IBM® WebSphere Commerce®

Manual de Controle de Acesso

Versão 54

IBM® WebSphere Commerce®

Manual de Controle de Acesso

Versão 54

Nota:
Antes de utilizar estas informações e o produto suportado por elas, leia as informações na seção de Avisos.

Primeira Edição (Março de 2002), Segunda revisão (Abril de 2002)

Esta edição se aplica aos seguintes produtos:

IBM WebSphere Commerce Business Edition para Windows NT e Windows 2000, Versão 5.4

IBM WebSphere Commerce Business Edition para AIX, Versão 5.4

IBM WebSphere Commerce Business Edition para Software Solaris Operating Environment, Versão 5.4

IBM WebSphere Commerce Studio, Business Developer Edition para Windows NT e Windows 2000, Versão 5.4

IBM WebSphere Commerce Professional Edition para Windows NT e Windows 2000, Versão 5.4

IBM WebSphere Commerce Professional Edition para AIX, Versão 5.4

IBM WebSphere Commerce Professional Edition para Software Solaris Operating Environment, Versão 5.4

IBM WebSphere Commerce Studio, Professional Developer Edition para Windows NT e Windows 2000, Versão 5.4

e a todos os releases e modificações subseqüentes dos produtos listados acima, até que seja indicado o contrário em novas edições. Certifique-se de utilizar a edição correta para o nível do produto.

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

A IBM agradece os seus comentários. Os comentários podem ser enviados através de um dos seguintes métodos:

1. Eletronicamente para o ID de rede listado abaixo. Inclua seu endereço de rede completo para obter uma resposta.

   `Internet: torrcf@ca.ibm.com`

2. Por correio para o seguinte endereço:

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

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

Onde Encontrar Informações

O WebSphere Commerce™ possui informações online e cópia impressa que descrevem a solução completa de e-commerce. Além disso, os produtos de software que acompanham o WebSphere Commerce fornecem mais informações, descrevendo os recursos e as funções específicos do software. Esta seção fornece uma rápida visão geral de onde localizar os diversos tipos de informações.

Publicações do WebSphere Commerce

- *IBM™ WebSphere Commerce - Fundamentos, Versão 5.4*
- *IBM™ WebSphere Commerce Programmer's Guide, Versão 5.4*
- *IBM™ WebSphere Commerce para Windows NT™ e Windows™ 2000, Quick Beginnings, Versão 5.4*
- *IBM™ WebSphere Commerce Studio Business Developer Edition para Windows NT™ e Windows™ 2000 Installation Guide, Versão 5.4*
- *IBM™ WebSphere Commerce Migration Guide, Versão 5.4*

Para obter atualizações sobre essas publicações, consulte o seguinte endereço da Web: `http://www.ibm.com/software/webservers/commerce/wc_be/lit-tech-general.html`

Ajuda Online do WebSphere Commerce

A ajuda online do WebSphere Commerce é composta por informações online que podem ser exibidas utilizando um navegador da Web. Trechos de informações online também foram compilados em documentos de áreas de assuntos relacionados no formato PDF (Portable Document Format).

A ajuda online pode ser acessada a partir de um navegador da Web que é executado com Internet Explorer, Versão 5.5 ou posterior utilizando o seguinte endereço:

`http://`*`host_name`*`/wchelp/`, em que *`host_name`* é o nome de sua máquina do WebSphere Commerce.

Além disso, no Windows, a ajuda pode ser acessada do menu **Iniciar** como segue:

Iniciar – >Programas – >IBM® WebSphere Commerce– > Documentação

Informações Adicionais na Web

Suporte

Para localizar as informações de suporte, incluindo grupos de notícias, FAQs, notas técnicas, informações sobre resolução de problemas e downloads, visite o seguinte endereço da Web:

Business

`http://www.ibm.com/software/webservers/commerce/wc_be/support.html`

Professional

http://www.ibm.com/software/webservers/commerce/wc_pe/support.html

Parceiros de software

Há vários parceiros de software que oferecem produtos e serviços para melhorar o WebSphere Commerce. Para obter informações sobre esses parceiros, visite o seguinte endereço da Web:
http://www.ibm.com/software/webservers/commerce/community e clique no link Software Developers.

Redbooks™

Para localizar informações técnicas mais avançadas, visite o site Redbooks na Web, situado em http://www.ibm.com/redbooks e pesquise por WebSphere Commerce.

Antes de Iniciar

O Manual de Acesso de Controle do *IBM WebSphere Commerce, Versão 5.4* destina-se a administradores de site que desejam gerenciar o acesso ao site do WebSphere Commerce. Os adminstradores de loja podem executar gerenciamento de acesso limitado da entidade organizacional para qual executam sua função.

Este manual oferece uma introdução ao gerenciamento de acesso, incluindo uma visão geral de organizações e usuários, políticas de controle de acesso, sua hierarquia e seus relacionamentos e as políticas padrão que são empacotadas com o produto. Este manual também oferece uma ampla gama de cenários para ajudar os administradores de site que desejam fazer personalizações básicas em suas políticas existentes, bem como diretrizes para teste de políticas modificadas e fazer considerações do desempenho.

Este manual é dividido nas seguintes seções:

Capítulo 1: Visão Geral Uma visão geral breve dos recursos-chave do sistema de controle de acesso do WebSphere Commerce, bem como uma descrição do que foi alterado desde o release anterior do WebSphere Commerce.

Capítulo 2: Informações Iniciais Uma introdução ao gerenciamento de acesso, incluindo como definir organizações e usuários, como as organizações e os usuários estão relacionados às políticas de controle de acesso, a estrutura básica de uma política de controle de acesso e como ler e identificar as peças-chave de uma política no WebSphere Commerce Administration Console, e no XML.

Capítulo 3: Conceitos do controle de acesso Informações conceituais sobre a estrutura de uma organização e suas sub-organizações, como é concedido aos usuários acesso a um sistema, descrições de funções padrão e terminologia relacionada.

Capítulo 4: Personalizando suas políticas de controle de acesso Uma análise profunda das políticas em nível de recursos e baseadas em função, seu relacionamento e sua hierarquia

Capítulo 5: Cenários de controle de acesso Uma variedade de cenários para mostrar-lhe como fazer modificações básicas nas políticas de controle de acesso padrão enviadas com o WebSphere Commerce.

Capítulo 6: Utilizando os arquivos XML para personalizar as políticas de controle de acesso Uma análise da personalização das partes de uma política de controle de acesso utilizando o XML. Inclui procedimentos passo-a-passo de como carregar informações da política a partir dos arquivos XML nas tabelas de banco de dados do controle de acesso e como extrair as informações de política das tabelas de banco de dados do controle de acesso em arquivos XML.

Apêndice: Tabela das políticas de controle de acesso padrão Uma lista completa de todas as políticas de controle de acesso padrão carregadas em seu sistema no momento da instalação.

Suposições

Este manual presume que você instalou e configurou com êxito o IBM WebSphere Commerce, Versão 5.4 em seu site e que tem acesso de Administrador do Site para a ferramenta WebSphere Commerce Administration Console. Os Administradores de Loja são capazes de gerenciar as políticas de controle de acesso para sua entidade organizacional utilizando a ferramenta WebSphere Commerce Administration Console, mas não são capazes de gerenciar os componentes das políticas, como os grupos de ações e de recursos, uma vez que são entidades em todo o sistema.

Este manual também considera que seu sistema atende a todos os requisitos de software e hardware para executar o WebSphere Commerce. Para obter mais informações sobre a instalação do WebSphere Commerce, incluindo pré-requisitos, consulte o *IBM WebSphere Commerce, Versão 5.4 Installation Guide*.

Convenções Utilizadas neste Manual

Este manual utiliza as seguintes convenções:

Negrito indica controles da GUI (interface gráfica com o usuário), como nomes de campos, botões ou opções de menus.

`Monoespaçado` indica exemplos de texto que você digita exatamente como mostrado, bem como caminhos de diretórios.

Itálico é utilizado para ênfase e para variáveis que você substitui com seus próprios valores.

 indica informações adicionais que podem ajudar a concluir uma tarefa.

NT indica informações específicas do WebSphere Commerce para o Windows NT ®.

2000 indica informações específicas do WebSphere Commerce para o Windows ® 2000.

AIX indica informações específicas do WebSphere Commerce para o AIX ®.

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

Linux indica informações específicas do WebSphere Commerce para Linux.

400 indica informações específicas do WebSphere Commerce para o IBM Eserver iSeries™ 400 ® (formalmente chamado AS/400 ®)

Professional indica informações específicas do WebSphere Commerce Professional Edition.

Business indica informações específicas do WebSphere Commerce Business Edition.

Índice

Onde Encontrar Informações iii
Publicações do WebSphere Commerce iii
Ajuda Online do WebSphere Commerce iii
Informações Adicionais na Web iii
Antes de Iniciar iv
Suposições v
Convenções Utilizadas neste Manual v

Capítulo 1. Uma Introdução ao Controle de Acesso 1
Novidades no WebSphere Commerce Versão 5.4? . . 1
Interface do Usuário Aprimorada 1
Controle Refinado 2
Componente Administrado Separadamente . . . 2
Adaptável a Novos Processos de Negócios . . . 2
Dimensionamento 2
O Que Significa Controle de Acesso para Você . . . 3

Capítulo 2. Introdução. 5
Definindo as Organizações e os Usuários 5
Definindo uma Organização de Vendedores . . . 6
Definindo uma Organização de Compradores . . 6
Compreendendo o Controle de Acesso. 7
O Que É uma Política de Controle de Acesso? . . 7
Como Funciona uma Política de Controle de Acesso? 7
Como Inicio a Utilização do Controle de Acesso? . . 8

Capítulo 3. Conceitos de Controle de Acesso 9
Hierarquia Organizacional 9
Organização Raiz 10
Organizações (Vendedor) 11
Organizações (Comprador) 11
Funções 12
Operações do Site 12
Desenvolvimento do Site e Conteúdo 13
Logística e Operações 13
Gerenciamento de Produtos 14
Gerenciamento de Vendas 14
Gerenciamento de Marketing 15
Gerenciamento Organizacional 15
Política de Controle de Acesso 16
Elementos de uma Política de Controle de Acesso 16
Conceitos da Política de Controle de Acesso . . 16
Propriedade de Política e de Recurso 22
Tipos de Políticas de Controle de Acesso . . . 22
Níveis de Controle de Acesso 24
Como o Controle de Acesso Impede Ações não Autorizadas 26
Verificando a Autorização antes de Executar uma Ação Iniciada pelo Usuário 26
Avaliando as Políticas de Controle de Acesso . . . 26
Hierarquia Organizacional 27
Usuários 27
Funções 27
Grupos de Acesso 27
Documentos 27
Avaliando Políticas Normais 28
Avaliando Políticas Modelos 30
Analisando uma Política em Detalhes 32
Exemplo 1: Lendo uma Política 33
Exemplo 2: Lendo uma Política em XML . . . 35
Exemplo 3: Identificando outras Políticas Associadas a sua Política 36

Capítulo 4. Personalizando as Políticas de Controle de Acesso Padrão 39
Identificando as Políticas Afetadas por uma Alteração 39
Compreendendo o Relacionamento entre as Políticas Baseadas em Funções e em Nível de Recurso. 39
Determinando se uma Política é Baseada em Funções ou em Nível do Recurso 43
Políticas Baseadas em Funções 43
Políticas em Nível do Recurso 44
Dicas para Alterar Políticas Padrão 45
Depois de Fazer as Alterações na Política 45
Testando as Alterações da Política 46
Extraindo as Alterações das Políticas em Arquivos XML 46

Capítulo 5. Cenários de Personalização 47
Cenário 1 de Leilões: Removendo a Capacidade dos Administradores de Leilões para Fechar o Lance do Leilão 48
Etapas a Serem Executadas 48
Cenário 2 de Leilões: Removendo a Capacidade dos Administradores de Leilão em Retirar Lances . . . 49
Etapas a Serem Executadas 49
Cenário 3 de Leilões: Remover a Capacidade dos Administradores de Leilão em Retirar Lances em uma Organização. 50
Etapas a Serem Executadas 50
Cenário 4 de Leilões: Limitando o Lance do Leilão aos Compradores 51
Etapas a Serem Executadas 51
Cenário 1 de Contratos: Remover a Capacidade dos Administradores de Contratos em Incluir ou Excluir Conexões para Contratos 52
Etapas a Serem Executadas 53
Cenário 2 de Contratos: Permitir que Operadores e Administradores de Contratos Implementem Contratos 53
Etapas a Serem Executadas 54
Cenário 1 de Pedidos: Permitindo que Apenas Compradores Criem Pedidos 55
Etapas a Serem Executadas 55

Cenário 2 de Pedidos: Permitindo que Apenas os Administradores de Comprador Modifiquem os Pedidos. 57
Etapas a Serem Executadas 57
Cenário 3 de Pedidos: Permitindo que Aprovadores RMA Aprovem todas RMAs 59
Etapas a Serem Executadas 60
Cenário 1 de Associação: Remover a Capacidade dos Usuários de Auto-Registrarem. 61
Etapas a Serem Executadas 61
Cenário 2 de Associação: Permitindo que Apenas Usuários Registrados e Aprovados Alterem suas Informações de Endereço 62
Etapas a Serem Executadas 62
Cenário 3 de Associação: Permitindo que os Registradores de Membros Registrem Usuários . . 63
Etapas a Serem Executadas 63
Cenário 1 de Cupons: Permitindo que Apenas Compradores Resgatem Cupons 65
Etapas a Serem Executadas 66
Cenário 2 de Cupons: Permitindo que Administradores de Cupons e Administradores de Loja Criem Promoções com Cupom Eletrônico. . . 67
Etapas a Serem Executadas 68
Cenário 1 de Procurement: Permitindo que os Gerentes de Carrinho de Compras Gerenciem o Carrinho de Compras do Procurement para Pedidos Criados por sua Organização 69
Etapas a Serem Executadas 70
Cenário 2 de Procurement: Permitir Administradores de Compradores de Procurement a Submeter o Carrinho de Compras de Procurement para Pedidos Criados por sua Organização 70
Etapas a Serem Executadas 71
Cenário 1 de Estoque: Permitir que os Gerentes do Centro de Distribuição Atualizem os Centros de Distribuição, Mas Não os Exclua 72
Etapas a Serem Executadas 72
Cenário 2 de Estoque: Permitir Apenas que os Gerentes de Logística e de Operações Criem, Atualizem ou Excluam Centros de Distribuição . . 73
Etapas a Serem Executadas 73
Cenário 1 Inteligência de Negócios: Permitindo que Auditores Exibam os Relatórios de Inteligência de Negócios 74
Etapas a Serem Executadas 74

Capítulo 6. Utilizando XML para Personalizar as Políticas de Controle de Acesso 77
Alterações que Apenas Podem ser Feitas Editando e Carregando Arquivos XML 77
Sobre os Arquivos XML para Controle de Acesso . . 77
Personalizando os Arquivos XML 79
Protegendo as Exibições 79
Protegendo os Comandos do Controlador . . . 81
Implementando o Controle de Acesso do Nível do Recurso 83
Protegendo os Beans de Dados 85
Agrupando Recursos por Atributos 87
Definindo Relacionamentos 89
Definindo Grupos de Relacionamentos 89
Grupos de Acesso 92
Políticas 95
Depois de Alterar os Arquivos XML. 102
Testando suas Alterações 102
Carregando suas Alterações no Banco de Dados 102
Carregando suas Alterações de XML no Banco de Dados. 102
Extraindo Definições da Política e do Grupo de Acesso do Banco de Dados em seus Arquivos XML 104

Apêndice. Políticas de Controle de Acesso Padrão. 107
Políticas Baseadas em Funções 108
Políticas em Nível do Recurso por Área de Negócios 109
Pedidos 109
Comércio (Contratos) 110
Aprovações 111
Leilões. 111
Inteligência de Negócios 111
Associação 112
Administration Console de Comprador 112
Campanhas 112
Catálogo 113
Conectividade e Notificação 113
Procurement. 114
Cupons 114
Perfil de Cliente 114
Descontos 114
Gerenciamento de Estoque 115
Estoque Programado 115
Gerenciamento de Estoque 115
Gerenciamento de Pedidos 116
Pagamento 117
Páginas do Administration Console para Editar Políticas, Grupos de Acesso, Grupos de Recursos e Grupos de Ação. 117
Consultor de Produto. 117
RFQ 117
Regras. 118
Programador 118

Avisos 119
Licença de Copyright. 120
Marcas 121

Capítulo 1. Uma Introdução ao Controle de Acesso

A função do e-commerce não apenas alterou a forma como as empresas estão fazendo negócios, como aumentou muito os tipos de relacionamentos que elas podem esperar ter com seus clientes e parceiros de negócio. A Web é um fator-chave na entrega de valor melhorado para seus clientes existentes e na abertura de caminho para novos clientes ávidos por beneficiar-se da força e da eficiência aprimorada da Internet. Junto com as vantagens de fazer negócios na Web e o potencial tremendo de aumentar sua base de clientes vem o desafio de gerenciar seus fluxos de negócios e de comerciar padrões enquanto mantém um ambiente altamente seguro, de autorizar transações adequadas e de dinamizar seus processos de trabalho.

