Payment Manager, você pode:

1. Criar os IDs de administração acima no WebSphere Commerce utilizando o Administration Console do WebSphere Commerce.
2. Na interface com o usuário do Payment Manager, selecione **Usuários**.
3. Remova a função de Administrador do Payment Manager desses dois IDs de administração.

Esteja ciente também da Senha de Instância do Payment Manager, que é necessária para iniciar, parar ou excluir uma instância do Payment Manager. Ela também é necessária para incluir cassetes em uma instância do Payment Manager. Se uma instância do Payment Manager for criada pelo Gerenciador de Configuração do WebSphere Commercer, a senha da instância do Payment Manager é a mesma que a senha de instância de logon, do WebSphere Commerce, que também é referida como uma senha de instância do perfil de usuário. Se uma instância do Payment Manager for criada a partir de uma sessão do iSeries utilizando o comando **CRTPYMMGR** ou a partir da Página de Tarefas do iSeries, você será solicitado a fornecer a senha.

Alterando a Senha do Gerenciador de Configuração

Você poderá alterar a senha do Gerenciador de Configuração quando lançar o Gerenciador de Configuração clicando em **Modificar** na janela em que digita seu ID do usuário e senha.

Windows AIX Solaris Linux de forma alternativa, para alterar o ID do usuário ou a senha do Gerenciador de Configuração mude para o subdiretório `bin` no caminho de instalação do WebSphere Commerce e digite o seguinte em uma janela de comando:

```
config_env
java com.ibm.commerce.config.server.PasswordChecker -action [action type]
   -pwfile [password file] -userid [user ID]
   -password [userid password] [-newpassword [new userid password]]
```

em que action types são `Incluir`, `Marcar`, `Excluir` ou `Modificar`. Os parâmetros são explicados abaixo:

pwfile
O caminho para o arquivo onde a senha será armazenada. O caminho padrão é o subdiretório `bin` sob o caminho de instalação do WebSphere Commerce. Esse parâmetro é requerido sempre.

userid
Digite o ID do usuário que deseja incluir, verificar, excluir ou modificar. Esse parâmetro é requerido sempre.

password
Digite a senha que deseja criar, verificar, excluir ou modificar. Este parâmetro deve ser utilizado juntamente com o parâmetro `userid`. Esse parâmetro é requerido sempre.

newpassword
Utilize este parâmetro para alterar a senha para um determinado ID do usuário. Esse parâmetro deve ser utilizado em conjunto com os parâmetros `userid` e `password`. Esse parâmetro é requerido ao se especificar o tipo de ação `Modificar`.

Definindo a Senha do Administrador do IBM HTTP Server

Windows AIX Solaris Linux Para definir a senha de administrador do seu IBM HTTP Server,

1. Vá para o diretório de instalação do IBM HTTP Server em sua máquina.
2. Digite o seguinte comando:

   Windows `htpasswd -b conf\admin.passwd` *`user password`*

   AIX Solaris Linux `htpasswd -b conf/admin.passwd` *`user password`* em que *user* e *password* são o ID do usuário e a senha nos quais você deseja ter autoridade administrativa para o IBM HTTP Server.

Agora você definiu com êxito sua senha administrativa do IBM HTTP Server.

Alterando a Senha do Arquivo de Chaves SSL

Windows AIX Solaris Linux Se você estiver utilizando o IBM HTTP Server, siga as etapas abaixo para alterar a senha do arquivo de chaves SSL.

1. Windows Clique no **Menu Iniciar** → **Programas** → **IBM HTTP Server** → **Utilitário de Gerenciamento de Chaves**.
2. No menu **Arquivo do Banco de Dados Chave**, selecione **Abrir**.
3. Mude para o subdiretório `ssl` sob o caminho de instalação do IBM HTTP Server em sua máquina. O arquivo de chaves (que possui a extensão de arquivo `.kdb`) deve estar nesta pasta. Se não estiver, crie um arquivo de chaves seguindo as instruções descritas em Capítulo 8, “Ativando o SSL para Produção com o IBM HTTP Server” na página 77.
4. No menu **Arquivo de Banco de Dados Chave**, selecione **Alterar Senha**. A janela Alterar Senha é exibida.
5. Digite sua nova senha e ative **Armazenar a senha em um arquivo**.
6. Clique em **OK**. Sua senha foi alterada.

Agora, você alterou, com êxito, sua senha de administração do arquivo de chave SSL.

Gerando Senhas Criptografadas para o WebSphere Commerce

Windows AIX Solaris Linux O WebSphere Commerce permite gerar senhas criptografadas. Para gerar senhas criptografadas, proceda da seguinte maneira:

1. Vá para o subdiretório `bin` sob o diretório de instalação do WebSphere Commerce.
2. Execute o seguinte script a partir de uma linha de comandos:

   Windows `wcs_password.bat` *`password SALT merchant_key`*

   AIX Solaris Linux `./wcs_password.sh` *`password SALT merchant_key`* em que

- *password* é a senha de texto corrido.
- *SALT* é uma cadeia aleatória utilizada na geração de uma senha. Ele é encontrado na coluna SALT da tabela USERREG do banco de dados para o usuário específico cuja senha está sendo editada.
- *merchant_key* é a chave do comerciante digitada durante a criação da instância.

400 Para o iSeries alterar a senha criptografada para compradores, utilize o comando CHGWCSPWD. Consulte a ajuda online F1 para obter detalhes de execução deste comando.

Gerando Senhas Criptografadas para o Payment Manager

O WebSphere Commerce permite gerar senhas criptografadas para o Payment Manager. Para gerar senhas criptografadas, proceda da seguinte maneira:

1. Vá para o subdiretório bin sob o diretório de instalação do WebSphere Commerce.
2. Execute o seguinte script a partir de uma linha de comandos:

   Windows `wcs_pmpassword.bat password SALT`

   AIX Solaris Linux `./wcs_pmpassword.sh password SALT`

   em que:

   - *password* é a senha de texto corrido.
   - *SALT* é uma cadeia aleatória utilizada na geração de uma senha. Ele é encontrado na coluna SALT da tabela USERREG do banco de dados para o usuário específico cuja senha está sendo editada.

400 Para o iSeries, gerar senha criptografada para o Payment Manager, utilize o comandoCRTWCSPMPW. Consulte a ajuda online F1 para obter detalhes de execução deste comando.

Capítulo 8. Ativando o SSL para Produção com o IBM HTTP Server

400 Esta seção não se aplica à plataformaiSeries. Para obter informações do iSeries, consulte “Ativando o SSL no IBM HTTP Server (iSeries)” na página 81.

Após ter criado sua instância do WebSphere Commerce com o IBM HTTP Server, O SSL (Secure Sockets Layer) é ativado com finalidade de teste. Antes de abrir seu site para compradores, você deve ativar o SSL para produção seguindo as etapas indicadas neste capítulo.

Sobre Segurança

O IBM HTTP Server oferece um ambiente seguro para suas transações de negócios utilizando tecnologia de criptografia. A criptografia é uma codificação das informações das transações através da Internet para que estas não possam ser lidas até que sejam decodificadas pelo receptor. O emissor utiliza um modelo de algoritmos ou chaves para codificar (criptografar) uma transação, e o receptor utiliza uma chave de decriptografia. Estas chaves são utilizadas pelo protocolo SSL (Secure Sockets Layer).

Seu servidor Web utiliza um processo de autenticação para verificar a identidade da pessoa com quem você está fazendo negócio (isto é, certificar-se de que ela seja quem diz que é). Isto envolve obter um certificado assinado por terceiros confiáveis chamado CA (certification authority - autoridade de certificação). Para os usuários do IBM HTTP Server, a AC pode ser Equifax® ou VeriSign® Inc. Outras ACs também estão disponíveis.

Para criar um arquivo de chaves de produção, conclua as seguintes etapas:

1. Crie um arquivo de chaves de segurança para produção.
2. Solicite um certificado seguro a uma autoridade de certificação.
3. Defina seu arquivo de chaves de produção como o arquivo de chaves atual.
4. Receba o certificado e teste o arquivo de chaves de produção.

Estas etapas são descritas detalhadamente a seguir.

Notas:

1. Se você já estiver utilizando um arquivo de chaves de produção assinado por uma autoridade de certificação, poderá pular estas etapas. Leia este capítulo para determinar isso.
2. Conforme essas etapas são efetuadas, seu navegador poderá exibir mensagens de segurança. Reveja cuidadosamente as informações de cada mensagem e decida como continuar.

Criar um Arquivo de Chaves Seguro para Produção

Para criar um arquivo de chaves de segurança para produção, faça o seguinte em sua máquina do servidor Web:

1. Pare o IBM HTTP Server.
2. Mude o diretório para o subdiretório `conf` sob o subdiretório de instalação do IBM HTTP Server em sua máquina.

3. Crie uma cópia de backup do `httpd.conf`.
4. Abra `httpd.conf` em um editor de texto.
5. Certifique-se de que as linhas a seguir não estejam comentadas para a porta 443:
   - Windows

     ```
     #LoadModule ibm_ssl_module modules/IBMModuleSSL128.dll
     #Listen 443#Listen 443#<VirtualHost host.some_domain.com:443>
     #SSLEnable
     #</VirtualHost>
     #SSLDisableKeyfile "unidade:/WebSphere/HTTPServer/ssl/keyfile.kdb"
     #SSLV2Timeout 100
     #</VirtualHost>
     #SSLDisable
     ```

   - AIX Solaris Linux

     ```
     #LoadModule ibm_ssl_module modules/IBMModuleSSL128.dll
     #AddModule mod_ibm_ssl.c
     #Listen 443#<VirtualHost host.some_domain.com:443>
     #SSLEnable
     #</VirtualHost>
     #SSLDisableKeyfile "keyfile"
     #SSLV2Timeout 100
     #</VirtualHost>
     #SSLDisable
     ```

     em que *keyfile* é:

     AIX `/usr/HTTPServer/ssl/keyfile.kdb`

     Solaris `/opt/IBMHTTPD/ssl/keyfile.kdb`

     Linux `/opt/IBMHTTPServer/ssl/keyfile.kdb`
6. Certifique-se de que as linhas a seguir não estejam comentadas para a porta 8000:
   a. `#Listen 8000`
   b. `#<VirtualHost host.some_domain.com:8000>`. Você também deve substituir o nome completo do host nesta linha.
   c. `#SSLEnable`
   d. `#</VirtualHost>`

   Nota: É recomendado que seu software de firewall bloqueie o acesso externo à porta que você configurou para Ferramentas do WebSphere Commerce (porta 8000 por padrão). Consulte a documentação do software de firewall que você está utilizando em seu site para obter informações sobre como fazer isso.
7. Salve as alterações.
8. Para assegurar que seu arquivo `httpd.conf` não contém erros de sintaxe, altere o subdiretório `bin` sob o diretório de instalação do IBM HTTP Server em sua máquina e execute o seguinte comando:

   AIX Solaris Linux `./apachectl configtest`

   Windows `apachectl configtest`
9. Inicie o IBM HTTP Server.