A marca do controle de acesso é a capacidade de supervisionar esses processos de trabalho, gerenciando as formas nas quais os usuários participam no seu sistema, baseados em suas atividades e seu relacionamento de negócios para seus produtos e serviços. Por exemplo, você pode apenas querer que os clientes tenham registrado em seu site para poder exibir produtos para leilões em sua loja e para efetuar lances neles. Da mesma forma, você pode autorizar designers gráficos a personalizar as páginas de sua loja, mas pode restringi-los de gerenciar o conteúdo real no catálogo de produtos.

O WebSphere Commerce lhe oferece as ferramentas certas para gerenciamento de acesso, incluindo mais de 200 políticas de controle de acesso padrão que são automaticamente carregadas no sistema no momento da criação da instância. Essas políticas foram atribuídas para encaminhar diversos requisitos de controle de acesso comuns de que seus negócios precisam e podem até mesmo ser personalizados para adequar-se à sua própria solução de e-commerce.

Gerenciar acesso a atividades no seu mercado eletrônico é uma parte integrante da proteção de recursos e ativos financeiros da sua empresa, para garantir transações seguras de negócios entre membros aprovados de seu site e para validar a legalidade de suas operações online. O controle de acesso se torna especialmente crucial no contexto de e-commerce, no qual a entrada para seu negócio é amplamente afetada pelos relacionamentos com clientes que começam pela Web.

Novidades no WebSphere Commerce Versão 5.4?

Para obter uma lista de outros novos recursos e aprimoramentos incluídos no WebSphere Commerce, consulte o *IBMNovidades do WebSphere Commerce, Versão 5.4*.

Interface do Usuário Aprimorada

Além das páginas de edição de política acessíveis a partir do menu Gerenciamento de acesso do Administration Console, o WebSphere Commerce agora também oferece páginas do visualizador adicionais para exibir políticas e seus grupos de ação, grupos de acesso e grupos de recursos relacionados. As páginas de exibição de políticas estão completamente integradas à interface do usuário do Administration Console e podem ser acessadas utilizando os botões incluídos às páginas de edição de políticas existentes.

Controle Refinado

O release anterior do WebSphere Commerce Suite ofereceu controle de acesso "grosseiro", que o habilitou a definir quem poderia chamar quais funções no sistema. Por exemplo, no release anterior do WebSphere Commerce Suite, você utilizou o controle de acesso grosseiro que permite aos compradores cancelar pedidos chamando a função `cancelar pedido`.

Agora no WebSphere Commerce, também lhe é oferecida a capacidade de controle de acesso "refinado", definindo quem pode chamar quais funções em comparação com quais instâncias do objeto de negócio (também conhecido como `recursos`). No mesmo exemplo, você não apenas pode dar permissão aos compradores para cancelar pedidos, mas também limitar os usuários a chamar a função cancelar pedido apenas em seus próprios pedidos, não nos pedidos de outros usuários.

O poder agregado do controle de acesso refinado combinado com o controle de acesso grosseiro, permite a você um âmbito maior de gerenciamento de acesso e a capacidade de refinar as atividades que os usuários têm permissão para fazer em seu site.

Componente Administrado Separadamente

No release anterior do WebSphere Commerce Suite, o controle de acesso refinado foi construído no código do sistema, que exigiu alterações no código para instituir a personalização de políticas em nível de recurso.

Agora, o WebSphere Commerce externaliza o controle de acesso grosseiro e refinado, codificando as políticas de controle de acesso nos arquivos XML que podem ser modificados utilizando a interface do visualizador de política incluída nas ferramentas do Administration Console ou utilizando um editor de texto padrão.

Uma vez que as políticas de controle de acesso grosseira e refinada agora estão disponíveis separadas do código do produto, adaptar o gerenciamento de acesso para suas necessidades de negócios requer que se faça alterações nas informações contidas nos arquivos XML e não no código do produto.

Adaptável a Novos Processos de Negócios

No mercado em constante mutação de hoje, a capacidade de personalizar rapidamente seu ambiente de negócios desempenha um papel importante na competição restante, no ajuste às alterações do mercado e na adaptação a novos processos de negócios. Externalizando tanto as políticas grosseiras quanto refinadas, as alterações que você deseja fazer nos níveis de acesso em seu sistema podem ser feitas de maneira rápida e fácil, modificando as políticas e não personalizando o código. Mais importante, expondo as políticas refinadas que estavam previamente disponíveis apenas para uma equipe de serviços de comprometimento, sua organização agora pode fazer muitas das modificações básicas nas políticas e reduzir os custos agregados de personalização do WebSphere Commerce para seu site na Web.

Dimensionamento

À medida que sua organização é alterada e cresce com o passar do tempo, o acesso ao seu sistema deve abranger também essas alterações. À medida que novos funcionários são contratados, que suas funções e responsabilidades são alteradas, seus níveis de acesso devem mudar de acordo para permitir que executem as

atividades que lhes são exigidas. Além disso, a tarefa de acompanhamento das atividades de cada usuário individual pode levar tempo, ser difícil e, até mesmo, impraticável.

No entanto, com o WebSphere Commerce, a concessão de acesso ao sistema pode ser gerenciada implicitamente, utilizando os grupos de acesso cuja associação é definida por um conjunto compartilhado de *atributos*, ao invés de suas identidades. Aos usuários são atribuídas funções e é dado acesso de acordo com essas funções. Por exemplo, aos Usuários A, B e C pode ser atribuída uma função `Comprador`, e a todos os compradores pode ser dada a capacidade de cancelar pedidos que não foram enviados, utilizando a política apropriada de controle de acesso. Se o Usuário A deixar a organização, as informações da função do Usuário A poderão ser excluídas, contanto que a política de controle de acesso associando as funções do comprador com cancelamento de pedidos permaneça inalterada para os Usuários B e C.

A capacidade de conceder acesso aos usuários do seu sistema implicitamente é um método poderoso para gerenciar atividades e exige muito menos tempo e esforço. Além disso, o esforço exigido para gerenciar o controle de acesso se torna um fator do número de políticas que você deseja alterar, não o tamanho do seu sistema, do número de usuários pertencentes à sua organização ou do nível de atividades de negócios que você conduz. As políticas de controle de acesso que são executadas em seu sistema podem ser aplicadas a organizações pequenas e grandes. Como resultado, a escalabilidade das políticas de controle de acesso que são executadas no WebSphere Commerce permite que sua empresa continue a alterar e a crescer sem impedir a estrutura ou a eficiência de suas operações.

O Que Significa Controle de Acesso para Você

O controle de acesso permite que você gerencie seus fluxos de trabalho de negócios e garanta que os usuários apenas executem aquelas atividades apropriadas para suas funções e responsabilidades. O WebSphere Commerce não só lhe oferece as políticas padrão que estão prontas para uso "fora da caixa", como também as ferramentas e a capacidade de personalizar as políticas para adequar-se às suas necessidades de negócios.

A tabela a seguir destaca apenas alguns exemplos de como modificações simples podem personalizar o acesso ao seu ambiente de negócios.

O que os usuários têm permissão para fazer por padrão	**O que os usuários têm permissão para fazer depois da personalização**
Os clientes podem se auto-registrar.	Apenas os administradores de vendedores podem registrar novos clientes.
Os compradores podem exibir as RFQs que eles criaram.	Apenas os vendedores podem exibir as RFQs se a RFQ resultou em um contrato.
Apenas os clientes podem cancelar pedidos criados por eles se o pedido estiver no estado pendente.	Os Representantes de Atendimento ao Cliente também podem cancelar pedidos no estado pendente, se o preço total do produto for menor que R$1.000.
Um pedido pode ser modificado pela pessoa que o criou.	Apenas um usuário da organização de compradores com a função de `comprador` pode modificar um pedido que foi criado.
Representantes de contas podem exibir todas as contas.	Representantes de Contas podem exibir apenas contas ativas.

Os funcionários com a função de Gerente de Logística podem criar e modificar centros de distribuição.	Os funcionários com a função de Gerente de Logística podem criar, mas não modificar os centros de distribuição.

No próximo capítulo, abordaremos como criar organizações e usuários e a política de controle de acesso em detalhes.

Capítulo 2. Introdução

No capítulo anterior, aprendemos sobre a importante função que o controle de acesso desempenha no e-commerce e seus benefícios-chave para melhorar a eficiência e a confiabilidade de fazer negócios pela Web.

Neste capítulo, discutiremos os princípios fundamentais do gerenciamento de acesso no WebSphere Commerce, como definição de organizações e usuários e como as políticas de controle de acesso são utilizadas para gerenciar as atividades que essas organizações e seus usuários executam através do sistema. Depois de destacar brevemente as etapas para configurar as organizações e os usuários, analisaremos detalhadamente as políticas de controle de acesso, sua função no WebSphere Commerce, e as estudaremos em detalhe.

O capítulo é dividido nas seguintes seções:

- Definindo as organizações e os usuários
- Compreendendo o controle de acesso
- Como inicio a utilização do controle de acesso?

Definindo as Organizações e os Usuários

Para os administradores do site, uma de suas primeiras tarefas depois da instalação e configuração do WebSphere Commerce é configurar e gerenciar o acesso ao site de e-commerce. Isso abrange a criação de organizações que participarão no site, bem como a definição dos usuários que serão membros daquelas organizações.

Em alguns casos, as organizações que se juntam ao seu site podem ser organizações de compradores, ou ainda, você pode ter clientes registrados em seu site que estejam empenhados em um relacionamento business-to-consumer com seu negócio. Independentemente de você estar administrando um site business-to-business ou business-to-consumer, definir a estrutura organizacional do site é uma etapa importante no gerenciamento dos tipos de acesso que os membros têm no seu sistema.

Nesta seção, forneceremos as etapas de alto nível necessárias para definir a estrutura do site. Se você já configurou suas organizações e seus usuários, poderá saltar para a próxima seção sobre controle de acesso. Caso contrário, utilize esta seção como uma diretriz para o planejamento futuro.

Para obter mais detalhes sobre a criação de organizações, usuários e funções, consulte a ajuda online, disponível na página da Technical Library:

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`

Recomendamos também que você consulte o *IBM WebSphere Commerce Fundamentos, Versão 5.4*.

Definindo uma Organização de Vendedores

Normalmente, a organização de vendedores é a organização que possui uma ou mais lojas em um site do WebSphere Commerce. A organização de vendedores também pode ter suborganizações ou divisões, que por sua vez, podem ter uma ou mais lojas. Por exemplo, a loja de exemplo, InFashion, que vende mercadorias da moda, pode ter uma divisão feminina e uma masculina, cada uma com lojas online separadas.

Até agora, vamos considerar que você está configurando uma organização de vendedores que não tem nenhuma suborganização. Para configurar a organização de vendedores, aqui está um amplo esquema do que você precisará fazer:

1. Crie uma nova organização. Ao criar uma nova organização, você criará um perfil para essa organização, que inclui o nome, a descrição, o endereço e a pessoa de contato da organização, bem como o tipo dela.
2. (Opcional) Defina quais tarefas dentro da organização de vendedores exigem aprovação, como processamento de pedidos ou registro de usuários. Esta etapa só é exigida para um site business-to-business. Consulte a ajuda online do produto para obter a documentação de aprovações.
3. Atribua funções à nova organização. Uma organização pode exercer apenas as funções que foram atribuídas a sua organização pai. Uma vez que a Organização Raiz é um antecessor de todas as outras organizações, ela deve ser atribuída a todas as funções possíveis. O WebSphere Commerce oferece um conjunto de funções padrão que você pode iniciar o uso imediatamente. Uma vez que você está criando uma organização de vendedores, funções típicas que podem ser atribuídas incluem Administrador de Vendedor, Administrador de Loja, Desenvolvedor de Loja, Vendedor e assim por diante. Consulte “Funções” na página 12 para obter uma lista das funções padrão.
4. Crie usuários. Da mesma forma que as organizações, você criará um perfil para cada usuário que inclui o nome do usuário, as informações de contato e a função atribuída àquele usuário. Ao atribuir funções, você as selecionará a partir da lista de funções atribuídas à organização na etapa anterior.

Todas as etapas descritas acima podem ser executadas do menu Gerenciamento de Acesso no Administration Console, por um Administrador de Site.

Nota: No WebSphere Commerce Professional Edition, pode haver apenas uma organização de vendedores.

Definindo uma Organização de Compradores

Se você estiver executando um site business-to-business, pode haver uma ou mais organizações de compradores pertencentes ao seu site. (Se você estiver executando um site busines-to-consumer, terá compradores individuais registrados na Organização Padrão). Depois de estabelecer quais empresas participarão em um relacionamento de compras em seu site, você terá que criar uma organização de compradores para cada empresa. Você pode ter quantas organizações de compradores precisar.

As organizações de compradores são estruturalmente semelhantes a organizações de vendedores. Da mesma forma que as organizações de vendedores, as de compradores também podem ter suborganizações ou divisões, que representam atividades de compras diferentes para a organização.

Até agora, vamos considerar que suas organizações de compradores não têm nenhuma suborganização. Para configurar uma organização de compradores, aqui está um esboço do que é necessário fazer:

1. Como foi feito ao criar a organização de vendedores, crie uma nova organização e defina as tarefas que podem ser aprovadas, se necessário. Novamente, definir as tarefas que podem ser aprovadas só é necessário para os sites business-to-business.
2. Atribua funções à nova organização de compradores. Uma vez que está criando uma organização de compradores, as funções típicas que podem ser atribuídas incluem Administrador de Comprador, Comprador, Autorizador do Comprador, e assim por diante.
3. Crie usuários e atribua funções a eles. Ao atribuir funções, você as selecionará a partir da lista de funções atribuídas à organização de compradores na etapa anterior.
4. Repita todo o procedimento para cada organização de compradores que desejar incluir no seu site.

Novamente, todas as etapas destacadas anteriormente são feitas a partir do menu Gerenciamento de acesso no Administration Console.

Nota: No WebSphere Commerce Professional Edition, todos os clientes pertencem à Organização Padrão.

Compreendendo o Controle de Acesso

Depois de concluir a definição das organizações e dos usuários que participarão no seu site de e-commerce, agora você pode gerenciar suas atividades por um conjunto de políticas, um processo conhecido como *controle de acesso*. Nesta próxima seção, analisaremos as políticas de controle de acesso e sua estrutura básica.

O Que É uma Política de Controle de Acesso?

Uma política de controle de acesso é uma regra que descreve qual grupo de usuários é autorizado a executar determinadas atividades no seu site. Essas atividades podem variar de registro a gerenciamento de leilões, a atualização de catálogo de produtos e a concessão de aprovações em pedidos, bem como qualquer uma das centenas de outras atividades exigidas para operar e manter um site de e-commerce.

As políticas são o que concede acesso aos usuários ao seu site. Exceto quando autorizados a executar suas responsabilidades por uma ou mais políticas de controle de acesso, os usuários não têm acesso a qualquer uma das funções do site.

Como Funciona uma Política de Controle de Acesso?

As políticas de controle de acesso são compostas por quatro partes: um grupo de acesso, um grupo de ação, um grupo de recursos e um relacionamento opcional.

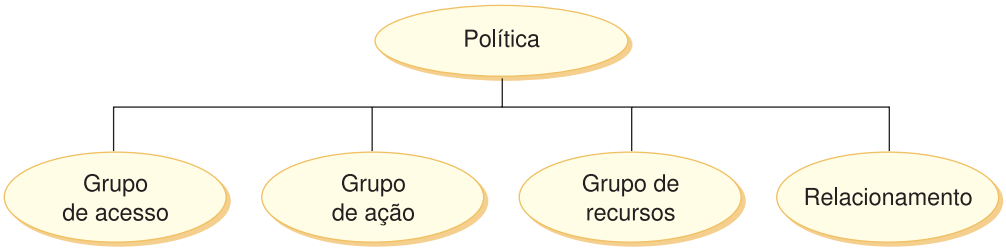
Um *grupo de acesso* é um grupo de usuários que compartilham acesso comum a um conjunto de funções em seu site. Um grupo de acesso geralmente inclui usuários que compartilham atributos comuns, como a mesma função, departamento ou conjunto de habilidades.

Um *grupo de ação* se refere a um grupo de ação que pode ser desempenhado no mesmo recurso. Em geral, o grupo de ação inclui ações associadas a uma área de negócios comum ou a um conjunto de atividades relacionados em seu site.