Solicitar um Certificado Seguro de uma Autoridade de Certificação

Para validar o arquivo de chaves de segurança que você acabou de criar na etapa anterior, é necessário ter um certificado de uma CA (autoridade de certificação) como a Equifax ou a VeriSign. O certificado contém a chave pública do servidor, o Nome Distinto associado ao certificado do servidor e o número serial e a data de expiração do certificado.

Se deseja utilizar uma CA diferente, contate-a diretamente para obter as informações sobre o procedimento a seguir.

Usuários da Equifax

Para solicitar um certificado de servidor seguro da Equifax, consulte o seguinte endereço da Web e siga as instruções fornecidas:

`http://www.equifax.com`

Você deve receber o certificado de servidor seguro via E-mail da Equifax em um prazo de 2 a 4 dias úteis.

Usuários da VeriSign

Para solicitar um certificado de servidor seguro da VeriSign, consulte a seguinte URL e siga as instruções fornecidas:

`http://www.verisign.com`

AIX Embora você esteja utilizando os procedimentos para o IBM HTTP Server, clique no link **Internet Connection Secure Server** (ICSS). Siga as instruções fornecidas. Quando você receber seu certificado, crie o arquivo de chaves de produção, conforme descrito na seção anterior, caso ainda não o tenha feito.

Solaris Mesmo que você esteja utilizando os procedimentos para IBM HTTP Server, siga a ligação para ICSS **(Internet Connection Secure Server)**. A página seguinte indica que os procedimentos se aplicam às plataformas OS/2 e AIX. Estas instruções também aplicam-se ao software Solaris.

Siga as instruções fornecidas. O certificado deve chegar três a cinco dias úteis após você submeter o pedido. Quando você recebê-lo, crie o arquivo de chaves de produção, conforme descrito na seção anterior, caso ainda não o tenha feito.

Receber e Definir seu Arquivo de Chaves de Produção como o Arquivo de Chaves Atual

Quando o certificado chegar da CA, você deve fazer o servidor Web utilizar o arquivo de chaves de produção. Execute as seguintes etapas:

1. Copie os arquivos *certificatename*`.kdb`, *certificatename*`.rdb` e *certificatename*`.sth` que você recebeu da autoridade de certificação para o subdiretório `ssl` sob o caminho de instalação do IBM HTTP Server em sua máquina, em que *certificatename* é o nome do certificado que você forneceu com seu pedido de certificado.
2. Abra o utilitário do Key Management.
3. Abra o arquivo *certificatename*`.kdb` e digite sua senha quando solicitado.
4. Selecione **Certificados Pessoais** e clique em **Receber**.
5. Clique em **Navegar**.

6. Selecione a pasta onde você armazenou os arquivos recebidos da autoridade de certificação. Selecione o arquivo *certificatename*.txt e clique em **OK**.
7. O quadro de listagem **Certificados Pessoais**, agora, deve listar o certificado *certificatename* da VeriSign ou o certificado *certificatename* da Equifax.
8. Saia do Utilitário de Gerenciamento de Chaves.
9. Mude o diretório para o subdiretório conf sob o caminho de instalação do IBM HTTP Server em sua máquina.
10. Crie uma cópia de backup do httpd.conf.
11. Abra httpd.conf em um editor de texto.
12. Certifique-se de que as linhas listadas na etapa 5 na página 78 não estejam comentadas.
13. Pesquise a diretriz Keyfile "*keyfile path name*" e altere o nome do caminho para indicar o arquivo criado nas etapas anteriores.
14. Encerre e reinicie o IBM HTTP Server.

Testar o Arquivo de Chaves de Produção

Para testar a chave de produção, faça o seguinte:

1. Vá para a seguinte URL com seu navegador:

   https://*host_name*

   Notas:

   a. Se tiver personalizado o servidor Web, pode ser preciso digitar o nome da primeira página do servidor Web após o nome do host.
   b. Certifique-se de digitar https, e *não* http.

   Se a sua chave estiver definida corretamente, você verá várias mensagens sobre o seu novo certificado.
2. No painel **Novo Certificado do Site**, se desejar aceitar esse certificado, selecione o botão de opção **Aceitar esse certificado para sempre (até que ele expire)**.
3. No navegador Web, restaure as definições do servidor de armazenamento em cache e proxy (ou soquetes) para seus estados originais.

Agora, você ativou o SSL no servidor.

Consideração SSL para o Payment Manager

Por padrão, a comunicação entre o WebSphere Commerce e o Payment Manager é através do SSL. Porém, se você lançar a interface do usuário do Payment Manager diretamente como segue:

http://*host_name*/webapp/Paymentmanager/

então você está chamando o Payment Managerutilizando comunicação não SSL. Para garantir que a comunicação seja através do SSL, você deve utilizar

https://*host_name*/webapp/Paymentmanager/

ou renomear o arquivo indexSSL.html para index.html no seguinte diretório:

- Windows *WAS_HOME*\installedApps\IBM_PaymentManager.ear\PaymentManager.war
- AIX Solaris

  Linux *WAS_HOME*/installedApps/IBM_PaymentManager.ear/PaymentManager.war

Dessa maneira, é possível continuar a utilizar o diretório **http://***host_name*/webapp/Paymentmanager/ e o arquivo renomeado index.html redicionará para o https (SSL).

Ativando o SSL no IBM HTTP Server (iSeries)

400 A seção se aplica à plataforma iSeries.

O SSL é um protocolo de segurança. O SSL assegura que dados transferidos entre um cliente e um servidor permaneçam confidenciais. Isto permite ao cliente autenticar a identidade do servidor e ao servidor autenticar a identidade do cliente.

Certificados digitais são documentos eletrônicos que autenticam os servidores e os clientes envolvidos em transações de segurança na Internet. O emissor de certificados digitais é chamado de autoridade de certificação (CA). O sistema iSeries pode executar a função de CA em um ambiente Intranet emitindo certificados de servidor e de cliente e ser executado como um servidor autenticado com certificados de servidor emitidos por um CA do iSeries ou por um CA da Internet como o VeriSign®. Como um servidor Web, o IBM HTTP Server para iSeries também pode ser configurado para solicitar certificados de cliente para autenticação de clientes ativados pelo SSL.

Para obter informações detalhadas sobre como ativar o SSL no IBM HTTP Server para iSeries, consulte o seguinte endereço da Web:

www.ibm.com/software/webservers/commerce/servers/lit-tech-os400.html

Em particular, olhe na seção **Dicas e Sugestões**.

Utilizando o SSL com o Payment Manager

Se você criar a loja de certificado do sistema após criar sua instância do WebSphere Commerce, você deve conceder tanto a instância do Payment Manager como o acesso da instância do WebSphere Commerce para a loja do certificado do sistema. Por exemplo, os seguintes comandos concederão a instância do Payment Manager o acesso requerido em um sistema V5R1:

```
CHGAUT OBJ('/QIBM/UserData/ICSS/Cert/Server') USER(QPYMSVR) DTAAUT(*RX)
CHGAUT OBJ('/QIBM/UserData/ICSS/Cert/Server/DEFAULT.KDB') USER(QPYMSVR) DTAAUT(*R)
```

e os seguintes comandos concederão o acesso requerido do WebSphere Commerce em um sistema V5R1:

```
CHGAUT OBJ('/QIBM/UserData/ICSS/Cert/Server') USER(QEJBSVR) DTAAUT(*RX)
CHGAUT OBJ('/QIBM/UserData/ICSS/Cert/Server/DEFAULT.KDB') USER(QEJBSVR) DTAAUT(*R)
```

Se você optar por utilizar uma instância Payment Manager remota, é necessário configurar tanto a instância do WebSphere Commerce como a instância do Payment Manager para confiar a autoridade de certificado remota que emite o certificado digital. Para estabelecer um relacionamento de confiança entre os dois aplicativos remotos, consulte o seguinte procedimento de alto nível:

1. Na máquina do WebSphere Commerce, utilize o Digital Certificate Manager para exportar a autoridade de certificado do servidor.
2. Transfira o arquivo de certificado para a máquina do Payment Manager.
3. Na máquina do Payment Manager, utilize o Digital Certificate Manager para importar a autoridade do certificado do servidor do WebSphere Commerce server.

4. Configure o servidor de aplicativo do Payment Manager para confiar a autoridade importada de certificado do servidor WebSphere Commerce.
5. Na máquina do Payment Manager, utilize o Digital Certificate Manager para exportar a autoridade de certificado do servidor.
6. Transfira o arquivo de certificado para a máquina doWebSphere Commerce.
7. Na máquina do WebSphere Commerce, utilize o Digital Certificate Manager para importar a autoridade de certificado do servidor do Payment Manager.
8. Configure o servidor de aplicativo do WebSphere Commerce para confiar a autoridade importada de certificado do servidor do Payment Manager.

Para informações mais detalhadas, consulte o seguinte endereço da Web e procure por **Dicas e Sugestões**.:

`www.ibm.com/software/webservers/commerce/servers/lit-tech-os400.html`

Capítulo 9. Ativação do SSL para o IBM SecureWay Directory Server (LDAP)

A seguir estão as etapas para configurar a segurança SSL para o IBM SecureWay Directory Server e o WebSphere Commerce.

Configurar o SecureWay

Para configurar o IBM SecureWay Directory Server:

1. Instale o IBM SecureWay Directory Server de acordo com as instruções de instalação do produto SecureWay Directory Server. Certifique-se de instalar o componente GSKit:
2. Após a conclusão da instalação, chame o IBM Key Manager (*unidade*:\Program Files\IBM\GSK4\bin\gsk4ikm.exe no Windows).
3. Crie um novo arquivo de banco de dados de chave CMS. Certifique-se de que **senha de armazenamento para arquivo** esteja selecionada (por exemplo,ldap_key.kdb)
4. Crie um certificado auto-assinado.
5. Extraia o certificado como o tipo de dados Dados ASCII baseados em Base64.
6. Crie uma nova classe de banco de dados de chave SSLight (por exemplo, keyring.class).
7. Na seção **Certificados Singer**, inclua o arquivo de certificado criado na etapa 5.
8. Abra um navegador para o seguinte endereço: http://hostname/ldap
9. Clique em **Segurança —> SSL —> Definições** e faça as seguintes alterações:
   - Status SSL: SSL ativo ou somente SSL
   - Método de autenticação: Autenticação do Servidor
   - Porta de segurança: 636
   - Caminho e nome do arquivo do banco de dados de chave:

     AIX Solaris Linux /Keys/ldap_key.kdb

     Windows *unidade* :\Keys\ldap_key.kdb
   - Rótulo de chave: *your_label* (O rótulo do certificado)
10. Clique em **Update** e inicie novamente o SecureWay.