Um *grupo de recursos* inclui os recursos controlados pela política. Um grupo de recursos pode incluir objetos de negócios como um contrato ou um conjunto de comandos relacionados.

Em alguns casos, um recurso pode apenas ser desempenhado por um usuário que tem um *relacionamento* com aquele recurso. Por exemplo, apenas aqueles usuários que criam um contrato têm permissão para modificá-lo.

Figura 1. As quatro partes de uma política de controle de acesso



Juntas, essas quatro partes definem uma política no WebSphere Commerce, especificando os usuários, as ações que eles executam, o objeto do negócio ou um conjunto de comandos no qual suas ações são executadas e, opcionalmente, o relacionamento que os usuários têm com o grupo de recursos.

Para obter informações mais detalhadas sobre os grupos de acesso, grupos de ações, grupos de recursos e relacionamentos, consulte Capítulo 3, “Conceitos de Controle de Acesso” na página 9.

Como Inicio a Utilização do Controle de Acesso?

Em alguns casos, não temos que fazer nada! Isso porque as políticas padrão no WebSphere Commerce são planejadas para fornecer uma estrutura básica do controle de acesso com base nos usuários típicos em seu sistema e as atividades que eles executam que são associadas as suas funções em uma organização. As políticas abrangem uma ampla gama de atividades de negócios comuns, incluindo associação, criação de pedidos e processamento, aprovações do fluxo de trabalho e comércio, como leilões, pedido para cotas e contratos. Depois de definir suas organizações e seus usuários, as políticas padrão podem ser utilizadas conforme fornecidas ou personalizadas para atender as necessidades individuais de sua empresa.

No entanto, antes de poder decidir se deseja utilizar as políticas padrão ou personalizá-las, é importante compreender com o que elas se parecem no WebSphere Commerce. Para obter uma consulta mais precisa da política padrão, consulte “Analisando uma Política em Detalhes” na página 32.

Capítulo 3. Conceitos de Controle de Acesso

O WebSphere Commerce exibe a autorização de controle de acesso 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 do 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.

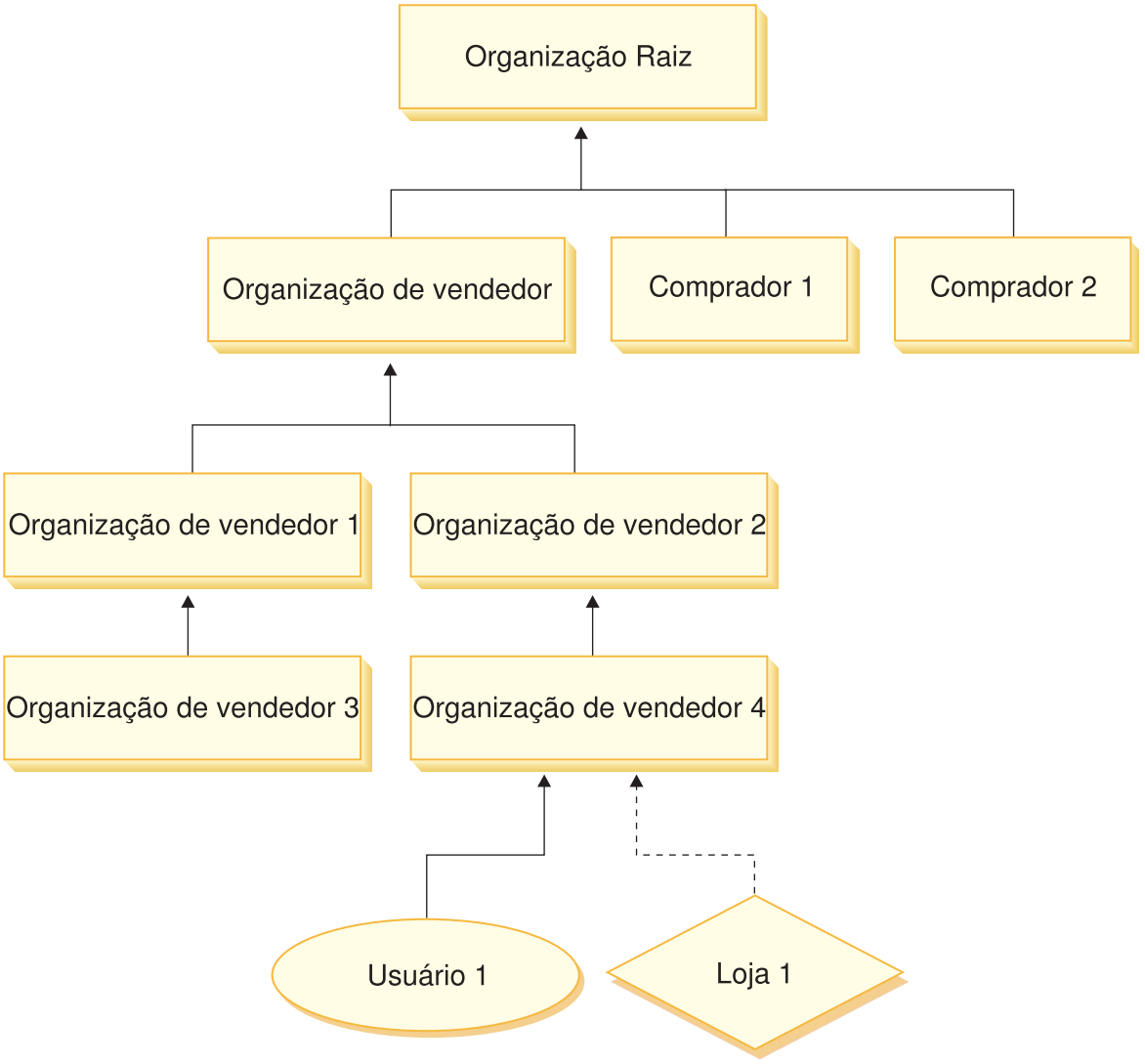


Figura 2. Hierarquia organizacional de um site de business-to-business

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 12.

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 àquelas 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 o frete em massa ou envio de transportadoras para 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 Esta função gerencia o processamento de pedidos, garantindo que os pedidos sejam preenchidos corretamente, que o pagamento seja recebido e que os 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 Business Gerente de Propaganda ou de B2C Produto rastreia compras do cliente, sugere descontos e determina a melhor forma de exibir, definir 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 objetos no sistema que precisam ser protegidos. Por exemplo RFQs, leilões, usuários e pedidos são alguns dos recursos doWebSphere Commerce que precisam ser protegidos. Cada recurso tem seu proprietário. A propriedade do recurso é utilizada para determinar quais políticas de controle de acesso se aplicam a ela. As políticas de controle de acesso têm um proprietário, que é uma entidade organizacional. Uma política só é aplicada a recursos que pertencem à mesma entidade organizacional que possui a política. As políticas pertencentes a entidades organizacionais antepassadas também são aplicadas ao recurso.

Recursos de Comandos do Controlador: Para controle de acesso baseado em função para os comandos do controlador, a política é estruturada de forma que a ação `Execute` esteja sendo executada no recurso de comandos do controlador. Essas políticas são destinadas a restringir a execução dos comandos do controlador para usuários com uma função especificada. O grupo de acesso para essas políticas é geralmente aquele com uma única função, por exemplo, Gerentes de produtos (aquele com a função de Gerente 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 *Manual do Programador do WebSphere Commerce 5.4* 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 *Manual do Programador do WebSphere Commerce 5.4* .

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 pendente (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. Par obter mais informações sobre como definir os grupos de relacionamentos, consulte “Definindo Grupos de Relacionamentos” na página 89.

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.

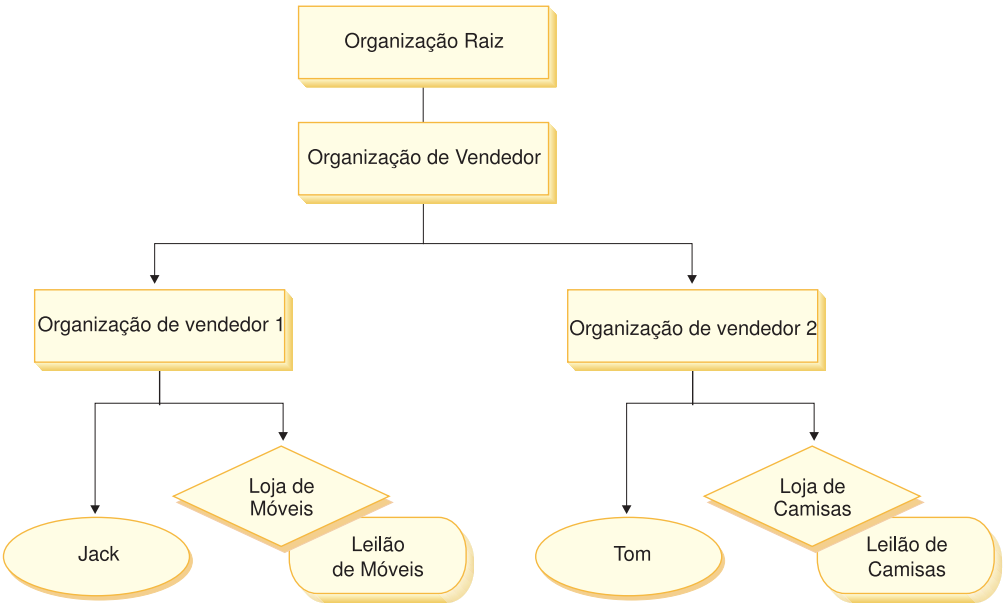
Substituindo Políticas Modelo: Outro recurso de políticas modelo é que elas podem ser substituídas para entidades organizacionais especificadas. Voltando ao exemplo acima, se uma 11a entidade organizacional for incluída no site do WebSphere Commerce, mas esta mais nova entidade organizacional não desejar 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 24, 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 mobílias, mas *não* o leilão de camisas. Tom pode modificar o leilão de camisas, mas *não* o leilão de mobílias.

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

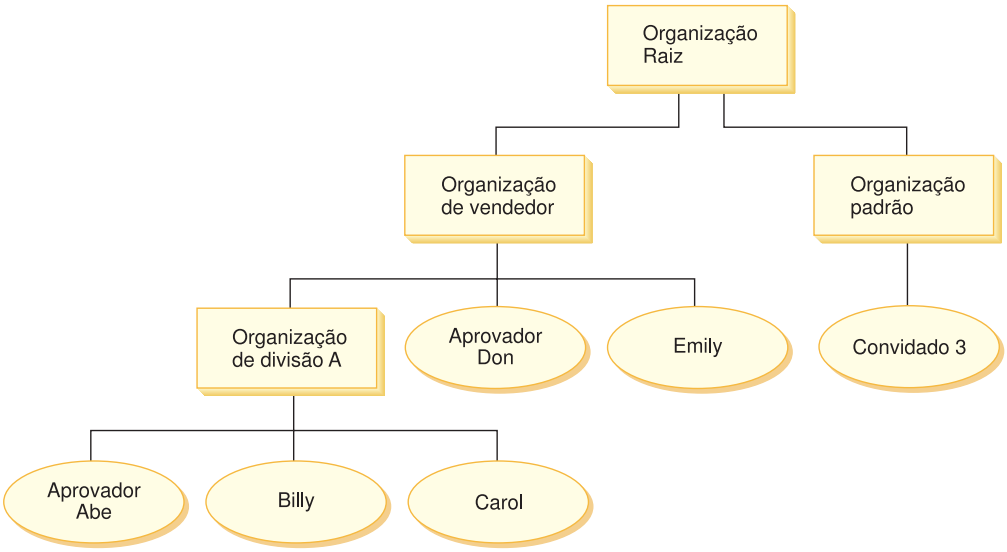
O *Gerenciador de Políticas* é o componente de controle de acesso que determina se o usuário atual tem permissão ou não para executar a ação especificada no recurso especificado. As políticas de controle de acesso são especificadas no formato XML. Na instalação, as políticas padrão são carregadas automaticamente 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.

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 22.

O diagrama a seguir 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 de 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 de 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 28.

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 de 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 de 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, - ]normal política 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.

Analisando uma Política em Detalhes

Agora que compreendemos a estrutura básica de uma política de controle de acesso, vamos analisar uma das políticas padrão em detalhes, utilizando uma série de exemplos diferentes. A política que estudaremos é a seguinte:

`AuctionAdministratorsForOrgExecuteAuctionManageCommandsOnAuctionResource`

Nota: Esta política é uma política de nível de recurso. Seu tipo de política é modelo.

No primeiro exemplo, aprendemos a ler a política utilizando oWebSphere Commerce Administration Console, identificar suas partes e compreender o que a política significa. O segundo exemplo analisará a política em XML para ajudá-lo a compreender que as informações iguais se parecem no código.

O terceiro exemplo vai uma etapa adiante na compreensão de como uma política está relacionada com outras políticas. Compreender dependências entre políticas é um pré-requisito importante para fazer alterações para acessar as políticas de controle ou criar novas.

Exemplo 1: Lendo uma Política

Neste exemplo, utilizaremos oWebSphere Commerce Administration Console para analisar uma política e identificar as partes que a definem. Também utilizaremos essas peças para formar uma descrição geral da política.

Analisando a Política no Administration Console

1. Efetue login no WebSphere Commerce Administration Console. No menu Gerenciamento de Acesso, selecione **Políticas**.
2. Verifique se o menu drop down Exibir está definido para sua organização.
3. Na página Políticas, role pela lista de políticas e localize a seguinte política: `AuctionAdministratorsForOrgExecuteAuctionManageCommandsOnAuctionResource`

   Observe que você pode rolar pela lista de políticas utilizando a barra de rolagem, bem como utilizando os links **Primeiro**, **Anterior**, **Avançar** e **Último**.

Exibindo as partes da política

1. Selecione a política clicando na caixa ao lado dela e clique em **Exibir grupo de ações**.
2. Na página Grupo de ações, você verá o grupo de ações, AuctionManage. Isso é um grupo de ações associado à política. Selecione `AuctionManage` e clique em **Exibir ações**.
3. Na próxima página, você verá a seguinte lista de ações ou comandos, incluída no grupo de ação `AuctionManage`:
   - `com.ibm.commerce.negotiation.commands.CloseBiddingCmd`
   - `com.ibm.commerce.negotiation.commands.DeleteAuctionCmd`
   - `com.ibm.commerce.negotiation.commands.ModifyAuctionCmd`

   Aqui, `AuctionManage` inclui o fechamento de um leilão (`CloseBiddingCmd`), a exclusão de um leilão (`DeleteAuctionCmd`) e a modificação de um leilão (`ModifyAuctionCmd`). Para obter mais informações sobre os comandos, consulte a seção de referência na documentação de ajuda online.

   Observe que você também pode acessar a mesma lista de ações a partir da página Políticas clicando em **Exibir ações**.
4. Para retornar para a página de políticas, selecione qualquer uma das ações e clique em **Exibir Políticas**.
5. Selecione a política novamente, mas agora clique em **Exibir Grupo de Membros** para ver o membro (grupo de acesso) ao qual esta política se aplica.
6. Anote o nome do grupo de membros (acesso). Neste caso, o grupo de membros (acesso) é `AuctionAdministratorsForOrg`.
7. No menu Gerenciamento de Acesso, selecione **Grupos de Acesso** .
8. Localize `AuctionAdministratorsForOrg`. Selecione-o e clique em **Alterar.**
9. Clique em **Critérios**. Na página de Critérios, procure em Organizações e funções selecionadas. Você deve ver as seguintes funções:
   - `Seller-For organization`
   - `Product Manager-For organization`
   - `Buyer (sell-side)-For organization`

- Category Manager-For organization

  Qualquer usuário a quem foi atribuído uma dessas funções da organização que possui o recurso de leilão é parte do grupo de acesso AuctionAdministratorsForOrg.

10. Deixe a página Critérios sem fazer quaisquer alterações. No menu Gerenciamento de Acesso, selecione **Políticas** novamente. Localize a seguinte política:

    AuctionAdministratorsForOrgExecuteAuctionManageCommandsOnAuctionResource

11. Selecione a política e Clique em **Exibir Recursos**. Na página Recursos, você verá o recursocom.ibm.commerce.negotiation.objects.Auction. Este é o recurso no qual as ações listadas no grupo de ações atua. Neste caso o recurso é um leilão. Observe que você pode acessar esta mesma lista na página Políticas clicando em **Exibir Grupo de Recursos** e detalhando para recursos individuais.
12. Selecione agora **Políticas** no menu Gerenciamento de Acesso, e localize a seguinte política:

    AuctionAdministratorsForOrgExecuteAuctionManageCommandsOnAuctionResource

13. Selecione a política e clique em **Alterar**. Na página Alterar Política, examine o menu drop down em **Relacionamento** . Observe que o relacionamento é definido como nenhum. Isso significa que a política não tem um relacionamento.
14. Clique em **Cancelar** e **OK** para a caixa de diálogo.

Compreendendo o que a Política significa

Agora que nós identificamos as partes individuais desta política, podemos começar a juntá-las para entender o que a política faz. Primeiro, sabemos que a política se aplica a todos os usuários que pertencem ao grupo AuctionAdministratorsForOrg. Aprendemos isso clicando em **Exibir Grupo de Membros**. De lá, utilizamos o menu Gerenciamento de Acesso para ir para a página Grupo de Acesso e vimos que o grupo de acesso incluía as seguintes funções: vendedor, gerente de produtos, comprador (lado de vendas) e o gerente de categorias. Coletivamente, os usuários com uma dessas quatro funções podem ser mencionados como um Administrador de Leilão.

Também sabemos que o grupo de ações contém os comandos para modificar, retirar e fechar um leilão e que o grupo de recursos inclui somente o recurso de leilão que está sendo gerenciado. Novamente, sabemos isso clicando em **Exibir Ações** e **Exibir Recursos** na página Políticas e detalhando para o nível de detalhamento. Por último, podemos dizer que a política não inclui um relacionamento entre o grupo de acesso e os recursos.

Reunindo tudo, podemos concluir que esta política permite que os Administradores de Leilão executem todas as atividades associadas ao gerenciamento de leilões, em um recurso de leilão, como modificar, retirar e fechar um leilão, desde que o administrador exerça a função para a organização que possui o leilão.

Podemos obter um sentido do que significa examinando seu nome. Neste exemplo, a política começa com o nome do grupo designado de usuários, AuctionAdministrator. ForOrg indica que a política é aplicada a organizações. AuctionManageCommands descreve o grupo de ação e AuctionResource descreve o grupo de recursos.

Exemplo 2: Lendo uma Política em XML

As políticas de controle de acesso padrão são armazenadas em um arquivo XML carregado em seu banco de dados durante a criação da instância. Quando você examina uma política no WebSphere Commerce Administration Console, está utilizando a interface para exibir e fazer alterações para as informações armazenadas no arquivo de banco de dados. As informações no banco de dados são utilizadas pelo Gerenciador de Políticas para avaliar o controle de acesso. Se as informações do banco de dados forem mais recentes que o arquivo XML, é possível utilizar a ferramenta Extractor para extrair as informações de política de controle de acesso do banco de dados para o arquivo XML.

A maior parte do tempo, você utilizará a interface do usuário doWebSphere Commerce Administration Console para gerenciar políticas. No entanto, se quiser ver uma política em XML ou se quiser fazer uma modificação avançada, é assim a aparência de uma política no arquivo XML:

```
<!-- AuctionAdministrators
manage Auctions (Retract/delete auction,
Modify auction, Close Auction)
-->
<Policy
Name="AuctionAdministratorsForOrgExecuteAuctionManageCommandsOnAuctionResource"
OwnerID="RootOrganization"
UserGroup="AuctionAdministratorsForOrg"
ActionGroupName="AuctionManage"
ResourceGroupName="AuctionDataResourceGroup"
PolicyType="template">
</Policy>
```

Aqui, a política é definida por:

`Name`: O nome da política.

`OwnerID`: A organização na qual a política se aplica.

`UserGroup`: O grupo de acesso.

`ActionGroupName`: O grupo de ações.

`ResourceGroupName`: O grupo de recursos.

`PolicyType`: O tipo de política, como a de nível de site, modelo ou organização.

O arquivo que contém todas as políticas de controle de acesso padrão é chamado `defaultAccessControlPolicies.xml` e está localizado no seguinte diretório:

`X:\`*`installation_directory`*`\xml\policies\xml`.

Nota: As descrições para cada arquivo de controle de acesso padrão são contida no arquivo `defaultAccessControlPolicies_`*`locale`*`.xml`, que podem ser encontradas no mesmo diretório. Uma alteração feita em uma política de controle de aceso padrão no arquivo de controle de acesso padrão precisa ter sua descrição correspondente atualizada em`defaultAccessControlPolicies_en_US.xml`. No entanto, recomendamos que as alterações feitas nos arquivos XML sejam reservadas para usuários avançados.

Exemplo 3: Identificando outras Políticas Associadas a sua Política

Neste último exemplo, examinaremos como uma política de controle de acesso pode ser dependente de outras políticas.

As políticas que definem os comandos (ações) que um grupo de usuários (um grupo de acesso) pode executar em um recurso são chamadas de políticas em nível do recurso. Por exemplo, a política que temos examinado em detalhes:

`AuctionAdministratorsForOrgExecuteAuctionManageCommandsOnAuctionResource` é um exemplo de uma política em nível do recurso.

No entanto, as ações permitidas pela política em nível do recurso também são dependentes das ações permitidas para cada função pertencente ao grupo de acesso da política. As políticas que descrevem quais ações são permitidas para uma determinada função são chamadas políticas baseadas em funções.

Para identificar as políticas baseadas em funções associadas a uma política em nível do recurso, faça o seguinte:

Analisando as funções associadas com a política

1. Efetue login noWebSphere Commerce Administration Console e localize a política de nível de recurso na página Políticas. Utilizando o mesmo exemplo, sabemos que a política que desejamos é a seguinte:
   `AuctionAdministratorsForOrgExecuteAuctionManageCommandsOnAuctionResource`
   .
2. Identifique o grupo de acesso associado à política. Nesse caso, já sabemos que o grupo de acesso é `AuctionAdministratorsForOrg`.
3. Procure as funções associadas ao grupo de acesso. Para `AuctionAdministratorsForOrg` , sabemos de exemplos anteriores que as funções são: `Compradores (lado de vendas)`, `Gerentes de Categoria`, `Gerentes de Produto` e `Vendedores`.

Analisando as políticas baseadas na função para cada função

1. Mude para o Apêndice no final deste manual e localize o cabeçalho da seção, Políticas Baseadas em Funções. Você utilizará o Apêndice para localizar cada política baseada em função associada a uma função.
2. Localize a política `Buyers(sell-side)ExecuteBuyers(sell-side)CommandsResourceGroup`. Esta política está associada à função `Compradores (lado de vendas)`. Sabemos isso porque `Buyers(sell-side)` é o prefixo da política.
3. Localize o restante das políticas baseadas em funções associadas a funções `Compradores (lado de vendas)`, `Gerente de Categorias`, `Gerente de Produtos` e `Vendedores`, utilizando seus prefixos para identificar as políticas corretas. Você deve apresentar a seguinte lista:
   - `Buyers(sell-side)ExecuteBuyers(sell-side)CommandsResourceGroup`
   - `Buyers(sell-side)ExecuteBuyers(sell-side)Views`
   - `CategoryManagersExecuteCategoryManagersCmdResourceGroup`
   - `CategoryManagersExecuteCategoryManagersViews`
   - `ProductManagersExecuteProductManagersCmdResourceGroup`
   - `ProductManagersExecuteProductManagersViews`

- SellersExecuteSellersCmdResourceGroup
- SellersExecuteSellersViews

4. Cada política baseada em funções permite que os usuários com aquela função executem determinados comandos ou exibições do controlador. Para ver qual ação está associada a uma política baseada em funções, procure a política na página Políticas no WebSphere Commerce Administration Console, utilizando o mesmo procedimento do Exemplo 1.

Porque é Importante Identificar Dependências entre Políticas

Compreender quais políticas baseadas em funções estão associadas a uma política em nível do recurso é, freqüentemente, um pré-requisito para personalizar suas políticas e para criar novas.

No Capítulo 5, "Cenários de Personalização" na página 47, você aprenderá mais sobre as políticas baseadas em funções e em nível de recursos, incluindo como reconhecê-las, compreender suas diferenças e ver como elas estão relacionadas uma com as outras.

Capítulo 4. Personalizando as Políticas de Controle de Acesso Padrão

As políticas de controle de acesso padrão fornecidas pelo WebSphere Commerce levam a requisitos básicos que as organizações têm para regular as ações e informações disponíveis para seus usuários. Freqüentemente, as políticas padrão podem ser suficientes para as necessidades do seu site. Ao mesmo tempo, as políticas padrão são altamente personalizáveis, o que permite que você as adapte para suas próprias necessidades.

A política `SiteAdministratorsCanDoEverything`, é uma política padrão especial que concede acesso de super-usuário aos administradores com a função Administrador de Site. Nesta política, um Administrador de Site pode executar qualquer ação em qualquer recurso, mesmo se tais ações ou recursos não tiverem sido definidos. É importante estar atento a isto ao atribuir esta função aos usuários.

Este capítulo oferece informações sobre como fazer alterações básicas nas políticas de controle de acesso padrão incluídas no WebSphere Commerce. Começamos apresentando determinados conceitos e relacionamentos necessários para a compreensão.

Nota: Se encontrar termos ou conceitos que não lhe sejam familiares, consulte Capítulo 3, “Conceitos de Controle de Acesso” na página 9´ para obter mais informações.

Identificando as Políticas Afetadas por uma Alteração

No capítulo anterior, você aprendeu que as políticas estão freqüentemente relacionadas com outras políticas. Você também aprendeu como iniciar uma política em nível do recurso e a identificar as políticas baseadas em funções associadas a ela. Nesta seção, explicaremos com mais detalhes como as políticas estão relacionadas uma com as outras e porque você precisa compreender seus relacionamentos antes de poder modificar uma política existente ou criar uma nova. Em muitos casos, você precisa alterar diversas políticas para implementar adequadamente uma alteração.

Compreendendo o Relacionamento entre as Políticas Baseadas em Funções e em Nível de Recurso

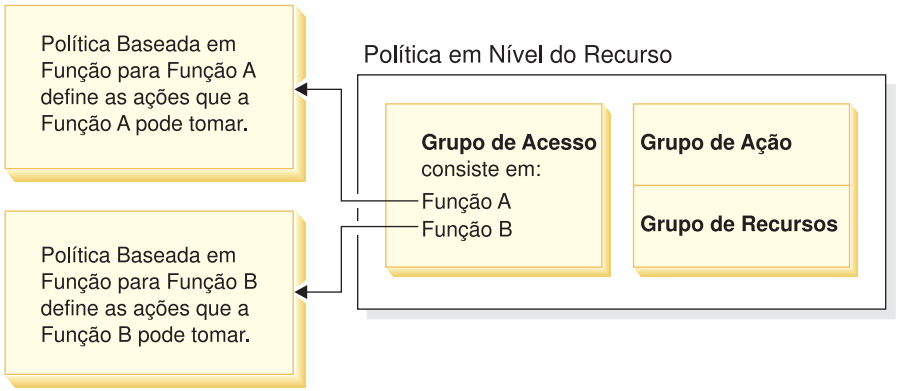
No WebSphere Commerce, cada ação que pode ser tomada por um usuário é atribuída a uma ou mais funções, utilizando as políticas baseadas em funções da seguinte maneira:

- Cada função padrão tem um grupo de acesso correspondente. Por exemplo, o grupo de acesso para a função Administrador do Site é `StoreAdministrators`.
- Cada grupo de acesso ″baseado em função″ geralmente tem duas políticas com base em funções associadas:
  - Uma política que define os comandos do controlador que a função está autorizada a executar.
  - Uma política que define as ações de exibição que a função está autorizada a executar. Mostra mapa de ações para exibições da tabela VIEWREG. Por exemplo, `StoreListView` exibe uma página da Web com a lista de lojas no sistema.

Alguns comandos do controlador possuem apenas uma política baseada na função, mas nenhuma política a nível do recurso. Isso ocorre se o comando não estiver operando em algum recurso protegível. Por exemplo. o comando `SetCurrencyPreferenceCmd` não precisa de uma política a nível do recurso, já que ela pode apenas alterar a preferência da moeda para o usuário que está executando o comando. Se fosse possível de alterar a preferência da moeda de outro usuário, então, o objeto do usuário deveria ser protegido e seria necessária uma política a nível do recurso. .

As políticas a nível do recurso para comandos do controlador estão diretamente relacionadas a determinadas políticas baseadas em funções para os comandos do controlador. Na política a nível do recurso, o comando do controlador faz parte do grupo de ação, mas na política baseada em funções, o comando do controlador faz parte do grupo de recursos. A figura abaixo ilustra este relacionamento. A política em nível do recurso inclui as Funções A e B em seu grupo de acesso, que põe as políticas baseadas em funções para as Funções A e B em jogo. Enquanto a política em nível do recurso concede autorização para usuários com funções A ou B para tomar determinadas ações em um conjunto de recursos específico, as políticas baseadas em funções associadas fornecem autorização para usuários com funções A e B para executar essas ações em geral.

Figura 3. Relacionamento entre uma política em nível do recurso e suas políticas baseadas em funções associadas



A figura a seguir mostra um exemplo de política em nível do recurso que autoriza usuários no grupo de acesso `Pessoas` a ler ou estudar determinados recursos - ou seja, livros, revistas e jornais. Esta política é corretamente formulada porque as políticas baseadas em funções para as funções `filho` e `adulto` também as autoriza a ler ou estudar livros, revistas e jornais.

Figura 4. Uma política em nível do recurso e as políticas baseadas em funções que a afetam.

Observe que em políticas baseadas em funções para comandos do controlador:

- O grupo de ação contém apenas uma única ação: `Executar`.
- O grupo de recursos contém o comando do controlador que pode ser executado.

Semelhantemente, em políticas baseadas em funções para exibições:

- O grupo de ação contém as exibições que podem ser executadas.
- O grupo de recursos contém um único recurso: `com.ibm.commerce.command.ViewCommand`.

Por outro lado, nas políticas em nível do recurso:

- O grupo de ação contém o conjunto de ações que podem ser executadas nos recursos no grupo de recursos.
- O grupo de recursos contém uma lista de recursos de negócios reais que podem ser desempenhados.

Uma política em nível do recurso pode apenas autorizar os usuários em uma determinada função para executar ações já autorizadas pela política baseada em função correspondente. Por exemplo, no exemplo acima, a função `filho` está autorizada a executar as seguintes ações:

- Estudar
- Ler
- Jogar

Suponha que a política em nível do recurso agora é alterada para incluir uma nova ação chamada `trabalhar`. Os usuários com a função `adulto` poderão executar a ação `trabalhar`. No entanto, os usuários com a função `filho` não. O motivo para isso é aparente quando você verifica as políticas baseadas em funções para duas funções. A política para `adulto` lista a ação `trabalhar` no seu grupo de recursos. A política para `filho` não. Embora `filho` e `adulto` sejam adequadamente autorizados pela política em nível do recurso, a política baseada em funções para `filho` não autoriza a ação `trabalhar`.

Por causa da forma que as políticas em nível do recurso estão ligadas às políticas baseadas em funções, a melhor maneira de acompanhar todas as políticas afetadas por uma determinada alteração é trabalhar de volta a partir da política em nível do recurso. A primeira etapa é examinar o grupo de acesso da política em nível do recurso e determinar se ela contém quaisquer funções. Você pode exibir a lista completa de funções padrão selecionando o Gerenciamento de Acesso > Funções no Administration Console.

Se o grupo de acesso da política em nível do recurso incluir funções, reveja as políticas baseadas em funções para ver se elas precisam ser alteradas. Se estiver incluindo uma ação no grupo de ação de uma política em nível do recurso, será necessário certificar-se de que as políticas baseadas em funções relevantes também autorizem a nova ação. Se estiver excluindo uma ação de uma política em nível do recurso, e nenhuma outra política em nível do recurso faz referência a esta ação, é melhor remover o recurso correspondente das políticas baseadas em funções associadas.

Compreendendo o Modelo da Política

Uma política de autorização deve ser apresentada para um usuário para executar uma ação. No entanto, o WebSphere Commerce permite que os usuários executem uma ação se **alguma** política fornecer a autorização necessária. Contudo, se você definir uma política nova mais limitada do que a padrão, deverá excluir ou modificar a política padrão mais ampla para evitar que ela substitua a nova.

Por exemplo, suponha que a política padrão A autoriza todos os usuários registrados a submeter lances no leilão. Você quer alterar esta política de forma que o lance do leilão seja limitado para os usuários com a função de compradores. Se você definir meramente uma nova política que autoriza os compradores a criar lances de leilão, então sua nova política não terá nenhum efeito. A política padrão A ainda permitirá que todos os usuários registrados submetam um lance. Para fazer com que sua nova política vigore, você deverá excluir a política padrão mais ampla.

A Tabela 1 resume as alterações adicionais que devem ser feitas ao criar, excluir ou alterar uma política em nível do recurso.

Tabela 1. Alterações adiconais necessárias quando você altera uma política em nível do recurso que utiliza as funções.