WebSphere Commerce

Para configurar o WebSphere Commerce de forma que trabalhe com o SecureWay Directory Server, você precisa modificar o arquivo *instance*.xml:

```
java.naming.security.ssl.keyring = keyring
'keyring' é o nome da classe do banco de dados de chave SSLight (keyring.class).
Esse arquivo de classe deve ser colocado no caminho de classe no WAS.

java.naming.security.ssl.authentication = ibm
'ibm' é a senha especificada ao criar a classe do banco de dados de chave SSLight.

java.naming.security.protocol = ssl
LdapPort = 636
```

```
<MemberSubSystem name="Member SubSystem"
                     ProfileDataStorage="LDAP"
                     AuthenticationMode="LDAP">
  <Directory LdapAdminDN="cn=root"
                 LdapAuthenticationMode="SIMPLE"
                 LdapTimeOut="0"
                 LdapVersion="3"
                 EntryFileName="WC_Install_Dir/xml/ldap/ldapentry.xml"
                 LdapPort="636"
                 SingleSignOn="0"
                 LdapAdminPW="EaDPFd9VAf0="
                 LdapHost="yazhuang.torolab.ibm.com"
                 MigrateUsersFromWCSdb="ON"
                 JNDIEnvPropName1="java.naming.security. ssl.keyring"
                 JNDIEnvPropValue1="keyring"
                 JNDIEnvPropName2="java.naming.security.ssl.authentication"
                 JNDIEnvPropValue2="ibm"
                 JNDIEnvPropName3="java.naming.security.protocol"
                 JNDIEnvPropValue3="ssl"
                 display="false"
                 LdapType="SECUREWAY" />
</Membersubsystem>
```

Reinicie o WebSphere Commerce.

Capítulo 10. Sign-on Único

Esse capítulo descreve como configurar sign-on único para o WebSphere Commerce.

Pré-requisitos

Para ativar o sign-on único, você deve atender os seguintes requisitos:

- Deve existir um servidor LDAP instalado e configurado. Para configurar um servidor LDAP, consulte a publicação *IBM WebSphere Commerce Version 5.4 Manual de Software Adicional*.
- O WebSphere Commerce deve estar instalado e configurado para utilizar o LDAP.
- A segurança do WebSphere Application Server deve estar ativada. Para ativar a segurança do WebSphere Application Server, consulte Capítulo 5, "Ativando a Segurança do WebSphere Application Server" na página 55.

Ativando Sign-on Único

Limitações

Existem algumas limitações importantes para o sign-on único quando é utilizado com o WebSphere Commerce. São elas:

- Os cookies do LTPA podem fluir entre diferentes portas de servidor da Web.
- Talvez seja necessário modificar o arquivo `ldapentry.xml` e incluir a classe de objeto `ePerson`. Esse é um atributo do elemento `ldapocs`.
- É necessário modificar `instance.xml` e assegurar que a migração esteja ″ativada″ para o usuário no componente LDAP.
- As máquinas participando da configuração de sign-on único devem ter os relógios de seus sistemas sincronizados.
- O sign-on único só é suportado entre aplicativos que possam ler e emitir o token LTPA (Light Weight Third Party Authentication) do WebSphere Application Server.

Para ativar o sign-on único você deve fazer o seguinte:

1. Ativar o sign-on único no WebSphere Application Server. Para obter mais informações pesquise por ″sign-on único″ no InfoCenter do WebSphere Application Server disponível no endereço:

   ```
   http://www.ibm.com/software/webservers/appserv/doc/v40/ae
     /infocenter/index.html
   ```

   Selecione **Sign-on Único: WebSphere Application Server** e conclua as seções a seguir:

   - **Configurando SSO para WebSphere Application Server** .
     - **Modificar as definições de segurança do WebSphere Application Server**.

       Nota: A etapa que detalha como preencher os campos do LDAP pode ser ignorada com segurança.

– **Exportar as chaves de LTPA para um arquivo**.

2. Em sua máquina WebSphere Commerce, inicie o Gerenciador de Configuração do WebSphere Commerce.
3. Para configurar o nó **Subsistema de Membros**, faça o seguinte:
   a. Expanda **WebSphere Commerce** → *host_name* → **Lista de Instâncias** → *instance_name* → **Propriedades da Instância** → **Subsistema de Membros**.
   b. No menu drop-down **Modo de Autenticação**, selecione **LDAP**.
   c. Ative a caixa de opção **Sign-on único**.
   d. No campo **Host**, digite o nome completo do seu servidor LDAP.
   e. Digite o nome distinto do administrador no campo **Nome Distinto do Administrador**. Deve ser o mesmo nome que foi utilizado no seu servidor LDAP.
   f. No campo **Senha do Administrador**, digite a senha do administrador. Deve ser a mesma senha que foi utilizada no seu servidor LDAP. Confirme a senha no campo **Confirmar Senha**.
   g. Preencha cada um dos campos remanescentes.
   h. Clique em **Aplicar**, em seguida clique em **OK**.
4. Reinicie o WebSphere Application Server.

Parte 4. Tarefas de Segurança do Desenvolvedor do WebSphere Commerce

Essa parte descreve as tarefas de segurança que devem ser feitas com a programação do WebSphere Commerce. Essas tarefas são geralmente executadas por programadores do WebSphere Commerce.

Capítulo 11. Controle de Acesso

Compreendendo o Controle de Acesso

O modelo de controle de acesso de um aplicativo WebSphere Commerce tem três conceitos principais: usuários, ações e recursos. Usuários são as pessoas que utilizam o sistema. Recursos são as entidades que são mantidas no aplicativo ou por ele. Por exemplo, recursos podem ser produtos, documentos ou pedidos. Os perfis de usuários que representam pessoas também são recursos. Ações são as atividades que os usuários podem executar nos recursos. O controle de acesso é o componente do aplicativo de e-commerce que determina se um determinado usuário pode executar uma determinada ação em um recurso específico.

Em um aplicativo WebSphere Commerce, há dois níveis principais de controle de acesso. O primeiro nível de controle de acesso é executado pelo WebSphere Application Server. Em relação a isso, o WebSphere Commerce utiliza o WebSphere Application Server para proteger beans corporativos e servlets. O segundo nível do controle de acesso é o sistema de controle de acesso fino do WebSphere Commerce.

A estrutura de controle de acesso do WebSphere Commerce utiliza as políticas de controle de acesso para determinar se um determinado usuário pode executar uma ação específica em um recurso específico. Essa estrutura de controle de acesso fornece controle de acesso minucioso. Ela funciona em conjunto, mas não substitui o controle de acesso fornecido pelo WebSphere Application Server.

Visão Geral de Proteção de Recursos no WebSphere Application Server

Os recursos do WebSphere Commerce a seguir são protegidos pelo controle de acesso do WebSphere Application Server:

- Beans de entidade
  Esses beans modelam objetos em um aplicativo e-commerce. Eles são objetos distribuídos que podem ser acessados por clientes remotos.
- Modelos JSP
  O WebSphere Commerce utiliza modelos JSP para exibir páginas. Cada modelo JSP pode conter um ou mais beans de dados que recuperam dados dos beans de entidade. Os clientes podem solicitar páginas JSP através da composição de um pedido de URL.
- Comandos do controlador e de exibição
  Os clientes podem solicitar os comandos do controlador e de exibição através da composição de pedidos de URL. Além disso, uma página de exibição pode conter um link para outra utilizando o nome do arquivo JSP ou o nome de exibição, conforme registrado na tabela VIEWREG.

O WebSphere Commerce server geralmente é configurado para utilizar os seguintes caminhos na Web:

- `/webapp/wcs/stores/servlet/*`
  É utilizado para solicitações para o servlet de solicitação.
- `/webapp/wcs/stores/*.jsp`
  Utilizado para solicitações para o servlet JSP.

O diagrama a seguir mostra a rota que as solicitações poderiam seguir para acessar os recursos do WebSphere Commerce, para a configuração do caminho da Web acima.

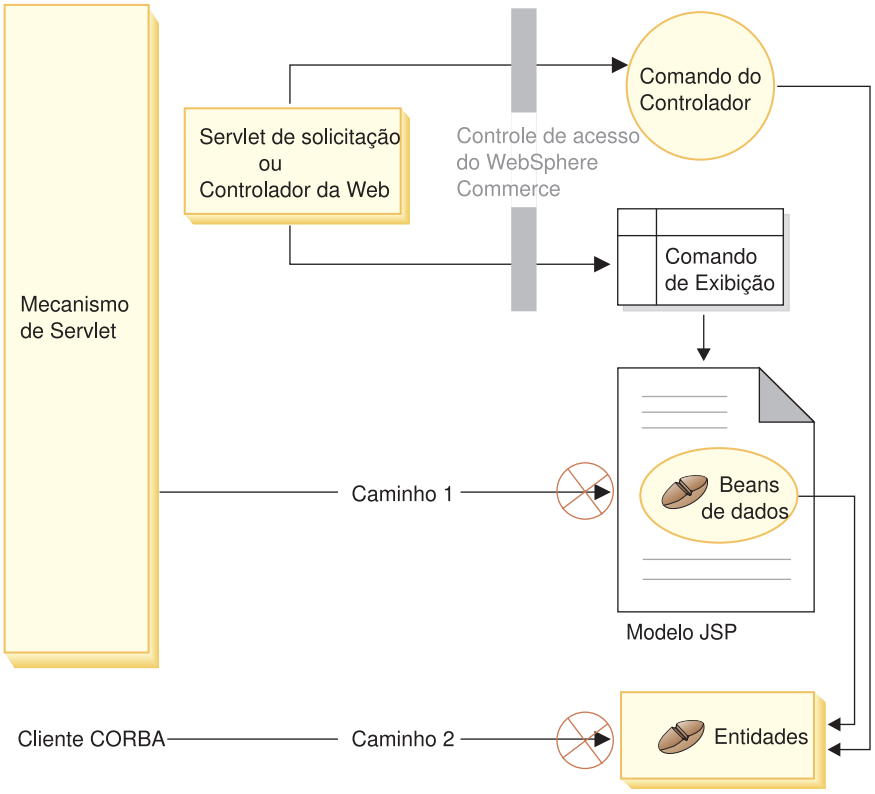


Figura 3.

Todos os pedidos legítimos devem ser direcionados para o Servlet de solicitação, que, em seguida, os direciona para o Controlador da Web. O Controlador da Web implementa o Controle de acesso do Comando do Controlador e da Exibição. Os caminhos da Web mostrados acima fazem isso, entretanto, possibilita que usuários maliciosos acessem diretamente o Modelos JSP (caminho 1) e os beans de entidade (caminho 2). A fim de evitar que esse procedimento dos usuários seja bem-sucedido, ele deve ser rejeitado em tempo de execução.