Quando você faz esta alteração em uma política em nível do recurso:	**Você também deve fazer a seguinte alteração se o grupo de acesso em nível do recurso utilizar as funções:**
Incluir uma ação no grupo de ação da política.	Garantir que as políticas baseadas em funções aplicáveis incluam a ação em seus grupos de recursos.
Remover uma ação do grupo de ação da política.	Nenhuma alteração adicional obrigatória.Por coerência, é melhor remover esta ação dos grupos de recurso correspondente nas políticas baseadas em funções relacionadas. Isso deveria ser feito apenas se nenhum outro grupo de ação estiver fazendo referência a esta ação. Se outro grupo de ação estiver fazendo referência a esta ação, provavelmente há políticas baseadas em funções que ainda precisam ter esta ação em seu grupo de recursos.
Utilizar um grupo de ação diferente.	Garantir que as políticas baseadas em funções aplicáveis incluam em seus grupos de recursos as novas ações do grupo de ação.
Incluir uma função no grupo de acesso da política.	Certifique-se de que a política baseada em função correspondente à nova função, refere-se a um grupo de recursos que inclui as ações especificadas na política em nível do recurso.
Remover uma função do grupo de acesso da política.	Nenhuma alteração adicional obrigatória.Por coerência, é melhor modificar a política baseada em função correspondente para que não mais faça referência a estas ações em seu grupo de recursos.
Utilizar um grupo de acesso diferente.	Garantir que as políticas baseadas em funções aplicáveis incluam nos seus grupos de recursos as ações no grupo de ação da política em nível do recurso.
Criar uma nova política.	Verificar se há uma política existente que autorize as mesmas ações. Excluir, se necessário.
Exclua a política.	Para impedir que alguns usuários executem essas ações da política, excluir quaisquer outras políticas que autorizem as mesmas ações.

Determinando se uma Política é Baseada em Funções ou em Nível do Recurso

As políticas baseadas em funções também são conhecidas como políticas em nível de comandos porque elas autorizam os usuários com uma determinada função a executar um conjunto de comandos. As políticas em nível do recurso autorizam um grupo de usuários a executar um conjunto de comandos em um determinado conjunto de recursos. Por exemplo, uma política baseada em funções pode autorizar crianças a comer. Enquanto uma política em nível do recurso pode autorizar crianças a comer arroz.

Geralmente você pode determinar se uma política é baseada em funções ou em nível do recurso examinando seu nome.

Políticas Baseadas em Funções

As políticas que definem os comandos do controlador que uma função pode executar seguem a convenção de nomenclatura:

<AccessGroupforRoleXYZ> Execute <XYZCmdResourceGroup>

Por exemplo: `ProductManagersExecuteProductManagersCmdResourceGroup`.

Nas políticas baseadas em funções para comandos do controlador, o grupo de ação contém uma única entrada chamada `Execute` e o grupo de recursos contém uma lista de comandos do WebSphere Commerce que os usuários com aquela função podem executar.

As políticas que definem as exibições que uma função pode executar seguem a convenção de nomenclatura:

<AccessGroupforRoleXYZ> Execute <XYZViews>

Por exemplo: `SalesManagersExecuteSalesManagerViews`.

Nas políticas baseadas em funções para exibições, o grupo de ação contém uma lista de exibições que os usuários com aquela função podem executar.

Políticas em Nível do Recurso

As políticas que definem quem pode executar ações nos recursos de dados (objetos de negócios que podem ser criados ou manipulados) seguem a convenção de nomenclatura:

<AccessGroupXYZ> Execute <XYZCommands> On <XYZResource>

Por exemplo: `AllUsersExecuteOrderProcessOnOrderResource`.

Nas políticas em nível do recurso, o grupo de ação contém os comandos do WebSphere Commerce e o grupo de recursos identifica os recursos de negócios específicos que podem ser desempenhados.

Uma exceção são as políticas que autorizam a criação de uma entidade como um pedido, um lance ou uma RFQ. Essas políticas não agem na entidade em si porque ela ainda não foi criada. Ao contrário, elas agem na entidade incluída. Por exemplo, um leilão é criado no contexto de uma loja, um usuário é criado no contexto de uma organização. A maioria dos recursos é criado no contexto de uma loja. Conseqüentemente, essas políticas têm nomes como:

<AccessGroupXYZs> Execute <XYZCommands> On <StoreEntityResource>

Por exemplo:
`AuctionAdministorsForOrgExecuteAuctionCreateCommandsOnStoreEntityResource`.

As políticas que definem quem pode exibir os recursos do Bean de Dados (os Beans de dados contêm informações sobre os recursos de dados, como um lance ou um pedido; geralmente utilizado em JSPs) seguem a convenção de nomenclatura:

<AccessGroupXYZs> Display <XYZDatabeanResourceGroup>

Por exemplo: `MembershipViewersForOrgDisplayMembershipDatabeanResourceGroup`.

Dicas para Alterar Políticas Padrão

Fique ciente do seguinte ao alterar suas políticas padrão:

- A maioria dos grupos de acesso é definida por funções de usuários como comprador ou gerente de produtos. Para compreender melhor estas funções e quais ações elas têm permissão para executar, consulte "Funções" na página 12.
- Antes de alterar uma política para utilizar um grupo de acesso diferente, reveja a definição desse grupo de acesso para garantir que atenda às suas exigências. Para isso, selecione **Gerenciamento de Acesso > Grupos de Acesso** no Administration Console.
- Dependendo do valor selecionado para Exibir, a página Políticas exibe tanto as políticas em nível de site quanto as políticas específicas para uma determinada organização:
  - Se você definir o campo Exibir como `Organização Raiz`, serão exibidas as políticas padrão pertencentes à organização raiz e as versões mestre das políticas de modelo.
  - Se definir o campo Exibir como o nome de uma organização, será exibido as políticas padrão pertencentes àquela organização e as políticas de modelo que podem ser modificadas por esta organização
- Renomeie quaisquer políticas padrão alteradas de forma que o nome da política reflita o que a política faz e que você possa identificar as políticas padrão que você alterou. Considere implementar uma convenção de nomenclatura para suas políticas personalizadas. Se adequado, você também deve modificar a descrição da política e seu nome de exibição.

Nota: O WebSphere Administration Console pode executar apenas modificações simples nas definições da política de controle de acesso e nas definições do grupo de acesso. A solução mais eficaz é atualizar os dados utilizando os arquivos XML. As operações a seguir podem ser feitas apenas através do XML:

1. Definir novas ações, recursos, atributos, relacionamentos e grupos de relacionamentos.
2. Definir grupos de recursos complexos implícitos e grupos de acesso complexos implícitos.

Depois de Fazer as Alterações na Política

Cada vez que você criar ou modificar uma política de controle de acesso, deverá executar determinados testes para verificar se a política está funcionando corretamente.

Após ter terminado de testar todas as suas políticas novas e alteradas que estão atualmente no banco de dados, é aconselhável extrair as informações nos arquivos XML. Estes arquivos possuem o mesmo formato que os arquivos relacionados à política de controle de acesso inicial: `defaultAccessControlPolices.xml`, `defaultAccessControlPolicies_locale.xml` e `ACUserGroup_locale.xml`. Esta etapa é necessária porque as alterações feitas utilizando o Administration Console afetam apenas as informações da política armazenadas nos bancos de dados. Os arquivos XML que foram utilizados para carregar as políticas de controle de acesso padrão e seus componentes durante a criação da instância não são atualizados automaticamente.

Você deve manter a consistência entre os arquivos XML e as informações de controle de acesso no banco de dados por diversos motivos:

- Quando você cria uma instância de WebSphere Commerce, a política e as definições do grupo de acesso são carregadas a partir dos arquivos XML.
- Os arquivos XML oferecem uma maneira conveniente de exibir e editar diretamente suas políticas e peças de componentes; portanto, manter os arquivos atualizados é essencial.

Testando as Alterações da Política

Para cada política, certifique-se do seguinte:

- Um usuário que pertence ao grupo de acesso da política pode executar as ações especificadas nos recursos especificados. Se você removeu autorização para executar uma ação, você também deve testar para certificar-se de que o usuário não pode mais executar a ação.
- Um usuário que não pertence ao grupo de acesso da política não pode executar as ações especificadas nos recursos especificados.

Por exemplo, suponha que você implemente o cenário 1 de personalização de Leilão no Capítulo 5, no qual remove a capacidade dos administradores de leilão em fechar o lance de leilões. Para testar se esta alteração está funcionando corretamente, efetue login como um usuário que pertence ao grupo de acesso `administrador de leilões` e execute as seguintes ações:

- Modificar um leilão
- Excluir um leilão.

Você também deve verificar se um Administrador de Leilões não pode fechar o leilão.

Em seguida, efetue login como um usuário que não pertence ao grupo de acesso `administrador de leilões` e tente executar as mesmas ações. Se a política estiver funcionando corretamente, suas tentativas falharão.

Extraindo as Alterações das Políticas em Arquivos XML

Quando tiver concluído e testado suas alterações na política, você deverá atualizar os arquivos XML para mantê-los em sincronia com as informações da política nos bancos de dados. O Apêndice descreve os arquivos XML diferentes relacionados às políticas de controle de acesso e os grupos de acesso. Também explica como extrair alterações de políticas dos bancos de dados em arquivos XML e como carregar as informações da política de arquivos XML em bancos de dados.

Capítulo 5. Cenários de Personalização

Os cenários de personalização apresentados a seguir permitem que você aplique o que você aprendeu sobre as políticas de controle de acesso para fazer uma série de alterações básicas em suas políticas padrão. Para todos esses cenários, presume-se que o Administrador do Site esteja modificando as políticas para Organização Raiz. Assim que você percorrer alguns cenários, poderá seguir a mesma metodologia para fazer alterações não abordadas aqui especificamente.

Os cenários são organizados por área de negócios. Em cada área de negócios, os cenários são apresentados na ordem de complexidade ampliada.

Tabela 2. Tabela de conteúdo para cenários

Área de negócios	**Começando na página**
Leilões	"Cenário 1 de Leilões: Removendo a Capacidade dos Administradores de Leilões para Fechar o Lance do Leilão" na página 48
Contratos	"Cenário 1 de Contratos: Remover a Capacidade dos Administradores de Contratos em Incluir ou Excluir Conexões para Contratos" na página 52
Pedidos	"Cenário 1 de Pedidos: Permitindo que Apenas Compradores Criem Pedidos" na página 55
Associação	"Cenário 1 de Associação: Remover a Capacidade dos Usuários de Auto-Registrarem" na página 61
Cupons	"Cenário 1 de Cupons: Permitindo que Apenas Compradores Resgatem Cupons" na página 65
Procurement	"Cenário 1 de Procurement: Permitindo que os Gerentes de Carrinho de Compras Gerenciem o Carrinho de Compras do Procurement para Pedidos Criados por sua Organização" na página 69
Estoque	"Cenário 1 de Estoque: Permitir que os Gerentes do Centro de Distribuição Atualizem os Centros de Distribuição, Mas Não os Exclua" na página 72
Inteligência de negócios	"Cenário 1 Inteligência de Negócios: Permitindo que Auditores Exibam os Relatórios de Inteligência de Negócios" na página 74

Se estiver procurando um cenário que ilustre um determinado tipo de alteração, consulte a Tabela a seguir, que faz referência cruzada a cenários por tipo de personalização ilustrada.

Tabela 3. Cenários de personalização organizados por tipo de personalização

Personalização	**Consulte a página**

Tabela 3. Cenários de personalização organizados por tipo de personalização (continuação)

Incluindo uma função em um grupo de acesso de política	67
Alterando o grupo de ação de uma política	70,72
Alterando o relacionamento de recursos de uma política	57,69
Alterando uma política para utilizar um grupo de acesso diferente	51,55,57,62,66,67
Criando um novo grupo de acesso e utilizando-o em uma política	59,63
Criando um novo grupo de ação e utilizando-o em uma política	63,70
Criando uma nova política em nível do recurso	53,70
Criando uma nova política baseada em funções	63,74
Criando uma nova função e utilizando-a em uma política em nível do recurso	63,74
Excluindo uma política	49,50,61
Removendo uma ação de um grupo de ação da política	3,52

Tabela 3: Cenários de Personalização Organizados por Tipo de Personalização

Cenário 1 de Leilões: Removendo a Capacidade dos Administradores de Leilões para Fechar o Lance do Leilão

Por padrão, os administradores de leilão para uma loja podem modificar ou excluir leilões da loja, bem como fechar lances. Em determinados casos, você pode não querer conceder aos administradores de leilão a autoridade para fechar lances, tanto porque você deseja que esta ação seja tratada por outros quanto porque você não exige esta ação para a loja.

Neste cenário, você removerá a autoridade dos administradores de leilão em fechar lances. Para realizar esta alteração, você fará o seguinte:

1. Utilize o Apêndice para localizar a política em nível do recurso que define as ações que os administradores de leilão podem tomar.
2. Determine o nome do grupo de ação para a política.
3. Exclua a ação para fechar o lance de leilão a partir do grupo de ação da política.

Etapas a Serem Executadas

Identificar a Política Cujo Grupo de Ação Deve Ser Alterado

1. Procure em Leilões, no Apêndice, para identificar a política em nível do recurso a ser alterada. A política é:

   ```
   AuctionAdministratorsForOrgExecuteAuctionManageCommandsOnAuctionResource
   ```

2. No Administration Console, clique em **Gerenciamento de Acesso > Políticas**.

3. Para Exibir, selecione **Organização Raiz** para exibir as políticas em nível do site.
4. Localize a política na lista.
5. Anote o nome do grupo de ação da política— `AuctionManage`. Este é o grupo de ação que você precisa alterar para remover a ação para fechar o lance.

Remover a Ação para Fechar o Lance do Grupo de Ação da Política

1. Clique em **Gerenciamento de Acesso > Grupo de Ação**.
2. Na lista dos grupos de ação, selecione **AuctionManage** .
3. Clique em **Alterar** para exibir a página Alterar Grupo de Recursos.
4. Na lista Ações Selecionadas, selecione **com.ibm.commerce.negotiation.commands.CloseBiddingCmd**.
5. Clique em **Remover**.
6. Clique em **OK**.

Atualizar o Registro da Política com suas Alterações

1. Clique em **Configuração > Registro**.
2. Da lista de registros, selecione **Políticas de Controle de Acesso**.
3. Clique em **Atualizar**.

Cenário 2 de Leilões: Removendo a Capacidade dos Administradores de Leilão em Retirar Lances

Por padrão, os administradores de leilão para uma loja podem retirar lances submetidos para seus leilões. Em alguns casos, talvez você não queira conceder esta autoridade a ninguém. Para fazer esta alteração, você deve localizar a política em nível do recurso que define quem pode retirar lances e excluí-la.

No Cenário 1 de Leilões, a ação, fechar lance, foi uma das muitas incluídas na política. Conseqüentemente, você teve apenas que remover a ação do grupo de ação da política. Neste cenário, no entanto, uma política inteira controla a retirada do lance. No entanto, você deve excluir uma política, não apenas uma ação.

Para excluir a política, é necessário fazer o seguinte:

- Utilize o Apêndice para localizar a política em nível do recurso que abrange a retirada dos lances de leilão por administradores de leilão.
- Exclua a política.

Nota: Antes de excluir a política, anote seu nome, o nome do grupo de acesso, o nome do grupo de recursos e nome do grupo de ação para que você possa recriá-la para o próximo cenário.

Etapas a Serem Executadas

1. Procure em Leilões, no Apêndice, para identificar a política em nível do recurso a ser alterada. A política é:

   `AuctionAdministratorsForOrgExecuteAdminRetractBidCommandsOnAuctionResource`
2. No Administration Console, clique em **Gerenciamento de Acesso > Políticas**.
3. Para Exibir, selecione **Organização Raiz** para exibir as políticas em nível de site.
4. Da lista de políticas, selecione o seguinte:

   `AuctionAdministratorsForOrgExecuteAdminRetractBidCommandsOnAuctionResource`

5. Clique em **Excluir**.

Atualizar o Registro da Política com suas Alterações

1. Clique em **Configuração > Registro**.
2. Da lista de registros, selecione **Políticas de Controle de Acesso**.
3. Clique em **Atualizar**.

Cenário 3 de Leilões: Remover a Capacidade dos Administradores de Leilão em Retirar Lances em uma Organização.

Por padrão, os administradores de leilão para uma loja podem retirar lances submetidos para seus leilões. Em alguns casos, como administrador do site, talvez você queira alterar esta política para uma determinada organização. Para fazer esta alteração, você deve excluir a política modelo que autoriza esta ação para esta organização.

Nota: No WebSphere Commerce Professional Edition, existem apenas três organizações, Organização Raiz, Organização Padrão e Organização de Vendedor.

Depois de excluir a política, aquele administrador de leilão da organização não poderá mais retirar lances. Os administradores de leilão para as outras organizações não serão afetados pela alteração.

Para excluir a política, é necessário fazer o seguinte:

- Utilize o Apêndice para localizar a política em nível do recurso que autoriza a retirada de lances de leilão.
- Localize a política na lista de políticas da organização.
- Exclua a política.

Etapas a Serem Executadas

Excluir a Política

1. Procure em Leilões, no Apêndice, para identificar a política em nível do recurso a ser alterada. A política é:

   `AuctionAdministratorsForOrgExecuteAdminRetractBidCommandsOnAuctionResource`
2. No Administration Console, clique em **Gerenciamento de Acesso > Políticas**.
3. Para Exibir, selecione a organização cuja política deseja excluir. Ao selecionar uma determinada organização, diferente de `Organização Raiz`, as alterações na sua política se aplicam apenas àquela organização em vez de para todas as organizações no site.
4. Da lista de políticas, selecione o seguinte:

   `AuctionAdministratorsForOrgExecuteAdminRetractBidCommandsOnAuctionResource`
5. Clique em **Excluir**.

Atualizar o Registro da Política de Controle de Acesso com suas Alterações

1. Clique em **Configuração > Registro**.
2. Da lista de registros, selecione **Políticas de Controle de Acesso**.
3. Clique em **Atualizar**.

Cenário 4 de Leilões: Limitando o Lance do Leilão aos Compradores

Por padrão, todos os usuários registrados têm permissão para submeter um lance para os produtos que estão sendo leiloados em uma loja, independentemente de seu cargo na organização. Em alguns casos, talvez você queira limitar o lance a um grupo restrito de usuários como àqueles com a função `comprador` no WebSphere Commerce.

Neste cenário, você irá alterar uma política em nível do recurso, bem como sua política baseada em funções associada. Para limitar os lances a membros de uma organização de compras com a função `comprador`, é necessário fazer o seguinte:

- Utilize o Apêndice para localizar a política em nível do recurso que especifica quem pode criar um lance de leilão.
- Altere o grupo de acesso da política de todos os usuários registrados para aqueles com a função `comprador`.
- Renomeie a política, descrição e o nome de exibição.
- Identifique o comando para criar lances.
- Utilize o Apêndice para localizar a política baseada em funções para compradores (buy-side). Esta política define os comandos que os usuários com a função Comprador (buy-side) podem executar. Você deve atualizar este grupo de recursos da política para permitir que os compradores executem o comando para criar lances.
- Atualize o grupo de recursos da política baseada nesta função para incluir o comando para criar lances.

Etapas a Serem Executadas

Identificar a Política em Nível do Recurso

1. Procure em Leilões, no Apêndice, para identificar a política em nível do recurso a ser alterada. A política é: `RegisteredApprovedUsersExecuteBidCreateCommandsOnAuctionResource`.
2. No Administration Console, clique em **Gerenciamento de Acesso > Políticas**.
3. Para Exibir, selecione **Organização Raiz** para exibir as políticas em nível de site.
4. Na lista de políticas, selecione **RegisteredApprovedUsersExecuteBidCreateCommandsOnAuction Resource**.
5. Anote o nome do grupo de ação da política — `BidCreate`. Este é o grupo de ação que você precisa exibir para localizar o nome do comando para criar um lance.

Alterar o Grupo de Acesso da Política

1. Clique em **Alterar** para exibir a página Alterar Política.
2. Para Grupos de Usuários, clique em **Localizar** e selecione **Compradores (lado de compra)**.
3. Clique em **OK**.
4. Renomeie a política, o nome de exibição e a descrição da política, editando o texto.
5. Clique em **OK**.

Identificar o Comando para Criar Lances

1. Clique em **Gerenciamento de Acesso > Grupos de Ação**.
2. Na lista de grupos de ação, selecione **BidCreate**.

3. Clique em **Alterar** para exibir a página Alterar Grupo de Ação. Anote o nome do comando para criar lances: `com.ibm.commerce.negotiation.commands.BidSubmitCmd`. Você deve incluir este comando ao grupo de recursos que contém a lista de comandos que um comprador pode executar.

Identificar a Política Baseada em Funções e o Grupo de Recursos para os Compradores (Lado de Compra)

1. Procure Políticas Baseadas em Funções, no Apêndice, para localizar a política baseada em funções para compradores (buy-side). A política é:
   `Buyers(buy-side)ExecuteBuyers(buyside)CommandsResourceGroup`.
2. Clique em **Gerenciamento de Acesso** > **Políticas**.
3. Para Exibir, selecione **Organização Raiz** para exibir as políticas em nível de site.
4. Anote o nome do grupo de recursos: `Buyers(buy-side)CommandsResourceGroup`. Agora você tem o nome do grupo de recursos que você precisa atualizar.

Atualizar o Grupo de Recursos na Política Baseada em Funções para Incluir o Comando para Criar Lances

1. Clique em **Gerenciamento de Acesso > Grupos de Recursos**.
2. Selecione **Buyers(buy-side)CommandsResourceGroup**.
3. Clique em **Alterar** para exibir a página Alterar Grupo de Recursos.
4. Clique em **Avançar** para exibir a página Detalhes.
5. Na lista Recursos Disponíveis, selecione **com.ibm.commerce.negotiation.commands.BidSubmitCmd**. Este é o comando para criar lances.
6. Clique em **Incluir** para incluí-lo no grupo de recursos.
7. Clique em **Concluir**.

Atualizar o Registro da Política de Controle de Acesso com suas Alterações

1. Clique em **Configuração >Registro**.
2. Da lista de registros, selecione **Políticas de Controle de Acesso**.
3. Clique em **Atualizar**.

Cenário 1 de Contratos: Remover a Capacidade dos Administradores de Contratos em Incluir ou Excluir Conexões para Contratos

Por padrão, os administradores de contrato para uma loja podem incluir ou excluir conexões para os contratos que eles gerenciam. Em alguns casos, talvez você não queira conceder esta autoridade aos administradores de contratos.

Neste cenário, você irá alterar uma política em nível do recurso que define as ações que um administrador de contratos pode executar. Para remover a autoridade dos administradores de contratos em incluir ou excluir conexões para contratos, será necessário fazer o seguinte:

- Utilize o Apêndice para localizar a política em nível do recurso que define as ações que os administradores de contrato podem tomar.
- Determine o nome do grupo de ação para a política.
- Exclua as ações para incluir e excluir conexões da lista de ações no grupo de ação da política.

Etapas a Serem Executadas

Identificar a Política em Nível do Recurso e o Grupo de Ação

1. Procure em Contratos, no Apêndice, para identificar a política em nível do recurso a ser alterada. A política é:

   `ContractAdministratorsForOrgExecuteContractManageCommandsOnContractResource`
2. No Administration Console, clique em **Gerenciamento de Acesso > Políticas**.
3. Para Exibir, selecione **Organização Raiz** para exibir as políticas em nível de site.
4. Localize a política na lista.
5. Anote o nome do grupo de ação da política—`ContractManage`. Este é o grupo de ação que você precisa alterar para remover as ações para incluir e excluir conexões.

Remover as Ações para Incluir e Excluir Conexões do Grupo de Ação da Política

1. Clique em **Gerenciamento de Acesso** > **Grupo de Ação**.
2. Na lista de grupo de ação, selecione **ContractManage** .
3. Clique em **Alterar** para exibir a página Alterar Grupo de Recursos.
4. Na Lista de ações selecionadas, selecione as seguintes ações: **com.ibm.commerce.contract.commands.ContractAttachmentAddCmd com.ibm.commerce.contract.commands.ContractAttachmentDeleteCmd**.
5. Clique em **Remover**.
6. Clique em **OK**.

Atualizar o Registro da Política de Controle de Acesso com suas Alterações

1. Clique em **Configuração > Registro**.
2. Da lista de registros, selecione **Políticas de Controle de Acesso**.
3. Clique em **Atualizar**.

Cenário 2 de Contratos: Permitir que Operadores e Administradores de Contratos Implementem Contratos

Por padrão, os operadores de contratos de uma loja podem implementar contratos. Em alguns casos, talvez você queira conceder esta autoridade aos administradores de contratos também.

O design flexível das políticas de controle de acesso oferece diversos métodos de implementar esta alteração:

- Você pode criar um novo grupo de acesso que contém operadores e administradores de contratos e atribuir o novo grupo de acesso à política que define quem pode implementá-los.
- Você pode incluir a ação `implementar contrato` na política que especifica as ações que um administrador de contratos pode executar.
- Você pode criar uma nova política que permite que os administradores de contratos implemente-os.

Este cenário ilustra a terceira abordagem. Ele exibe como criar uma nova política em nível do recurso que autoriza os administradores de contratos a implementá-los.

Para criar esta política, será necessário fazer o seguinte:

- Utilize o Apêndice para localizar a política em nível do recurso que autoriza os operadores de contratos a implementá-los.
- Anote o nome do grupo de ação para esta política.
- Anote o nome do grupo de recursos para esta política.
- Defina uma nova política do grupo de acesso `administrador de contratos`, especificando o grupo de ação e o grupo de recursos da política que autoriza os operadores de contratos a implementá-los.

Etapas a Serem Executadas

Identificar o Grupo de Ação e o Grupo de Recursos a Serem Utilizados na Nova Política

1. Procure Contratos, no Apêndice, para localizar a política em nível do recurso que autoriza os operadores de contrato a implementar contratos. A política é: `ContractOperatorsForOrgExecuteContractDeployCommandsOnContractResource`.
2. No Administration Console, clique em **Gerenciamento de Acesso > Políticas**.
3. Para Exibir, selecione **Organização Raiz** para exibir as políticas em nível do site.
4. Localize a política na lista.
5. Anote o nome do grupo de ação da política—`ContractDeploy`. Este é o grupo de ação que você precisa utilizar na definição de sua nova política.
6. Anote o nome do grupo de recursos—`ContractDataResourceGroup` . Este é o grupo de recursos que você precisa utilizar na definição de sua nova política.

Definir a Nova Política

1. Clique em **Novo** para exibir a página Nova Política.
2. Para Nome, especifique:
   `ContractAdministratorsForOrgExecuteContractDeployCommandsOnContractResource`
3. Para Nome de Exibição, especifique uma descrição resumida da política em seu idioma local.
4. Para Descrição, especifique uma descrição mais longa do que a política faz em seu idioma local.
5. Para Grupo de Usuários, clique em **Localizar** e selecione **ContractAdministratorForOrg**.
6. Clique em **OK**.
7. Para Grupo de Recursos, selecione **ContractDataResourceGroup** .
8. Para Grupo de Ação, selecione **ContractDeploy** .
9. Para Tipo de Política, selecione **Política Modelo** para designar a política como uma política de modelo.
10. Clique em **OK**.

Atualizar o Registro da Política de Controle de Acesso com suas Alterações

1. Clique em **Configuração > Registro**.
2. Da lista de registros, selecione **Políticas de Controle de Acesso**.
3. Clique em **Atualizar**.

Cenário 1 de Pedidos: Permitindo que Apenas Compradores Criem Pedidos

Por padrão, todos os usuários têm permissão para criar pedidos para produtos, independentemente de sua posição na organização. Em alguns casos, talvez você queira limitar a capacidade de criar pedidos para um grupo restrito de usuários, como funcionários da organização de compras. Geralmente, é atribuído a estes funcionários a função Comprador (buy-side) para a organização de compras.

Para limitar a criação de pedidos para os membros de uma organização de compras com a função `comprador`, é necessário fazer o seguinte:

- Utilize o Apêndice para localizar a política em nível do recurso que especifica quem pode criar um pedido.
- Altere o grupo de acesso da política de todos os usuários para aqueles com a função `comprador`.
- Atualize o nome da política, o nome da exibição e a descrição.
- Identifique o comando para criar pedidos.
- Utilize o Apêndice para localizar a política baseada em funções para compradores (buy-side). Esta política define os comandos que os usuários com a função Comprador (buy-side) podem executar. Você deve atualizar este grupo de recursos da política para permitir que os compradores executem o comando para criar pedidos.
- Atualize o grupo de recursos da política baseada nesta função para incluir os comandos para criar pedidos.

Nota: Esta política em nível do recurso é uma política de modelo. Neste cenário, nós alteramos a cópia mestra deste modelo em nível de Organização Raiz. Se deseja alterá-la apenas para uma organização em particular, diferente da Organização Raiz, será necessário alterar a Exibição para outra organização antes de alterar a política. Isto resulta em uma política de modelo sendo substituída por esta única organização. Então, uma nova política padrão é criada para esta organização, que possui o grupo de acesso mais restrito dos usuários Comprador (buy-side). Já que a política de modelo menos restritiva ainda se aplica a nível da Organização Raiz, ela deve ser substituída igualmente neste nível. Atualmente, a única maneira de se fazer isso é atualizar manualmente a tabela ACORGPOL no banco de dados e executar o seguinte SQL:

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

Etapas a Serem Executadas

Identificar a Política em Nível do Recurso

1. Procure em Pedidos, no Apêndice, para identificar a política em nível do recurso a ser alterada. A política é:
   `AllUsersExecuteOrderCreateCommandsOnStoreResource .`
2. No Administration Console, clique em **Gerenciamento de Acesso > Políticas**.
3. Para Exibir, selecione **Organização Raiz** para exibir as políticas em nível do site.
4. Na lista de políticas, selecione **AllUsersExecuteOrderCreateCommandsOnStoreResource.** Anote o nome do

grupo de ação da política—OrderCreateCommands. Este é o grupo de ação que você precisa exibir para localizar os nomes dos comandos para criar um pedido.

Alterar o Grupo de Acesso

1. Clique em **Alterar** para exibir a página Alterar Política.
2. Para Grupos de Usuários, clique em **Localizar** e selecione **Compradores (lado de compra)**.
3. Clique em **OK**.
4. Atualize o nome da política, o nome da exibição e a descrição para refletir a alteração do grupo de acesso.
5. Clique em **OK**.

Identificar o Comando para Criar Pedidos

1. Clique em **Gerenciamento de Acesso > Grupos de Ação**.
2. Na lista de grupos de ação, selecione **OrderCreateCommands** .
3. Clique em **Alterar** para exibir a página Alterar Grupo de Ação. Anote os nomes dos comandos para criar pedidos:

   ```
   com.ibm.commerce.order.commands.OrderCopyCmd
   com.ibm.commerce.order.commands.OrderScheduleCmd
   com.ibm.commerce.orderitems.commands.OrderItemMoveCmd
   com.ibm.commerce.orderitems.commands.OrderItemUpdateCmd
   com.ibm.commerce.requisitionlist.commands.RequisitionListSubmitCmd
   ```

   Você deve incluir esses comandos ao grupo de recursos que contém a lista de comandos que um comprador pode executar.

   Nota: O comando, com.ibm.commerce.orderitems.commands.AdminOrderItemUpdateCmd, não é necessário.

Identificar a Política Baseada em Funções para Compradores (Lado de Compra)

1. Procure Políticas Baseadas em Funções, no Apêndice, para localizar a política baseada em funções para compradores (buy-side). A política é: Buyers(buyside)ExecuteBuyers(buyside)CommandsResourceGroup.
2. Clique em **Gerenciamento de Acesso** > **Políticas**.
3. Para Exibir, selecione **Organização Raiz** para exibir as políticas em nível do site.
4. Localize a política na lista.
5. Anote o nome do grupo de recursos—Buyers(buyside)CommandsResourceGroup. Este é o grupo de recursos que você precisa atualizar.

Atualizar o Grupo de Recursos na Política Baseada em Funções para Incluir os Comandos para Criar Pedidos

1. Clique em **Gerenciamento de Acesso > Grupos de Recursos**.
2. Na lista de grupos de recursos, selecione **Buyers(buyside)CommandsResourceGroup**.
3. Clique em **Alterar** para exibir a página Alterar Grupo de Recursos.
4. Clique em **Avançar** para exibir a página Detalhes.
5. Na lista Recursos Disponíveis, selecione os seguintes comandos para criar pedidos:

```
com.ibm.commerce.order.commands.OrderCopyCmd

com.ibm.commerce.order.commands.OrderScheduleCmd
com.ibm.commerce.orderitems.commands.OrderItemMoveCmd
com.ibm.commerce.orderitems.commands.OrderItemUpdateCmd
com.ibm.commerce.requisitionlist.commands.RequisitionListSubmitCmd
```

6. Clique em **Incluir.**
7. Clique em **Concluir**.

Atualizar o Registro da Política de Controle de Acesso com suas Alterações

1. Clique em **Configuração > Registro**.
2. Da lista de registros, selecione **Políticas de Controle de Acesso**.
3. Clique em **Atualizar**.

Cenário 2 de Pedidos: Permitindo que Apenas os Administradores de Comprador Modifiquem os Pedidos

Nota: Este cenário não se aplica ao WebSphere Commerce Professional Edition.