O acesso direto ao Modelo JSP e aos beans de entidade podem ser evitados utilizando uma das seguintes abordagens:

Segurança do WebSphere Application Server
O WebSphere Application Server fornece um recurso de segurança. Utilizando essa abordagem, todos os métodos de bean corporativo e Modelo JSP serão configurados para que sejam invocados apenas pela Identidade do Sistema. Para acessar estes recursos do WebSphere Commerce, um pedido de URL deve ser roteado para o servlet de pedido que define a Identidade do Sistema para o thread atual, passando-o antes ao controlador da Web. O controlador da Web garante, então, que o originador da chamada possui a autorização requerida antes de passar o pedido ao comando do controlador ou exibição correspondente. Todas as tentativas para acessar diretamente o Modelo JSP e os Beans de entidades (ou seja, sem utilizar o controlador da Web) serão rejeitadas pelo componente de segurança do WebSphere Application Server.

Para obter informações sobre como configurar o WebSphere Application Server para assegurar recursos do WebSphere Commerce, consulte o *WebSphere Commerce Manual de Instalação*. Para obter informações sobre segurança dentro do WebSphere Application Server, consulte o tópico Administração do Sistema na documentação do WebSphere Application Server.

Para obter informações sobre a configuração de segurança do WebSphere Application Server para métodos em beans corporativos personalizados, consulte as seções ″Construindo um novo bean corporativo no aplicativo corporativo″ e ″Construindo um bean corporativo modificado no aplicativo corporativo″ no *WebSphere Commerce 5.4 - Manual do Programador*.

Proteção de Firewall

Quando um WebSphere Commerce Server é executado atrás de um firewall, os clientes da Internet não conseguem acessar diretamente os beans de entidade. Utilizando essa abordagem, a proteção dos modelos JSP é fornecida pelo bean de dados que está incluído nesta página. O bean de dados é ativado pelo gerenciador de bean de dados. O gerenciador de bean de dados detecta se o modelo JSP foi encaminhado por um comando de exibição. Se não foi encaminhado por um comando de exibição, será lançada uma exceção e o pedido para o modelo JSP será rejeitado.

Introdução às Políticas de Controle de Acesso do WebSphere Commerce

O modelo de controle de acesso do WebSphere Commerce baseia-se na aplicação de políticas de controle de acesso. As políticas de controle de acesso permitem que as regras de controle de acesso sejam exteriorizadas do código da lógica de negócios, removendo então a necessidade de colocar as instruções de controle de acesso em código permanente. Por exemplo, não é necessário incluir código similar ao seguinte:

```
if (user.isAdministrator())
   then {}
```

As políticas de controle de acesso são aplicadas pelo gerenciador de políticas de controle de acesso. Em geral, quando um usuário tenta acessar um recurso protegido, o gerenciador de política de controle de acesso primeiro determina quais políticas de controle de acesso são aplicáveis para o recurso protegido e, em seguida, com base nas políticas de controle de acesso aplicáveis, determina se o usuário pode acessar os recursos solicitados.

Uma política de controle de acesso é uma política de 4 tuplas armazenada na tabela ACPOLICY. Cada política de controle de acesso tem o seguinte formato:

```
AccessControlPolicy [UserGroup, ActionGroup, ResourceGroup, Relationship]
```

Os elementos na política de controle de acesso de 4-tuplas especificam que um usuário pertence a um grupo de acesso específico tem permissão para executar ações no grupo de ação especificando nos recursos que pertencem ao grupo de recursos especificado, desde que o usuário atenda às condições especificadas no relacionamento ou grupo de relacionamento com relação ao recurso em questão. Por exemplo, `[AllUsers, UpdateDoc, doc, creator]` especifica que todos os usuários podem atualizar um documento, caso sejam o criador do documento.

O grupo de usuários é um tipo específico de grupo de membros definido na tabela de banco de dados MBRGRP. Um grupo de usuários precisa estar associado ao tipo de grupo de membros `-2`. O valor `-2` representa um grupo de acesso e está

definido na tabela MBRGRPTYPE. A associação entre o tipo do grupo de usuários e do grupo de membros está armazenada na tabela MBRGRPUSG.

A associação de um usuário a um grupo de usuários específico pode ser declarada explícita ou implicitamente. Uma especificação explícita ocorre se a tabela MBRGRPMBR afirmar que o usuário pertence a um grupo de membros específico. Uma especificação implícita ocorre se o usuário atender a uma condição (por exemplo, todos os usuários que tiverem a função de Gerente de Produto) declarada na tabela MBRGRPCOND. Pode haver também condições combinadas (por exemplo, todos os usuários que tiverem a função de Gerente de Produtos e que estejam no cargo há pelo menos 6 meses) ou exclusões explícitas.

A maioria das condições de inclusão ou exclusão de um usuário em um grupo de usuários está baseada no atendimento de uma função específica pelo usuário. Por exemplo, pode existir uma política de controle de acesso que permita que todos os usuários que preencham a função de Gerente de Produtos, executem operações de gerenciamento de catálogo. Nesse caso, qualquer usuário que tenha a função de Gerente de Produtos atribuída na tabela MBRROLE estará incluído implicitamente no grupo de usuários.

Para obter mais detalhes sobre o subsistema de grupos de membros, consulte a ajuda online do WebSphere Commerce.

O elemento ActionGroup vem da tabela ACACTGRP. Um grupo de ações refere-se a um grupo de ações especificado explicitamente. A listagem de ações está armazenada na tabela ACACTION e o relacionamento de cada ação com seu(s) grupo(s) de ação está armazenado na tabela ACACTACTGP. Um exemplo de um grupo de ações é o ″OrderWriteCommand″. Esse grupo de ações inclui as seguintes ações que são utilizadas para atualizar pedidos:

- com.ibm.commerce.order.commands.OrderDeleteCmd
- com.ibm.commerce.order.commands.OrderCancelCmd
- com.ibm.commerce.order.commands.OrderProfileUpateCmd
- com.ibm.commerce.order.commands.OrderUnlockCmd
- com.ibm.commerce.order.commands.OrderScheduleCmd
- com.ibm.commerce.order.commands.ScheduledOrderCancelCmd
- com.ibm.commerce.order.commands.ScheduledOrderProcessCmd
- com.ibm.commerce.order.commands.OrderItemAddCmd
- com.ibm.commerce.order.commands.OrderItemDeleteCmd
- com.ibm.commerce.order.commands.OrderItemUpdateCmd
- com.ibm.commerce.order.commands.PayResetPMCmd

Um grupo de recursos é um mecanismo para agrupar tipos específicos de recursos. A associação de um recurso a um grupo de recursos pode ser especificada de uma das seguintes maneiras:

- Utilizando a coluna de condições da tabela ACRESGRP
- Utilizando a tabela ACRESGPRES

Na maioria dos casos, utilizar a tabela ACRESGPRES para associar recursos a um grupo de recursos é suficiente. Através desse método, os recursos são definidos na tabela ACRESCGRY utilizando seus nomes de classe Java. Então, esses recursos são associados aos grupos de recursos adequados (tabela ACRESGRP) utilizando-se a tabela de associação ACRESGPRES. Nos casos em que o próprio nome de classe Java não é suficiente para definir os membros de um grupo de recursos (por

exemplo, se você precisar restringir mais objetos dessa classe com base em um atributo do recurso), o grupo de recursos não pode ser definido inteiramente utilizando-se a coluna Condições da tabela ACRESGRP. Observe que para executar esse agrupamento de recursos com base em um atributo, o recurso também deve implementar a interface Groupable.

O diagrama a seguir mostra um exemplo de uma especificação de agrupamento de recursos. Nesse grupo de recursos de exemplo, `10023` inclui todos os recursos associados a ele na tabela ACRESGPRES. O grupo de recursos `10070` é definido utilizando-se a coluna do campo de condições da tabela ACRESGRP. Esse grupo de recursos inclui instâncias da interface remota do Pedido que também têm status = `"Z"` (especificando uma lista de requisições compartilhada).

Nota: Os detalhes sobre as informações XML para a coluna Condições da tabela ACRESGRP são encontrados no *WebSphere Commerce - Manual de Controle de Acesso*.

ACRESGRP

AcResGrp_Id	GrpName	Condições
10023	AccountRepresentatives CmdResourceGroup	null
10070	SharedRequisitionList ResourceGroup	<profile> <andListCondition> <simpleCondition> <variable name="Status"/> <operator name="="/> <value data="Z"/> </simpleCondition> <simpleCondition> <variable name="classname"/> <operator name="="/> <value data="com.ibm.commerce.order.objects.Order"/> </simpleCondition> </andListCondition> </profile>

ACRESGRPES

AcResGrp_Id	AcResCgry_Id
10023	10246
10023	10247
10023	10248
10023	10249
10023	10250

ACRESCGRY

AcResCgry_Id	ResClassname
10246	com.ibm.commerce.contract.commands.ContractCreateCmd
10247	com.ibm.commerce.contract.commands.ContractCreateCmd
10248	com.ibm.commerce.contract.commands.ContractCreateCmd
10249	com.ibm.commerce.contract.commands.ContractCreateCmd
10250	com.ibm.commerce.contract.commands.ContractCreateCmd

Figura 4.

A coluna MEMBER_ID das tabelas ACACTGRP, ACRESGRP e ACRELGRP deve ter um valor `-2001` (Organização Raiz).

A política de controle de acesso pode opcionalmente incluir um elemento Relationship ou RelationshipGroup como seu quarto elemento.

Se a política de controle de acesso utilizar um elementoRelationship, este virá da tabela ACRELATION. Se, por outro lado, ela incluir um elemento RelationshipGroup, este virá da tabela ACRELGRP. Observe que nenhum precisa ser incluído, mas se você incluir um, não poderá incluir o outro. Uma especificação RelationshipGroup da tabela ACRELGRP tem precedência sobre as informações de Relationship da tabela ACRELATION.

A tabela ACRELATION especifica os tipos de relacionamentos que existem entre usuários e recursos. Alguns exemplos de tipos de relacionamentos incluem o criador, o submissor e o proprietário. Um exemplo do uso do elemento relationship é utilizá-lo para assegurar que o criador de um pedido possa sempre atualizar o pedido.

A tabela ACRELGRP especifica os tipos de grupos de relacionamentos que podem ser associados a recursos específicos. Um grupo de relacionamentos é um agrupamento de uma ou mais cadeias de relacionamentos. Uma cadeia de relacionamentos é uma série de um ou mais relacionamentos. Um exemplo de um grupo de relacionamentos é especificar que um usuário deve ser o criador do recurso e também pertencer à entidade organizacional de compra referida no recurso.

A especificação do grupo de relacionamentos (ou relacionamento) é uma parte opcional da política de controle de acesso. Ela será normalmente utilizada se você tiver criado seus próprios comandos e estes não estiverem restritos a determinadas funções. Nesses casos, você poderá querer reforçar um relacionamento entre o usuário e o recurso. Geralmente, se os comandos tiverem de ser restritos a determinadas funções, isso será executado através do elemento UserGroup da política de controle de acesso em vez de através do elemento Relationship.

Outro conceito importante relacionado a políticas de controle de acesso é o de um *proprietário* de política de controle de acesso. Um proprietário de política de controle de acesso é a entidade organizacional que possui a política de controle de acesso. Conhecer o proprietário de uma política de controle de acesso é importante porque uma política de controle de acesso pode ser aplicada apenas a recursos que são de propriedade do proprietário da política de controle de acesso.

Para cada recurso em questão, o gerenciador de política de controle de acesso aplica políticas de controle de acesso que sejam de propriedade da entidade organizacional ou de suas entidades organizacionais superiores na hierarquia de membros, até que uma política que conceda permissão seja encontrada ou até que todas as políticas tenham sido verificadas e nenhuma permissão concedida.

Considere o seguinte diagrama, que mostra uma hierarquia de membros.

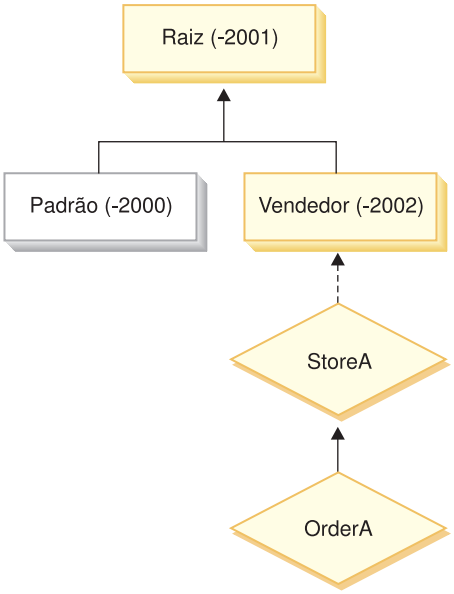


Figura 5.

Para o recurso "OrderA", qualquer política de controle de acesso que seja de propriedade da organização de Vendedor ou Raiz pode ser aplicada. Se o gerenciador da política de controle de acesso encontrar uma política pertencente a qualquer uma dessas organizações que conceda permissão ao usuário (baseado nos quatro elementos da política de controle de acesso) ele irá parar imediatamente a pesquisa nas políticas de controle de acesso. No entanto, se não encontrar nenhuma política de controle de acesso pertencente a essas organizações que conceda a permissão ao usuário para executar a ação nos recursos protegidos, então o acesso será negado.

Grupos de Relacionamentos

Um grupo de relacionamentos permite especificar vários relacionamentos. Um relacionamento pode ser diretamente entre um usuário e o recurso em questão ou ser uma cadeia de relacionamentos que relaciona indiretamente o usuário ao recurso.

Nota: Para as seguintes seções relacionadas a grupos de relacionamento, é importante reconhecer que as únicas organizações disponíveis no WebSphere Commerce Professional Edition são RootOrganization, DefaultOrganization e SellerOrganization. Os exemplos que referem-se a outras organizações, aplicam-se somente ao WebSphere Commerce Business Edition.

Comparando relacionamentos e grupos de relacionamentos: As políticas de controle de acesso podem especificar um usuário que deve cumprir um relacionamento específico com relação ao recurso que está sendo acessado ou elas podem especificar que um usuário deve cumprir as condições especificadas em um grupo de relacionamentos.

Na maioria dos casos, a especificação de um relacionamento deve satisfazer os requisitos de controle de acesso de seu aplicativo. Se, no entanto, a política for tal que você deve especificar um relacionamento que não está diretamente entre o usuário e o recurso, mas que seja na verdade uma série de relacionamentos entre o usuário e o recurso, será então necessário utilizar um grupo de relacionamentos.

Por exemplo, se você precisar especificar uma associação entre um usuário e uma organização de compra na qual o relacionamento requer que o usuário exerça uma função específica para essa organização ou que ele seja membro de uma organização de compra, então será necessário utilizar um grupo de relacionamentos e uma cadeia de relacionamentos.

Se você simplesmente precisar reforçar uma associação que está diretamente entre o usuário e o recurso em questão, poderá utilizar um relacionamento simples. Por exemplo, seria o caso se você precisasse reforçar que o usuário deve ser o criador do recurso.

Se você combinar vários relacionamentos simples, por exemplo, o usuário deve ser o criador *ou* o submissor, então isso se tornará uma cadeia de relacionamentos e você precisará utilizar um grupo de relacionamentos. Essa combinação de relacionamentos simples poderá ocorrer ao utilizar o WebSphere Commerce Professional Edition ou o WebSphere Commerce Business Edition.

Informações gerais sobre grupos de relacionamentos: Uma cadeia de relacionamentos é uma série de um ou mais relacionamentos. O comprimento de uma cadeia de relacionamentos é determinado pelo número de relacionamentos que ela contém. Isso pode ser determinado examinando-se o número de elementos de `<parameter name="aName" value="aValue" />` na representação XML da cadeia de relacionamentos.

Somente o último elemento `<parameter name="Relationship" value="aValue" />` deve ser manipulado pelo método fulfills() do recurso. O restante é manipulado internamente pelo gerenciador de política de controle de acesso.

Quando uma cadeia de relacionamentos tem um comprimento 2, o primeiro elemento `<parameter name="aName" value="aValue" />` está entre um usuário e uma entidade organizacional.O último elemento `<parameter name="aName" value="aValue" />` está entre uma entidade organizacional e o recurso.

Se você precisar definir grupos de relacionamentos, deverá fazê-lo através da definição das informações do grupo de relacionamentos em um arquivo XML. Você pode modificar o arquivo `defaultAccessControlPolicies.xml` ou criar seu próprio arquivo XML. Para obter mais informações sobre a criação dessas informações baseadas em XML, consulte o *WebSphere Commerce - Manual de Controle de Acesso*.

As seguintes seções mostram exemplos de tipos diferentes de grupos de relacionamentos.

Grupos de relacionamentos compostos de uma única cadeia de relacionamentos:

Business Como parte de uma política de controle de acesso, você pode ser solicitado a reforçar que um usuário deve pertencer à entidade organizacional que é a BuyingOrganizationalEntity do recurso. Isso requer a criação de um grupo de relacionamentos composto de uma cadeia de relacionamentos que tem comprimento dois. O comprimento da cadeia de relacionamentos é determinado como "dois", porque ele consiste em dois relacionamentos separados. O primeiro relacionamento está entre o usuário e sua entidade organizacional pai. O usuário é o "filho" nesse relacionamento. Para o segundo relacionamento, o gerenciador de política de controle de acesso verifica se a entidade organizacional pai preenche o relacionamento BuyingOrganizationalEntity com o recurso. Em outras palavras, ele retornará "true" se for a entidade organizacional de compra do recurso.

O seguinte fragmento XML foi obtido do arquivo `defaultAccessControlPolicies.xml` e mostra como definir esse tipo de grupo de relacionamentos:

```
<RelationGroup Name="MemberOf->BuyerOrganizationalEntity"
     OwnerID="RootOrganization">
 <RelationCondition><![CDATA[
   <profile>
    <openCondition name="RELATIONSHIP_CHAIN">
     <parameter name="HIERARCHY" value="child"/>
     <parameter name="RELATIONSHIP" value="BuyingOrganizationalEntity"/>
    </openCondition>
   </profile>
 ]]></RelationCondition>
</RelationGroup>
```

Business Outro exemplo seria reforçar que o usuário deve ter a função de Representante de Contas para a entidade organizacional que é a entidade organizacional de compra do recurso em questão. Novamente, isso utiliza um grupo de relacionamentos composto de uma cadeia de relacionamentos que tem comprimento dois. A primeira parte da cadeia encontrará todas as entidades organizacionais nas quais o usuário tem a função Representante de Contas. Então, para esse conjunto de entidades organizacionais, o gerenciador de política de controle de acesso verifica se pelo menos uma delas preenche o relacionamento BuyingOrganizationalEntity com o recurso. Em outras palavras, ele retornará true se uma delas for a entidade organizacional de compra do recurso.

O seguinte fragmento XML foi obtido do arquivo `defaultAccessControlPolicies.xml` e mostra como definir esse tipo de grupo de relacionamentos:

```
<RelationGroup Name="AccountRep->BuyerOrganizationalEntity"
     OwnerID="RootOrganization">
 <RelationCondition><![CDATA[
   <profile>
    <openCondition name="RELATIONSHIP_CHAIN">
            <parameter name="ROLE" value="Account Representative"/>
            <parameter name="RELATIONSHIP" value="BuyingOrganizationalEntity"/>
    </openCondition>
   </profile>
 ]]></RelationCondition>
</RelationGroup>
```

Grupos de relacionamentos compostos de várias cadeias de relacionamentos: É possível compor um grupo de relacionamentos para que ele contenha várias cadeias de relacionamentos. Ao fazer isso, você deve especificar se o usuário deve satisfazer todas as cadeias de relacionamentos, o que significa que é um cenário *AND* ou se o usuário deve satisfazer pelo menos uma das cadeias de relacionamentos, o que significa que é um cenário *OR*.

Business Para demonstrar esse tipo de relacionamento, o seguinte fragmento XML é utilizado para reforçar que um usuário deve ser o criador do recurso e que ele também deve pertencer à BuyingOrganizationalEntity especificada no recurso. A primeira cadeia, que especifica que o usuário deve ser o criador do recurso, tem comprimento um. A segunda cadeia que especifica que o usuário deve pertencer à BuyingOrganizationalEntity especificada no recurso tem comprimento dois.

```
<RelationGroup Name="Creator_And_MemberOf->BuyerOrganizationalEntity"
      OwnerID="RootOrganization">
 <RelationCondition><![CDATA[
  <profile>
   <andListCondition>
```

```
    <openCondition name="RELATIONSHIP_CHAIN">
     <parameter name="RELATIONSHIP" value="creator" />
    </openCondition>
    <openCondition name="RELATIONSHIP_CHAIN">
     <parameter name="HIERARCHY" value="child"/>
     <parameter name="RELATIONSHIP" value="BuyingOrganizationalEntity"/>
    </openCondition>
   </andListCondition>
  </profile>
 ]]></RelationCondition>
</RelationGroup>
```

Se, em vez do cenário *AND*, você solicitar que o usuário satisfaça qualquer uma das duas cadeias de relacionamentos, a tag `<andListCondition>` deverá ser alterada para a tag `<orListCondition>`.