Por padrão, todos os usuários têm permissão para modificar pedidos que eles criaram, independentemente de sua posição na organização. Em alguns casos, talvez você queira apenas que o administrador de comprador da organização tenha autoridade para modificar pedidos.

Neste cenário, você irá alterar uma política no nível do recurso, bem como uma política baseada em funções. Para permitir apenas que os administradores de comprador modifiquem pedidos pertencentes a membros de uma organização de compradores, é necessário fazer o seguinte:

- Utilize o Apêndice para localizar a política em nível do recurso que especifica quem pode modificar um pedido.
- Altere o grupo de acesso da política de todos os usuários para aqueles com a função `administrador de comprador`.
- Remova a especificação do relacionamento do recurso para permitir que os administradores de comprador modifiquem pedidos pertencentes a outros usuários.
- Atualize o nome da política, o nome da exibição e a descrição.
- Identifique os comandos para modificar pedidos.
- Utilize o Apêndice para localizar a política baseada em funções para o administrador de comprador. Essa política define os comandos que os usuários com a função de administrador de comprador podem executar. Você deve atualizar este grupo de recursos da política para permitir que os administradores de comprador executem os comandos para modificar os pedidos.
- Atualize o grupo de recursos da política baseada em funções para incluir os comandos para modificar pedidos.

Etapas a Serem Executadas

Identificar a Política em Nível do Recurso

1. Procure Pedidos, no Apêndice, para identificar a política em nível do recurso a ser alterada. A política é: `AllUsersExecuteOrderWriteCommandsOnOrderResource`.
2. No Administration Console, clique em **Gerenciamento de Acesso > Políticas**.

3. Para Exibir, selecione **Organização Raiz** para exibir as políticas em nível do site.
4. Na lista de políticas, selecione **AllUsersExecuteOrderWriteCommandsOnOrderResource**.
5. Anote o nome do grupo de ação da política—`OrderWriteCommands`. Você precisa exibir este grupo de ação para localizar o nome do comando para criar um pedido.

Alterar o Grupo de Acesso

1. Clique em **Alterar** para exibir a página Alterar Política.
2. Para Grupo de Usuários, clique em **Localizar** e selecione **Administradores de Comprador**.
3. Clique em **OK**.
4. Atualize o nome da política, o nome da exibição e a descrição para refletir a alteração do grupo de acesso.
5. Clique em **OK**.

Identificar os Comandos para Modificar Pedidos

1. Clique em **Gerenciamento de Acesso > Grupos de Ação**.
2. Na lista de grupos de ação, selecione **OrderWriteCommands** .
3. Clique em **Alterar** para exibir a página Alterar Grupo de Ação. Anote os nomes dos comandos para modificar os pedidos:

   ```
   com.ibm.commerce.order.commands.OrderCancelCmd
   com.ibm.commerce.order.commands.OrderCopyCmd-Write
   com.ibm.commerce.order.commands.OrderUnlockCmd
   com.ibm.commerce.orderitems.commands.OrderItemAddCmd
   com.ibm.commerce.orderitems.commands.OrderItemDeleteCmd
   com.ibm.commerce.orderitems.commands.OrderItemMoveCmd
   com.ibm.commerce.orderitems.commands.OrderItemUpdate.Cmd
   ```

   Você deve incluir esses comandos ao grupo de recursos que contém a lista de comandos que um comprador pode executar.

   Notas:

   a. O comando, `com.ibm.commerce.orderitems.commands.AdminOrderItemUpdateCmd`, não é necessário.

   b. Ao incluir o comando, `com.ibm.commerce.order.commands.OrderCopyCmd-Write` no grupo de recursos, ele aparece em Recursos Disponíveis como `com.ibm.commerce.order.commands.OrderCopyCmd.`

Identificar a Política Baseada em Funções para a Função de Administrador de Comprador

1. Procure Políticas Baseadas em Funções no Apêndice para localizar a política baseada em funções para administradores de comprador. A política é: `BuyerAdministratorsExecuteBuyersAdministratorsCommands`.
2. Clique em **Gerenciamento de Acesso** > **Políticas**.
3. Para Exibir, selecione **Organização Raiz** para exibir as políticas em nível do site.
4. Localize a política na lista.
5. Anote o nome do grupo de recursos—`BuyersAdministratorsCommmandsResourceGroup`.

   Este é o nome do grupo de recursos que você precisa atualizar.

Atualizar o Grupo de Recursos na Política Baseada em Funções para Incluir os Comandos para Modificar Pedidos

1. Clique em **Gerenciamento de Acesso > Grupos de Recursos**.
2. Selecione **BuyersAdministratorsCommandsResourceGroup**.
3. Clique em **Alterar** para exibir a página Alterar Grupo de Recursos.
4. Clique em **Avançar** para exibir a página Detalhes.
5. Na lista Recursos Disponíveis, selecione os comandos para modificar pedidos:

   ```
   com.ibm.commerce.order.commands.OrderCancelCmd
   com.ibm.commerce.order.commands.OrderCopyCmd
   com.ibm.commerce.order.commands.OrderUnlockCmd
   com.ibm.commerce.orderitems.commands.OrderItemAddCmd
   com.ibm.commerce.orderitems.commands.OrderItemDeleteCmd
   com.ibm.commerce.orderitems.commands.OrderItemMoveCmd
   com.ibm.commerce.orderitems.commands.OrderItemUpdate.Cmd
   ```

6. Clique em **Incluir** para incluir o comando no grupo de recursos.
7. Clique em **Concluir**.

Atualizar o Registro da Política de Controle de Acesso com suas Alterações

1. Clique em **Configuração > Registro**.
2. Da lista de registros, selecione **Políticas de Controle de Acesso**.
3. Clique em **Atualizar**.

Cenário 3 de Pedidos: Permitindo que Aprovadores RMA Aprovem todas RMAs

Por padrão, os aprovadores de RMA (autorização para devolução de mercadorias) de uma loja só têm permissão para aprovar RMAs para suas próprias lojas. Em alguns casos, talvez você queira dar permissão aos aprovadores de RMA para aprovar RMAs para qualquer loja. Isso pode ser desejável se diversas lojas pertencerem à mesma organização ou se a mesma pessoa manipular as aprovações de RMA para diversas lojas.

Neste cenário, você criará um novo grupo de acesso e o utilizará em uma nova política em nível do recurso. Para permitir que aprovadores de RMA aprovem RMAs em qualquer loja, será necessário fazer o seguinte:

- Utilize o Apêndice para localizar a política em nível do recurso que permite que os aprovadores de RMA de uma organização aprovem RMAs para suas organizações.
- Anote o nome do grupo de recursos e do grupo de ação utilizados na política.
- Exiba o grupo de acesso da política, `RMAApproversForOrg`, e anote as funções que ele inclui. O grupo de acesso é definido utilizando as organizações e funções como critérios de seleção. Para dar aos usuários autoridade para executar uma ação através de diversas organizações, o grupo de acesso deverá ser definido sem critérios organizacionais.
- Crie um novo grupo de acesso, `RMAApprovers`, que utilize as mesmas funções, mas que não inclua os critérios organizacionais.
- Crie uma nova política utilizando:
  - O novo grupo de acesso, `RMAApprovers`
  - O grupo de ação da política existente
  - O grupo de recursos da política existente

Etapas a Serem Executadas

Identificar o Grupo de Ação e o Grupo de Recursos a Serem Utilizados na Definição da Nova Política

1. Procure Pedidos, no Apêndice, para localizar a política em nível do recurso que autoriza `RMAApproversForOrg` para aprovar RMAs para suas lojas. A política é: `RMAApproversForOrgExecuteRMAApproveCommandsOnRMAResource`
2. No Administration Console, clique em **Gerenciamento de Acesso > Políticas**.
3. Para Exibir, selecione **Organização Raiz** para exibir as políticas em nível do site.
4. Localize a política na lista.
5. Anote o nome do grupo de ação da política—`RMAApproveCommands`. Este é o grupo de ação que você utilizará na definição da nova política.
6. Anote o nome do grupo de recursos—`RMADataResourceGroup`. Este é o grupo de recursos que você utilizará na definição da sua nova política.
7. Anote o nome do grupo de acesso—`RMAApproversForOrg`. Exiba este grupo de acesso para ver as funções a serem incluídas no novo grupo de acesso.

Identificar as Funções a Serem Utilizadas no Novo Grupo de Acesso

1. Clique em **Gerenciamento de Acesso > Grupos de Acesso**.
2. Na lista de grupos de acesso, selecione **RMAApproversForOrg**.
3. Clique em **Alterar**.
4. Selecione os **Critérios** para exibir a página Critérios.
5. Em Organizações e Funções Selecionadas, anote as regras utilizadas no grupo de acesso:
   - `Supervisor do Atendimento ao Cliente`
   - `Vendedor`
   - `Gerente de Vendas`
   - `Gerente de Operações`
6. Clique em **Cancelar** para voltar para a lista dos grupos de acesso.

Definir o Novo Grupo de Acesso

1. Clique em **Novo** para exibir a página Detalhes para o novo grupo de acesso.
2. Para Nome, especifique `RMAApprovers`.
3. Para Descrição, especifique uma descrição do grupo de acesso.
4. Para Organização Pai, selecione Organização Raiz.
5. Clique em **Avançar** para exibir a página Critérios do novo grupo de acesso.
6. Clique em **Critérios baseados em organizações e funções**.
7. Na lista de funções, selecione as seguintes:
   - **Supervisor do Atendimento ao Cliente**
   - **Vendedor**
   - **Gerente de Vendas**
   - **Gerente de Operações**
8. Clique em **Concluir**.

Definir a Nova Política

1. Clique em **Gerenciamento de Acesso > Políticas**.
2. Clique em **Novo** para exibir a página Nova política.

3. Para Nome, especifique:
   `RMAApproversExecuteRMAApproveCommandsOnRMAResource`
4. Para Nome de Exibição, especifique uma descrição resumida da política em seu idioma local.
5. Para Descrição, especifique uma descrição mais longa do que a política faz em seu idioma local.
6. Para Grupo de Usuários, clique em **Localizar** e selecione **RMAApprovers**.
7. Clique em **OK**.
8. Para Grupo de Recursos, selecione **RMADataResourceGroup**.
9. Para Grupo de Ação, selecione **RMAApproveCommands**.
10. Clique em **OK**.

Atualizar o Registro da Política de Controle de Acesso com suas Alterações

1. Clique em **Configuração > Registro**.
2. Da lista de registros, selecione **Políticas de Controle de Acesso**.
3. Clique em **Atualizar**.

Cenário 1 de Associação: Remover a Capacidade dos Usuários de Auto-Registrarem

Por padrão, os usuários têm permissão para se auto-registrarem se pertencerem a uma organização registrada. Os administradores de associação também são autorizados a registrar usuários que pertencem à sua organização. Para sites que exigem acesso estritamente controlado, pode ser necessário remover a capacidade de se auto-registrar e exigir que os usuários sejam registrados pelos administradores de associação.

Nota: No WebSphere Commerce Professional Edition, existem apenas três organizações, Organização Raiz, Organização Padrão e Organização de Vendedor.

Neste cenário, você removerá a política em nível do recurso que permite que os usuários se auto-registrem, mas deixem no lugar uma política que permite que os administradores de associação registrem usuários em sua organização.

Para excluir a política em nível do recurso que permite que os usuários se auto-registrem, faça o seguinte:

- Utilize o Apêndice para localizar a política em nível do recurso que permite que os usuários se auto-registrem.
- Exclua a política.

Etapas a Serem Executadas

Excluir a Política

1. Procure Associação, no Apêndice, para localizar a política em nível do recurso que permite aos usuários se auto-registrarem. A política é: `GuestsExecuteUserSelfRegistrationCommandsOnOrganizationResource`.
2. No Administration Console, clique em **Gerenciamento de Acesso > Políticas**.
3. Para Exibir, selecione **Organização Raiz** para exibir as políticas em nível do site.

4. Na lista de políticas, selecione **GuestsExecuteUserSelfRegistrationCommandsOnOrganizationResource**
5. Clique em **Excluir**.

Atualizar o Registro da Política de Controle de Acesso com suas Alterações

1. Clique em **Configuração > Registro**.
2. Da lista de registros, selecione **Políticas de Controle de Acesso**.
3. Clique em **Atualizar**.

Cenário 2 de Associação: Permitindo que Apenas Usuários Registrados e Aprovados Alterem suas Informações de Endereço

Por padrão, os usuários podem modificar suas informações de endereço se seu registro tiver sido aprovado ou tiver aprovação pendente. Em alguns casos, talvez você queira que apenas usuários registrados e aprovados gerenciem seus endereços.

Neste cenário, você irá alterar o grupo de acesso para a política em nível do recurso que autoriza os usuários a gerenciar suas informações de endereço, como segue:

- Utilize o Apêndice para localizar a política em nível do recurso que permite aos usuários gerenciar as informações de seus endereços.
- Altere o grupo de acesso para a política.

  Uma vez que o grupo de acesso `RegisteredApprovedUsers` não contém quaisquer funções, não é necessário atualizar uma política baseada em funções para esta alteração.

Etapas a Serem Executadas

Alterar o Grupo de Acesso da Política em Nível do Recurso

1. Procure Associação, no Apêndice, para localizar a política em nível do recurso que permite que os usuários gerenciem suas informações de endereço. A política é—`NonRejectedUsersExecuteAddressManageCommandsOnUserResource`.

   Nota: Usuários não rejeitados são usuários cujo registro não foi rejeitado. Seu registro foi aprovado ou está pendente de aprovação.
2. No Administration Console, clique em **Gerenciamento de Acesso > Políticas**.
3. Para Exibir, selecione **Organização Raiz** para exibir as políticas em nível do site.
4. Na lista de políticas, selecione **NonRejectedUsersExecuteAddressManageCommandsOnUserResource.**
5. Clique em **Alterar** para exibir a página Alterar Política.
6. Para Grupo de Usuários, clique em **Localizar** e selecione **RegisteredApprovedUsers**.
7. Clique em **OK**.
8. Atualize o nome da política, o nome da exibição e a descrição para refletir a alteração do grupo de acesso.
9. Clique em **OK**.

Atualizar o Registro da Política de Controle de Acesso com suas Alterações

1. Clique em **Configuração > Registro**.
2. Da lista de registros, selecione **Políticas de Controle de Acesso**.
3. Clique em **Atualizar**.

Cenário 3 de Associação: Permitindo que os Registradores de Membros Registrem Usuários

Por padrão, os administradores de associação para uma organização são autorizados a registrar membros de sua organização. O grupo de acesso `MemberAdministratorsForOrg` inclui diversas funções como administrador de comprador e de vendedor, que são autorizados a executar uma série de tarefas administrativas. Em alguns casos, talvez você queira criar uma função separada que seja autorizada apenas para registrar membros da organização:

Aqui está uma visão geral das etapas envolvidas:

- Crie uma nova função e, para ela, um novo grupo de acesso, um novo grupo de recursos e uma nova política baseada em funções.
- Modifique uma política em nível do recurso existente para utilizar a nova função.

Neste cenário, você fará o seguinte:

- Defina uma nova função chamada `Registrador de Membro`.
- Defina um novo grupo de acesso chamado `MemberRegistrars`, que inclui a função de registrador de membros.
- Utilize o Apêndice para localizar a política em nível do recurso que permite aos administradores de associação registrarem membros.
- Anote o nome da ação no seu grupo de ação. Você deve criar um novo grupo de recursos com esta ação e utilizá-lo na política baseada em funções para a nova função. Tenha em mente que, nas políticas baseadas em funções para ações, o grupo de ação contém apenas uma única ação executar. O grupo de recursos contém as ações (comandos) que podem ser executadas.
- Defina um novo grupo de recursos, chamado `MemberRegistrationCommands`, que inclui o comando para registrar membros. Você utilizará este grupo de recursos na política baseada em funções para a função de registro de membros.
- Defina uma nova política baseada em funções para registradores de membros, que utiliza o grupo de acesso MemberRegistrars e o grupo de recursos MemberRegistrationCommands.
- Modifique a política em nível do recurso que define quem pode registrar membros e altere seu grupo de acesso de MembershipAdministrators para MemberRegistrars.

Etapas a Serem Executadas

Definir a Nova Função

1. No administration console, clique em **Gerenciamento de Acesso > Funções**.
2. Na página Funções, clique em **Nova**.
3. Para Nome, especifique Registrador de membro.
4. Para Descrição, especifique uma descrição da função de registrador de membros em seu idioma local.