Professional Business Para demonstrar um grupo de relacionamentos que pode ser utilizado no WebSphere Commerce Professional Edition (bem como no WebSphere Commerce Business Edition), considere um grupo de relacionamentos que é utilizado para reforçar que o usuário deve ser o criador ou o submissor do recurso. Isso é mostrado no seguinte fragmento.

```
<RelationGroup Name="Creator_Or_Submitter"
     OwnerID="RootOrganization">
   <RelationCondition><![CDATA [
   <profile>
      <orListCondition>
         <openCondition name="RELATIONSHIP_CHAIN">
            <parameter name="RELATIONSHIP"value="creator"/>
         </openCondition>
         <openCondition name="RELATIONSHIP_CHAIN">
            <parameter name="RELATIONSHIP"value="submitter"/>
         </openCondition>
      </orListCondition>
   </profile>
   ]]></RelationCondition>
</RelationGroup>
```

Tipos de Controle de Acesso

Há dois tipos de controle de acesso, os dois são baseados em políticas: controle de acesso no nível de comando e controle de acesso no nível de recurso.

O controle de acesso no nível de comando (também conhecido como baseado na função) utiliza um tipo amplo de política. É possível especificar que todos os usuários de uma função específica podem executar determinados tipos de comandos. Por exemplo, você pode especificar que os usuários com a função Representante de Contas podem executar qualquer comando no grupo de recursos AccountRepresentativesCmdResourceGroup. Ou, como descrito no diagrama a seguir, outra política de exemplo especifica que todos os administradores de loja podem executar qualquer ação especificada no Grupo ExecuteCommandAction em qualquer recurso que é especificado pelo StoreAdminCmdResourceGrp.

Nota: As informações XML para a coluna Condições da tabela ACRESGRP são geradas quando você utiliza o Administration Console para configurar grupos de acesso. Para obter informações sobre a utilização do Administration Console para configurar grupos de acesso, consulte a ajuda online do WebSphere Commerce.

ACPOLICY

PolicyName	Member_Id	MbrGrp_Id	AcActGrp_id	AcResGrp_Id	AcRelGrp_Id
StoreAdministrators ExecuteStoreAdmin CmdResourceGroup	-2001	-8	10052	10018	null

MBRGRP

MbrGrp_Id	MbrGrpName
-8	StoreAdministrators

MBRGRPCOND

MbrGrp_Id	Condições
-8	<profile> <simpleCondition> <variable name="role"/> <operator name="="/> <value data="Store Administrator"/> </simpleCondition> </profile>

ACACTGRP

AcActGrp_Id	GroupName
10052	ExecuteCommandActionGroup

ACRESGRP

AcResGrp_Id	GrpName
10018	StoreAdminCmdResourceGroup

Figura 6.

Uma política de controle de acesso no nível de comando sempre tem o `ExecuteCommandActionGroup` como o grupo de ações para comandos do controlador. Para as exibições, o grupo de recursos sempre é `ViewCommandResourceGroup`.

Todos os comandos do controlador devem ser protegidos pelo comando-controle de nível de acesso. Além disso, qualquer exibição que possa ser chamada diretamente ou que possa ser lançada por um redirecionador de outro comando (em contraste a ser lançado pelo encaminhamento da visualização) pode ser protegido pelo comando-controle de nível de acesso.

O comando-controle de nível de acesso não considera o recurso sobre o qual o comando agiria. Ele meramente determina se o usuário tem permissão para executar o comando específico. Se o usuário tiver permissão para executar o comando, uma política de controle de acesso no nível do recurso subseqüente poderá ser aplicada para determinar se o usuário pode acessar o recurso em questão.

Considere quando um administrador de loja tenta executar uma tarefa administrativa. O primeiro nível de verificação de controle de acesso seria determinar se o usuário tem permissão para executar o comando de administração da loja específico. Uma vez determinado que o usuário realmente tem permissão

para fazer isso (porque os administradores de loja têm permissão para executar comandos no grupo storeAdminCmds), uma política de controle de acesso no nível do recurso poderá ser chamada. Essa política pode afirmar que os administradores de loja têm permissão somente para executar tarefas administrativas de propriedade da organização na qual o usuário é um administrador de loja.

Para resumir, no controle de acesso no nível de comando, o comando é o próprio "recurso" e a "ação" deve simplesmente executar o comando (em outras palavras, instanciar o objeto de comando). O controle de acesso verifica se o usuário tem permissão para executar o comando. Por comparação, no controle de acesso no nível de recurso, o "recurso" é qualquer recurso protegido que o comando ou o bean acessam e a "ação" é o próprio comando.

Interações do Controle de Acesso

Esta seção apresenta o diagrama de interação que mostra como o controle de acesso funciona na estrutura de políticas de controle de acesso do WebSphere Commerce.

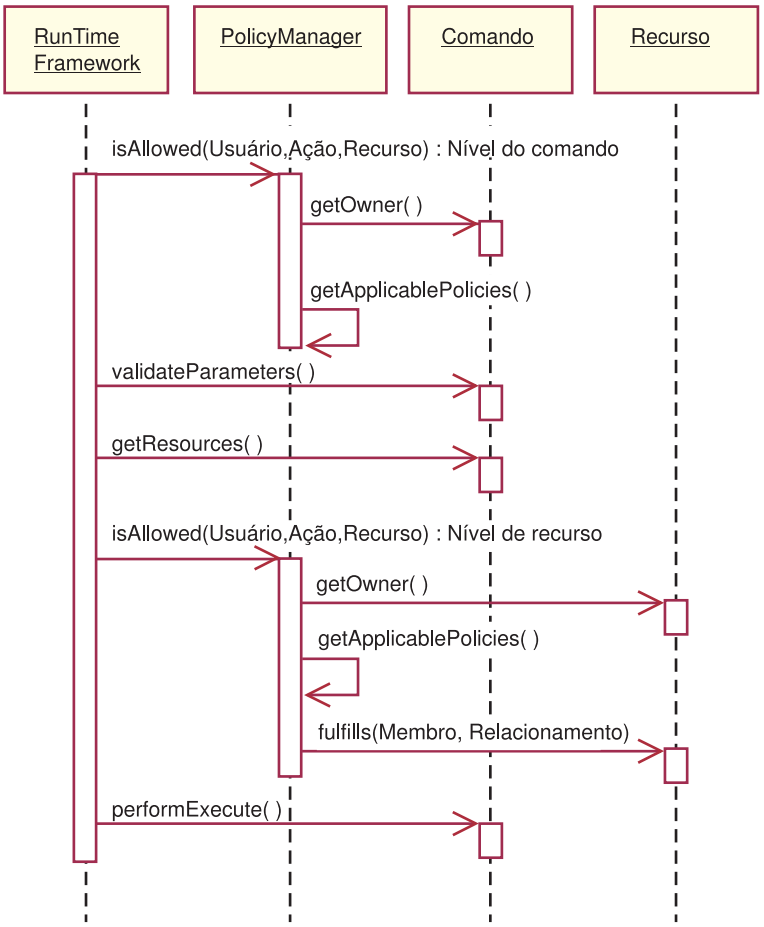


Figura 7.

O diagrama acima mostra ações executadas pelo *gerenciador de política* de controle de acesso. O gerenciador de política de controle de acesso é o componente de controle de acesso que determina se o usuário atual tem permissão ou não para executar a ação especificada no recurso especificado. Ele determina isso

pesquisando as políticas pertencentes ao proprietário do recurso e suas organizações ascendentes. Se pelo menos uma política conceder acesso, então a permissão será concedida.

A lista a seguir descreve as ações do diagrama de interação acima. Elas estão organizadas de cima para baixo no diagrama.

1. `isAllowed()`
   Os componentes de tempo de execução determinam se o usuário tem acesso no nível de comando para o comando de controlador ou de exibição.
2. `getOwner()`
   O gerenciador de política de controle de acesso determina o proprietário do recurso no nível de comando. A implementação padrão retorna o identificador de membro (`memberId`) do proprietário da loja (`storeId`) que está no contexto do comando. Se não houver nenhum identificador de loja no contexto do comando, então a organização raiz (`-2001`) será retornada.
3. `getApplicablePolicies()`
   O gerenciador de política de controle de acesso localiza e processa as políticas aplicáveis, com base no usuário, ação e recurso especificados.
4. `validateParameters()`
   Verificação e resolução inicial de parâmetros.
5. `getResources()`
   Retorna um vetor de acesso que é um vetor de pares recurso-ação.

   Se nada for retornado, a verificação de controle de acesso no nível de recurso não será executada. Se houver recursos que devem ser protegidos, um vetor de acesso (que consista em pares recurso-ação) deverá ser retornado.

   Cada *recurso* é uma instância de um objeto que pode ser protegido (um objeto que implementa a interface `com.ibm.commerce.security.Protectable`. Em muitos casos, o recurso é um bean de acesso.

   Um bean de acesso pode não implementar a interface `com.ibm.commerce.security.Protectable`, no entanto, a verificação do controle de acesso ainda pode ocorrer desde que o bean corporativo correspondente esteja protegido, de acordo com as informações incluídas em "Implementando Controle de Acesso em Beans Corporativos" na página 103.

   A *ação* é uma cadeia que representa a operação a ser executada no recurso. Na maioria dos casos, a ação é o no nome da interface do comando.
6. `isAllowed()`
   Os componentes do tempo de execução determinam se o usuário tem acesso no nível do recurso para todos os pares recurso-ação especificados por `getResources()`.
7. `getOwner()`
   O recurso retorna `memberId` de seu proprietário. Isso determina quais políticas se aplicam. Somente as políticas que pertencem ao proprietário do recurso e suas organizações ascendentes se aplicam.
8. `getApplicablePolicies()`
   O gerenciador de política de controle de acesso pesquisa políticas aplicáveis e, em seguida, as aplica. Se pelo menos uma política por par recurso-ação que concede permissão ao usuário para acessar o recurso for encontrada, então o acesso será concedido; caso contrário, o acesso será negado.
9. `fulfills()`
   Se uma política aplicável tiver um grupo de relacionamentos especificado, será feita uma verificação no recurso para verificar se o membro satisfaz o(s) relacionamento(s) especificado(s) em relação ao recurso.

10. `performExecute()`
    A lógica de negócios do comando.

Interface Protectable

Um fator chave para que um recurso seja protegido pelas políticas de controle de acesso do WebSphere Commerce é que o recurso deve implementar a interface `com.ibm.commerce.security.Protectable`. Essa interface é mais comumente utilizada com beans corporativos e beans de dados, mas somente os beans específicos que requerem proteção precisam implementar a interface.

Com a interface Protectable, um recurso deve fornecer dois métodos chave: `getOwner()` e `fulfills(Long member, String relationship)`.

As políticas de controle de acesso pertencem a organizações ou entidades organizacionais. O método `getOwner` retorna o memberId do proprietário do recurso protegível. Após o gerenciador de políticas de controle de acesso determinar o proprietário do recurso, ele também obtém o memberId de cada um dos ascendentes do proprietário na hierarquia de membros. Todas as políticas de controle de acesso que pertencem ao proprietário do pedido getOwner original, assim como todas as políticas de controle de acesso que pertencem a qualquer ascendente do proprietário serão então aplicadas.

As políticas de controle de acesso que se aplicam ao proprietário especificado, assim como as políticas de controle de acesso que se aplicam a qualquer ascendente de nível superior do proprietário na hierarquia de membros são aplicadas.

O método `fulfills` somente retornará true se o membro fornecido satisfizer o relacionamento obrigatório em relação ao recurso. Geralmente, o membro é um usuário simples, no entanto, ele também pode ser uma organização. Ele será uma organização se você estiver utilizando um grupo de relacionamentos na política de controle de acesso.

Interface Groupable

O aplicativo de uma política de controle de acesso é específico de um grupo de recursos. Agrupamentos de recursos podem ser feitos com base em atributos como o nome da classe, o estado de um pedido ou o valor do storeId.

Se um recurso for agrupado por um atributo diferente de seu nome de classe com a finalidade de aplicar políticas de controle de acesso, o recurso precisa implementar a interface `com.ibm.commerce.grouping.Groupable`.

O fragmento de código a seguir representa a interface Groupable:

```
Groupable interface {
 Object getGroupingAttributeValue (String attributeName, GroupContext context)
}
```

Por exemplo, para implementar uma política que aplica-se somente a pedidos que encontram-se no estado pendente (`status = P (pendente)`), a interface remota do bean de entidade Order implementará a interface Groupable e o valor de attributeName será definido para `"status"`.

A utilização da interface Groupable é rara.

Procurando Mais Informações sobre Controle de Acesso

Para obter mais informações sobre o modelo de controle de acesso do WebSphere Commerce, consulte o *WebSphere Commerce - Manual de Controle de Acesso*. Esse manual fornece uma visão geral detalhada do controle de acesso e descreve como utilizar o Administration Console para criar ou modificar políticas, grupos de ação e grupos de recursos.

Implementando o Controle de Acesso

Esta seção descreve como implementar o controle de acesso em código personalizado.

Identificando Recursos que Podem ser Protegidos

Em geral, beans corporativos e beans de dados são recursos que você pode querer proteger. No entanto, nem todos os beans corporativos e beans de dados devem ser protegidos. No aplicativo WebSphere Commerce existente, os recursos que requerem proteção já implementam a interface que pode ser protegida. A dúvida do que proteger aparece quando você cria novos beans corporativos e beans de dados. Decidir quais recursos proteger vai depender de seu aplicativo.

Se um comando retorna um bean corporativo no método `getResources`, então o bean corporativo precisa ser protegido, porque o gerenciador de políticas de controle de acesso chamará o método getOwner do bean corporativo. O método `fulfills` também será chamado se um relacionamento for especificado na política de controle de acesso no nível de recurso correspondente.

Se você implementasse a interface protegível (e, portanto, colocasse o recurso sob proteção) para todos os seus próprios beans corporativos e beans de dados, seu aplicativo poderia requerer muitas políticas. À medida em que o número de políticas aumenta, o desempenho pode cair e o gerenciamento de políticas torna-se mais desafiador.

Uma distinção teórica é feita entre os recursos principais e o recurso dependente. Um *recurso principal* pode existir por si só. Um *recurso dependente* existe somente quando existe o recurso principal relacionado a ele. Por exemplo, no código de aplicativo fornecido com o WebSphere Commerce, o bean corporativo Order é um recurso que pode ser protegido, mas o bean de entidade OrderItem não é. A razão para isso é que a existência de um OrderItem depende de um Order -- o Order é o recurso principal e o OrderItem é um recurso dependente. Se um usuário tiver acesso a um Order, ele também deve ter acesso aos itens do pedido.

De forma similar, o bean de entidade User é um recurso protegível, mas o bean de entidade Address não é. Nesse caso, a existência do endereço depende do usuário, portanto, qualquer coisa que tenha acesso ao usuário, também deve ter acesso ao endereço.

Recursos principais devem ser protegidos, mas recursos dependentes freqüentemente não requerem proteção. Se um usuário tiver permissão para acessar um recurso principal, faz sentido que, por padrão, o usuário deva ter permissão também para acessar seus recursos dependentes.

Implementando Controle de Acesso em Beans Corporativos

Se você criar novos beans corporativos que requerem proteção por políticas de controle de acesso, será necessário fazer o seguinte:

1. Criar um novo bean corporativo, assegurando que ele estenda de com.ibm.commerce.base.objects.ECEntityBean.
2. Certifique-se de que a interface remota do bean estenda a interface com.ibm.commerce.security.Protectable.
3. Se os recursos com os quais o bean interage estiverem agrupados por um atributo diferente do nome da classe Java do recurso, a interface remota do bean também deverá estender a interface com.ibm.commerce.grouping.Groupable.
4. A classe de bean corporativo contém implementações padrão para os seguintes métodos:
   - getOwner
   - fulfills
   - getGroupingAttributeValue

   Substitua os métodos que precisar. No mínimo, você deverá substituir o método getOwner.
   As implementações padrão desses métodos são exibidas nos fragmentos de código a seguir:

```
*****************************************************************************
public Long getOwner() throws Exception, java.rmi.RemoteException
{
   return null;
}
*****************************************************************************
*****************************************************************************
public boolean fulfills(Long member, String relationship)
  throws Exception, java.rmi.RemoteException
{
      return false;
}
*****************************************************************************
*****************************************************************************
public Object getGroupingAttributeValue(String attributeName,
   GroupingContext context) throws Exception, java.rmi.RemoteException
{
      return null;
}
*****************************************************************************
```

   A seguir estão exemplos de implementações desses métodos, com base no bean OrderBean:

```
*****************************************************************************
public Long getOwner() throws Exception, java.rmi.RemoteException
{
   com.ibm.commerce.common.objects.StoreEntityAccessBean storeEntAB = new
   com.ibm.commerce.common.objects.StoreEntityAccessBean();
   storeEntAB.setInitKey_storeEntityId(getStoreEntityId().toString());
   return storeEntAB.getMemberIdInEJBType();
}
*****************************************************************************
*****************************************************************************
public boolean fulfills(Long member, String relationship)
  throws Exception, java.rmi.RemoteException
   {
      if (relationship.equalsIgnoreCase("creator"))
      {
         return member.equals(getMemberId());
      }
      else if (relationship.equalsIgnoreCase (
         com.ibm.commerce.base.helpers.EJBConstants.
```

```
         SAME_ORGANIZATIONAL_ENTITY_AS_CREATOR_RELATION)) {
            com.ibm.commerce.user.objects.UserAccessBean creator = new
               com.ibm.commerce.user.objects.UserAccessBean();
            creator.setInitKey_MemberId(getMemberId().toString());
            com.ibm.commerce.user.objects.UserAccessBean ab = new
               com.ibm.commerce.user.objects.UserAccessBean();
            ab.setInitKey_MemberId(member.toString());
            if (ab.getParentMemberId().equals
            (creator.getParentMemberId()))
     return true;
          }
      return false;
}
*****************************************************************************
*****************************************************************************
public Object getGroupingAttributeValue(String attributeName,
   GroupingContext context) throws Exception
   {
      if (attributeName.equalsIgnoreCase("Status"))
         return getStatus();
   return null;
   }
*****************************************************************************
```

5. Criar (or recriar) o bean de acesso e o código gerado do bean corporativo.

Implementando Controle de Acesso em Beans de Dados

Se um bean de dados tiver de ser protegido, ele pode ser protegido direta ou indiretamente por políticas de controle de acesso. Se um bean de dados for protegido diretamente, então, existe uma política de controle de acesso que aplica-se a esse bean de dados específico. Se um bean de dados for protegido indiretamente, ele delega proteção para outro bean de dados, para o qual existe uma política de controle de acesso.

Se você criar um novo bean de dados que deve ser protegido diretamente por uma política de controle de acesso, o bean de dados deve fazer o seguinte:

1. Implementar a interface `com.ibm.commerce.security.Protectable`. Dessa forma, o bean precisa fornecer uma implementação dos métodos `getOwner()` e `fulfills(Long member, String relationship)`. Eles devem ser implementados na interface remota do bean.

   Quando um bean de dados implementa a interface Protectable, o gerenciador de bean de dados chama o método `isAllowed` para determinar se o usuário tem os privilégios de controle de acesso apropriados, de acordo com a política de controle de acesso atual. O método `isAllowed` é descrito pelo seguinte fragmento de código:

   ```
   IsAllowed(Context, "Display", protectable_databean);
   ```

2. Se os recursos com os quais o bean interage estiverem agrupados por um atributo diferente do nome da classe Java do recurso, o bean deverá implementar a interface `com.ibm.commerce.grouping.Groupable`.
3. Implementar a interface `com.ibm.commerce.security.Delegator`. Essa interface é descrita pelo seguinte fragmento de código:

   ```
   Interface Delegator {
    Protectable getDelegate();
   }
   ```

   Nota: Para estar diretamente protegido, o método `getDelegate` deve retornar o próprio bean de dados (ou seja, o bean de dados delega si mesmo para a finalidade de controle de acesso).

A distinção entre quais beans de dados devem ser protegidos diretamente versus quais devem ser protegidos indiretamente é similar à distinção entre os recursos principal e dependente. Se o objeto bean de dados pode existir por si só, ele deve ser protegido diretamente. Se a existência do bean de dados depender da existência de outro bean de dados, então, deve delegar ao outro bean de dados a proteção.

Um exemplo de bean de dados que deve ser protegido diretamente é o bean de dados Order. Um exemplo de um bean de dados que deve ser protegido indiretamente é o bean de dados OrderItem.

Se você criar um novo bean de dados que não é protegido indiretamente por uma política de controle de acesso, o bean de dados deve fazer o seguinte:

1. Implementar a interface `com.ibm.commerce.security.Delegator`. Essa interface é descrita pelo seguinte fragmento de código:

   ```
   Interface Delegator {
    Protectable getDelegate();
   }
   ```

   Nota: O bean de dados retornado por `getDelegate` deve implementar a interface Protectable.

Se um bean de dados não implementar a interface Delegator, ele será preenchido sem a proteção das políticas de controle de acesso.

Implementando Controle de Acesso em Comandos do Controlador

Ao criar um novo comando do controlador, a classe de implementação para o novo comando deve estender a classe `com.ibm.commerce.commands.ControllerCommandImpl` e sua interface deve estender a interface`com.ibm.commerce.command.ControllerCommand`.

Para políticas de nível de comando para os comandos do controlador, o nome da interface do comando é especificado como um recurso. Para que um recurso seja protegido, ele devem implementar a interface Protegida. De acordo com o modelo de programação do WebSphere Commerce, isso pode ser realizado fazendo com que a interface do comando se estenda a partir da interface `com.ibm.commerce.command.ControllerCommand`, e a implementação do comando se estenda a partir de `com.ibm.commerce.commands.ControllerCommandImpl`. A interface `ControllerCommand` estende a interface`com.ibm.commerce.command.AccCommand`, a qual por sua vez estende a `Protectable`. A interface `AccCommand` é a interface mínima que um comando deve implementar para ser protegido pelo controle de acesso de nível de comando.

Se o comando acessar recursos que devem ser protegidos, crie uma variável de instância particular do tipo `AccessVector` para receber os recursos. Em seguida, substitua o método `getResources`, uma vez que a implementação padrão desse método é retornar um valor nulo e, portanto, não ocorrerá nenhuma verificação de recurso.

No novo método `getResources`, você deve retornar uma matriz de recursos ou de pares recurso-ação sobre a qual o comando pode agir. Quando uma ação não é especificada explicitamente, ela é padronizada com o nome da interface do comando que está sendo executado.

Além disso, recomenda-se que o método determine se ele deve instanciar o recurso ou se ele pode utilizar a variável de instância existente que contém a referência para o recurso. Verificar se o objeto de recurso já existir pode ajudar a melhorar o desempenho do sistema. Em seguida, você pode utilizar o mesmo método `getResources`, se necessário, no método `performExecute` do novo comando do controlador.

A seguir há um exemplo do método `getResources`:

```
private AccessVector resources = null;

public AccessVector getResources() throws ECException {

   if (resources == null) {
      OrderAccessBean orderAB = new OrderAccessBean();
      orderAB.setInitKey_orderId(getOrderId().toString());
      resouces = new AccessVector(orderAB);
      }
   return resources;
}
```

Como um exemplo, considere o comando OrderItemUpdate. O método `getResources` desse comando retorna os objetos de proteção Order e User. Como a ação não é especificada, o padrão é a interface do comando OrderItemUpdate.

Vários recursos podem ser retornados pelo método `getResources`. Quando isso ocorre, uma política que fornece acesso ao usuário para todos os recursos especificados precisa ser encontrada se a ação dever ser executada. Se um usuário tiver acesso a dois de três recursos, a ação pode não prosseguir (três de três seria necessário).

Se você precisar executar verificação adicional de parâmetros ou resolver parâmetros no comando de controlador, pode utilizar o método `validateParameters()`. Isso é opcional.

Verificação Adicional no Nível do Recurso

Nem sempre é possível determinar todos os recursos que precisam ser protegidos, no momento em que o método `getResources` do comando de controlador é chamado.

Se necessário, um comando de tarefa também pode implementar um método `getResources` para retornar uma lista de recursos, na qual o comando pode agir.

Outra maneira de a verificação no nível do recurso é fazer chamadas diretas ao gerenciador de políticas de controle de acesso, utilizando o método `checkIsAllowed(Object resource, String action)`. Esse método está disponível para qualquer classe que estenda da classe `com.ibm.commerce.command.AbstractECTargetableCommand`. Por exemplo, as classes a seguir estendem da classe `AbstractECTargetableCommand`:

- `com.ibm.commerce.command.ControllerCommandImpl`
- `com.ibm.commerce.command.DataBeanCommandImpl`

O método `checkIsAllowed` também está disponível para as classes que estendem a classe `com.ibm.commerce.command.AbstractECCommand`. Por exemplo, a seguinte classe se estende da classe `AbstractECCommand`:

- `com.ibm.commerce.command.TaskCommandImpl`

A seguir há a assinatura do método `checkIsAllowed`:

```
void checkIsAllowed(Object resource, String action)
   throws ECException
```

Este método envia um ECApplicationException se o usuário atual não estiver permitido a desempenhar a ação especificada no recurso especificado. Se o acesso for concedido, então o método simplesmente retorna.

Controle de Acesso para Comandos “create”

Como o método `getResources` é chamado antes do método `performExecute` em um comando, é necessária uma abordagem diferente para controle de acesso de recursos que ainda não foram criados. Por exemplo, se você tiver um `WidgetAddCmd`, o método `getResources` não poderá retornar o recurso que está prestes a ser criado. Nesse caso, o método `getResources` deve retornar o criador dos recursos. Por exemplo, um comando é criado por uma fábrica de comandos, um pedido é criado em uma loja e um usuário é criado em uma organização.

Implementações Padrão para Controle de Acesso no Nível de Comando

Para controle de acesso no nível de comando, a implementação padrão do método getOwner() retorna o memberId do proprietário da loja, se o storeId for especificado. Se o storeId não for especificado, o memberId da organização raiz será retornado (`memberId = -2001`).

A implementação padrão do método `getResources()` retorna `null`.

A implementação padrão de `validateParameters()` não faz nada.

Implementando Políticas de Controle de Acesso em Exibições

O controle de acesso no nível de recurso para exibições é executado pelo gerenciador de bean de dados. O gerenciador de bean de dados é chamado nos seguintes casos:

1. Quando o modelo JSP inclui a tag `<useBean>` e o bean de dados não está na lista de atributos.
2. Quando o modelo JSP inclui o seguinte método ativo:
   ```
   DataBeanManager.activate(xyzDatabean, request);
   ```

Nota: Qualquer bean de dados que deve ser protegido (direta ou indiretamente) deve implementar a interface Delegator. Qualquer bean de dados que deve ser protegido diretamente delegará a si próprio e, portanto, também implementará a interface Protectable. Os beans de dados que são protegidos indiretamente, devem delegar a um bean de dados que implementa a interface Protectable.

Apesar de não ser recomendável, um desvio das verificações de controle de acesso ocorre nos seguintes casos:

1. Se o modelo JSP fizer chamadas diretas a beans de acesso, em vez de utilizar beans de dados.
2. Se o modelo JSP chamar diretamente o método populate() do bean de dados.

Se os resultados de um comando de controlador precisarem ser encaminhados para uma exibição (utilizando o ForwardViewCommand), o controle de acesso no nível de comando não será executado nas exibições. Além disso, se o comando de controlador colocar os beans de dados preenchidos (utilizados na exibição) na lista de atributos da propriedade de resposta e avançar para uma exibição, o modelo JSP poderá acessar os dados sem passar pelo gerenciador de bean de dados. Isso

requer que as tags <useBean> sejam utilizadas no modelo JSP. Essa pode ser uma maneira de tornar um modelo JSP mais eficiente, uma vez que ele pode ignorar qualquer verificação de controle de acesso no nível de recurso redundante em recursos (beans de dados) para os quais o usuário já obteve acesso por meio do comando de controlador.

Parte 5. Apêndices

Avisos

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

É possível que a IBM não ofereça os produtos, serviços ou recursos discutidos nesta publicação em outros países. Consulte um representante IBM local para obter informações sobre produtos e serviços disponíveis atualmente em sua área. Qualquer referência a produtos, programas ou serviços IBM não significa que apenas os produtos, programas ou serviços IBM possam ser utilizados. Qualquer produto, programa ou serviço funcionalmente equivalente, que não infrinja nenhum direito de propriedade intelectual da IBM ou outros direitos legalmente protegidos, poderá ser utilizado em substituição a este produto, programa ou serviço. Entretanto, a avaliação e verificação da operação de qualquer produto, programa ou serviço não-IBM são de responsabilidade do Cliente.

Qualquer referência nesta publicação a um programa licenciado da IBM não significa que apenas o programa licenciado IBM possa ser utilizado. Qualquer produto, programa ou serviço funcionalmente equivalente, que não infrinja nenhum direito de propriedade intelectual da IBM ou outros direitos legalmente protegidos, poderá ser utilizado em substituição a este produto, programa ou serviço. A avaliação e verificação da operação em conjunto com outros produtos, exceto aqueles expressamente designados pela IBM, são de inteira responsabilidade do Cliente.

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

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

Para pedidos de licença relacionados a informações de byte-duplo (DBCS), entre em contato com o Departamento de Propriedade Intelectual da IBM em seu país ou envie pedidos de licença, por escrito, para:

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

O parágrafo a seguir não se aplica a nenhum 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 NÃO SE LIMITANDO ÀS GARANTIAS IMPLÍCITAS DE NÃO-VIOLAÇÃO, MERCADO 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.

Esta publicação pode 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 sites não-IBM na Web são fornecidas apenas por conveniência e não representam de forma alguma um endosso a esses sites na Web. Os materiais contidos nestes sites da Web não fazem parte dos materiais deste produto IBM e a utilização desses sites da Web é de inteira responsabilidade do Cliente.

A IBM pode utilizar ou distribuir as 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 o 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:

Gerência de Relações Comerciais e Industriais da IBM Brasil
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 uma taxa.

O programa licenciado descrito neste documento e todo o material licenciado disponível são fornecidos pela IBM sob os termos do Contrato com o Cliente IBM, do Contrato de Licença do Programa Internacional IBM ou de qualquer outro contrato equivalente.

Todos 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 de nível de desenvolvimento e não há garantia de que estas medidas serão iguais em sistemas geralmente disponíveis. Além disso, algumas medidas podem ter sido estimadas por 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 junto aos fornecedores dos respectivos produtos, de seus anúncios publicados ou de outras fontes disponíveis publicamente. A IBM não testou estes produtos e não pode confirmar a precisão de seu desempenho, compatibilidade nem qualquer outra reivindicação relacionada a produtos não-IBM. Dúvidas sobre os recursos de produtos não-IBM devem ser encaminhadas diretamente a seus fornecedores.

Todas as declarações relacionadas aos objetivos e intenções futuras da IBM estão sujeitas a alterações ou cancelamento sem aviso prévio e representam apenas metas e objetivos.

Estas informações foram projetadas apenas com o propósito de planejamento. As informações aqui contidas estão sujeitas a alterações antes que os produtos descritos estejam disponíveis.

Estas informações contêm exemplos de dados e relatórios utilizados nas operações diárias de negócios. Para ilustrá-los da forma mais completa possível, os exemplos podem incluir nomes de indivíduos, empresas, marcas e produtos. Todos estes nomes são fictícios e qualquer semelhança aos nomes e endereços utilizados por uma empresa real é mera coincidência.

Imagens, marcas e nomes comerciais de cartão de crédito fornecidos neste produto devem ser utilizados apenas por comerciantes autorizados pelo proprietário do cartão de crédito para que o pagamento seja aceito através desse cartão.

Marcas

Os termos a seguir são marcas ou marcas registradas da International Business Machines Corporation nos Estados Unidos e/ou em outros países:

400	AIX	AS/400
DB2	IBM	iSeries
OS/2	SecureWay	WebSphere

Domino é uma marca registrada da Lotus Development Corporation e/ou da IBM Corporation nos Estados Unidos e/ou em outros países.

Netscape é uma marca registrada da Netscape Communications Corporation nos Estados Unidos e/ou em outros países.

Solaris, Solaris Operating Environment, Java, JavaBeans e todas as marcas e logotipos baseados em Java são marcas ou marcas registradas da Sun Microsystems, Inc.

VeriSign e o logotipo do VeriSign são marcas e marcas de serviço ou marcas registradas e marcas de serviço da VeriSign, Inc.

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

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

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