5. Clique em **OK**.

Definir um Novo Grupo de Acesso Contendo a Função de Registrador de Membros

1. Clique em **Gerenciamento de Acesso > Grupos de Acesso**.
2. Na página Grupos de Acesso, clique em **Novo** para exibir a página Detalhes para o novo grupo de acesso.
3. Para Nome, especifique: MemberRegistrars.
4. Para Organização Pai, selecione Organização Raiz.
5. Para Descrição, especifique uma descrição do grupo de acesso em seu idioma local.
6. Clique em **Avançar** para exibir a página Critérios do novo grupo de acesso.
7. Clique em **Baseada em organizações e funções**.
8. Na lista Funções, selecione **Registradores de Membros**.
9. Clique em **Para Organização** para especificar que a função deve estar dentro da própria organização de usuários.
10. Clique em **Concluir**.

Identificar as Ações a Serem Utilizadas no Grupo de Recursos para a Política Baseada em Funções do Registrador de Membros

1. Procure Associação, no Apêndice, para localizar a política que permite aos administradores de associação registrarem usuários. A política é:

   ```
   MembershipAdministratorsForOrgExecuteUserAdminRegistration
   CommandsOnOrganizationResource
   ```

2. Clique em **Gerenciamento de Acesso > Políticas**.
3. Para Exibir, selecione **Organização Raiz** para exibir as políticas em nível do site.
4. Localize a política na lista.
5. Anote o nome do grupo de ação da política—`UserAdminRegistration`. Este é o grupo de ação que você precisa exibir para identificar as ações para registrar membros.
6. Clique em **Gerenciamento de Acesso > Grupos de Ação**.
7. Na lista de grupos de ação, selecione **UserAdminRegistration**.
8. Clique em **Alterar** para exibir a página Alterar Grupo de Ação.
9. Anote o nome do comando para registrar membros: `com.ibm.commerce.usermanagement.commands.UserRegistrationAdminAddCmd`.

Definir o Novo Grupo de Recursos a Ser Utilizado na Política Baseada em Funções para Registradores de Membros

1. Clique em **Gerenciamento de Acesso > Grupos de Recursos** para exibir a página Grupos de Recursos.
2. Clique em **Novo** para exibir a página Geral para o novo grupo de recursos.
3. Para Nome, especifique `UserAdminRegistrationCommands`.
4. Para Nome de Exibição, especifique uma descrição do grupo de recursos em seu idioma local.
5. Para Descrição, especifique uma descrição mais longa do grupo de recursos em seu idioma local.
6. Para Tipo, selecione **Grupo de Recursos Explícito**.
7. Clique em **Avançar**.

8. Clique em **Avançar** para exibir a página Detalhes para o novo grupo de recursos.
9. Da lista de Recursos Disponíveis, selecione o seguinte:

   com.ibm.commerce.usermanagement.commands.
   UserRegistrationAdminAddCmd
10. Clique em **Incluir**.
11. Clique em **Concluir**.

Definir uma Política Baseada em Funções para a Função de Registrador de Membros

1. Clique em **Gerenciamento de Acesso** > **Políticas**.
2. Na página Políticas, clique em **Novo**.
3. Para Nome, especifique **MemberRegistrarsExecuteUserAdminRegistrationCommands**.
4. Para Nome de Exibição, especifique uma descrição da política em seu idioma local.
5. Para Descrição, especifique uma descrição mais longa do que a política faz em seu idioma local.
6. Para Grupo de usuários, clique em **Localizar** e selecione **MemberRegistrars**.
7. Clique em **OK**.
8. Para Grupo de Recursos, selecione **UserAdminRegistrationCommands**.
9. Para Grupo de Ação, selecione **ExecuteCommandActionGroup**.
10. Clique em **OK**.

Modificar a Política em Nível do Recurso para Utilizar o Novo Grupo de Acesso

1. Da lista de políticas, selecione o seguinte:

   MembershipAdministratorsForOrgExecuteUserAdminRegistration
   CommandsOnOrganizationResource

   .
2. Clique em **Alterar** para exibir a página Alterar Política.
3. Atualize o nome da política, o nome da exibição e a descrição para refletir a alteração do grupo de acesso.
4. Para Grupo de usuários, clique em **Localizar** e selecione **MemberRegistrars**.
5. Clique em **OK**.

Atualizar o Registro da Política de Controle de Acesso com suas Alterações

1. Clique em **Configuração > Registro**.
2. Da lista de registros, selecione **Políticas de Controle de Acesso**.
3. Clique em **Atualizar**.

Cenário 1 de Cupons: Permitindo que Apenas Compradores Resgatem Cupons

Por padrão, todos os usuários registrados têm permissão para resgatar cupons. Em alguns casos, talvez você queira limitar o resgate de cupons para usuários com a função de `comprador` no WebSphere Commerce.

Neste cenário, você irá alterar uma política em nível do recurso, bem como sua política baseada em funções associada. Para limitar o resgate de cupons para usuários com a função de `comprador`, é necessário fazer o seguinte:

- Utilize o Apêndice para localizar a política em nível do recurso que especifica quem pode resgatar um cupom.
- Altere o grupo de acesso da política de todos os usuários registrados para aqueles com a função `comprador`.
- Identifique o comando para resgatar cupons.
- Utilize o Apêndice para localizar a política baseada em funções para compradores (buy-side). Essa política define os comandos que os usuários com a função buyer(buy-side) podem executar. Você deve atualizar este grupo de recursos da política para permitir que os compradores executem o comando para resgatar cupons.
- Atualize o grupo de recursos da política baseada nesta função para incluir os comandos para resgatar cupons.

Etapas a Serem Executadas

Identificar a Política em Nível do Recurso e seu Grupo de Ação

1. Procure Cupons, no Apêndice, para identificar a política em nível do recurso a ser alterada. A política é:

   `RegisteredApprovedUsersExecuteCouponRedemptionCommandsOnCouponWalletResource`
2. No Administration Console, clique em **Gerenciamento de Acesso > Políticas**.
3. Para Exibir, selecione **Organização Raiz** para exibir as políticas em nível do site.
4. Da lista de políticas, selecione o seguinte:

   `RegisteredApprovedUsersExecuteCouponRedemption CommandsOnCouponWalletResource`
5. Anote o nome do grupo de ação da política— `CouponRedemption`. Este é o grupo de ação que você deve exibir para localizar o nome dos comandos para resgatar cupons.

Alterar o Grupo de Acesso

1. Clique em **Alterar** para exibir a página Alterar Política.
2. Para Grupos de Usuários, clique em **Localizar** e selecione **Compradores (lado de compra)**.
3. Clique em **OK**.
4. Atualize o nome da política, o nome da exibição e a descrição para refletir a alteração do grupo de acesso.
5. Clique em **OK**.

Identificar os Comandos para Resgatar Cupons

1. Clique em **Gerenciamento de Acesso > Grupos de Ação**.
2. Na lista de grupos de ação, selecione **CouponRedemption**.
3. Clique em **Alterar** para exibir a página Alterar Grupo de Ação. Anote o nome dos comandos para criar lances:

   ```
   com.ibm.commerce.couponredemption.commands.CouponDSSCmd
     com.ibm.commerce.couponredemption.commands.UseCouponIdCmd
   ```

   Você deve incluir esses comandos ao grupo de recursos que contém a lista de comandos que um comprador pode executar.

Identificar a Política Baseada em Funções para Compradores (Lado de Compra)

1. Procure Políticas Baseadas em Funções, no Apêndice, para localizar a política baseada em funções para compradores (buy-side). A política é:

   `Buyers(buy-side)ExecuteBuyers(buyside)CommandsResourceGroup`
2. Clique em **Gerenciamento de Acesso** > **Políticas**.
3. Para Exibir, selecione **Organização Raiz** para exibir as políticas em nível de site.
4. Localize a política na lista.
5. Anote o nome do grupo de recursos: `Buyers(buyside)CommandsResourceGroup`. Este é o nome do grupo de recursos que você precisa atualizar.

Atualizar o Grupo de Recursos na Política Baseada em Funções para Incluir o Comando para Criar Lances

1. Clique em **Gerenciamento de Acesso > Grupos de Recursos**.
2. Selecione **Buyers(buy-side)CommandsResourceGroup**.
3. Clique em **Alterar** para exibir a página Alterar Grupo de Recursos.
4. Clique em **Avançar** para exibir a página Detalhes.
5. Na lista Recursos Disponíveis, selecione **com.ibm.commerce.couponredemption.commands.CouponDSSCmd com.ibm.commerce.couponredemption.commands.UseCouponIdCmd**. Esses são os comandos para resgatar cupons.
6. Clique em **Incluir** para incluir os comandos no grupo de recursos.
7. Clique em **Concluir**.

Atualizar o Registro da Política de Controle de Acesso com suas Alterações

1. Clique em **Configuração > Registro**.
2. Da lista de registros, selecione **Políticas de Controle de Acesso**.
3. Clique em **Atualizar**.

Cenário 2 de Cupons: Permitindo que Administradores de Cupons e Administradores de Loja Criem Promoções com Cupom Eletrônico

Por padrão, os administradores de cupom de uma loja podem criar promoções com cupons eletrônicos para sua loja. Em alguns casos, talvez você queira conceder esta autoridade também aos administradores de loja.

O design flexível das políticas de controle de acesso oferece diversos métodos de implementar esta alteração:

- Você pode incluir a função de administrador de loja ao grupo de acesso para a política que especifica quem pode criar promoções com cupons eletrônicos.
- Você pode criar uma nova política que permite aos administradores de loja criarem promoções com cupons eletrônicos.

Este cenário ilustra a primeira abordagem. Ele mostra como incluir a função de administrador da loja na política em nível do recurso que autoriza os administradores de cupom a criá-los.

Para efetuar esta alteração, é necessário fazer o seguinte:

- Utilize o Apêndice para localizar a política em nível do recurso que especifica quem pode criar promoções com cupons eletrônicos.

- Altere o grupo de acesso da política para incluir usuários na função de `administrador de loja`.
- Exiba o grupo de ação da política em nível do recurso para identificar o comando para criar promoções com cupons eletrônicos.
- Utilize o Apêndice para localizar a política baseada em funções para `administradores de loja`. Essa política define os comandos que os usuários com a função de `administrador de loja` podem executar. Você deve atualizar este grupo de recursos da política para permitir que os administradores de loja executem os comandos para criar promoções com cupons eletrônicos.
- Atualize o grupo de recursos da política baseada nesta função para incluir o comando para criar promoções com cupons eletrônicos.

Etapas a Serem Executadas

Identificar o Grupo de Ação e o Grupo de Acesso para a Política em Nível do Recurso

1. Procure Leilões, no Apêndice, para identificar a política em nível do recurso a ser alterada. A política é:

   `CouponAdministratorsForOrgExecuteCouponPromotionCreateCommands OnStoreEntityResource`
2. No Administration Console, clique em **Gerenciamento de Acesso > Políticas**.
3. Para Exibir, selecione **Organização Raiz** para exibir as políticas em nível do site.
4. Localize a política na lista.
5. Anote o nome do grupo de ação da política—`CouponPromotionCreate`. Este é o grupo de ação que você deve exibir para localizar o nome do comando para criar promoções com cupons eletrônicos.
6. Anote o nome do grupo de acesso da política—`CouponAdministratorsForOrg`. Este é o grupo de acesso que você deve atualizar para incluir a função do administrador de loja.

Alterar o Grupo de Acesso

1. Clique em **Gerenciamento de Acesso > Grupos de Acesso**.
2. Na lista de grupos de acesso, selecione **CouponAdministratorsForOrg**
3. Clique em **Alterar** para exibir a página Detalhes.
4. Clique em **Critérios** para exibir a página Critérios.
5. Na lista Funções, selecione **Administrador de Loja**.
6. Clique em **Para Organização** para especificar que a função deve estar dentro da própria organização de usuários.
7. Clique em **Incluir** .
8. Clique em **OK**.

Identificar os Comandos para Criar Promoções com Cupons Eletrônicos

1. Clique em **Gerenciamento de Acesso > Grupos de Ação**.
2. Na lista de grupos de ação, selecione **CouponPromotionCreate**.
3. Clique em **Alterar** para exibir a página Alterar Grupo de Ação. Anote o nome do comando para criar promoções com cupons eletrônicos — `com.ibm.commerce.tools.ecoupon.ECouponPromotionSaveCmd`. Você deve incluir este comando no grupo de recursos que contém a lista de comandos que um administrador de loja pode executar.

Identificar a Política Baseada em Funções para Administradores de Loja

1. Procure Políticas Baseadas em Funções no Apêndice para localizar a política baseada em funções para administradores de loja. A política é: `StoreAdministratorsExecuteStoreAdministratorsCmdResourceGroup.`
2. Clique em **Gerenciamento de Acesso** > **Políticas**.
3. Para Exibir, selecione **Organização Raiz** para exibir as políticas em nível do site.
4. Localize a política na lista.
5. Anote o nome do seu grupo de recursos — `StoreAdministratorsCmdResourceGroup`. Este é o nome do grupo de recursos que você precisa atualizar.

Atualizar o Grupo de Recursos na Política Baseada em Funções para Incluir o Comando para Criar as Promoções com Cupons Eletrônicos

1. Clique em **Gerenciamento de Acesso > Grupos de Recursos**.
2. Selecione **StoreAdministratorsCmdResourceGroup**.
3. Clique em **Alterar** para exibir a página Alterar Grupo de Recursos.
4. Clique em **Avançar** para exibir a página Detalhes.
5. Na lista Recursos Disponíveis, selecione `com.ibm.commerce.tools.ecoupon.ECouponPromotionSaveCmd`. Este é o comando para criar promoções com cupons eletrônicos.
6. Clique em **Incluir**.
7. Clique em **Concluir**.

Atualizar o Registro da Política de Controle de Acesso com suas Alterações

1. Clique em **Configuração > Registro**.
2. Da lista de registros, selecione **Políticas de Controle de Acesso**.
3. Clique em **Atualizar**.

Cenário 1 de Procurement: Permitindo que os Gerentes de Carrinho de Compras Gerenciem o Carrinho de Compras do Procurement para Pedidos Criados por sua Organização

Nota: Este cenário não se aplica ao WebSphere Commerce Professional Edition.

Por padrão, os gerentes de carrinhos de compras de procurement são autorizados a gerenciar o carrinho de compras de procurement quando eles criaram o pedido. Em alguns casos, talvez você possa querer ampliar a autoridade dos gerentes de carrinhos de compras de procurement para permitir que eles gerenciem o carrinho de procurement para pedidos criados por qualquer membro de sua organização.

Para efetuar esta alteração, é necessário fazer o seguinte:

- Utilize o Apêndice para localizar a política em nível do recurso que autoriza administradores de carrinhos de compras de procurement a gerenciá-los.
- Altere o relacionamento de recursos para esta política de `criador` para `mesma entidade organizacional como criador`.

Etapas a Serem Executadas

Alterar o Relacionamento de Recursos para Política em Nível do Recurso

1. Procure Procurement, no Apêndice, para localizar a política em nível do recurso que autoriza os gerentes de carrinhos de compras de procurement a gerenciá-los para pedidos. A política é:

   ```
   ProcurementShoppingCartManagersExecuteProcurementShopping
   CartManageOnOrderResource
   ```

2. No Administration Console, clique em **Gerenciamento de Acesso > Políticas**.
3. Para Exibir, selecione **Organização Raiz** para exibir as políticas em nível de site.
4. Da lista de políticas, selecione o seguinte:

   ProcurementShoppingCartManagersExecuteProcurementShopping CartManageOnOrderResource

5. Clique em **Alterar** para exibir a página Alterar Política.
6. Para Relacionamento, selecione **sameOrganizationalEntityAsCreator**.
7. Clique em **OK**.

Atualizar o Registro da Política de Controle de Acesso com suas Alterações

1. Clique em **Configuração > Registro**.
2. Da lista de registros, selecione **Políticas de Controle de Acesso**.
3. Clique em **Atualizar**.

Cenário 2 de Procurement: Permitir Administradores de Compradores de Procurement a Submeter o Carrinho de Compras de Procurement para Pedidos Criados por sua Organização

Nota: Este cenário não se aplica ao WebSphere Commerce Professional Edition.

Por padrão, os gerentes de carrinhos de compras de procurement podem salvar ou submeter os carrinhos de compras de procurement se eles criaram o pedido. Em alguns casos, talvez você queira dividir a responsabilidade para essas tarefas. Você pode permitir que os gerentes de carrinhos de compras de procurement salvem esses carrinhos contendo pedidos que eles criaram, porém dar aos administradores de compradores de procurement na mesma organização que o criador do pedido autoridade para submeter o carrinho de compras de procurement. Isso pode ser benéfico se você quiser que o administrador de compras de procurement reveja as compras planejadas antes de elas serem submetidas.

Para efetuar esta alteração, é necessário fazer o seguinte:

- Utilize o Apêndice para localizar a política em nível do recurso que autoriza os gerentes de carrinhos de compras de procurement a centralizar os gerentes para gerenciar os centros de distribuição.
- Remova a ação para submeter um carrinho de compras de procurement do grupo de ação da política.
- Defina um novo grupo de ação contendo o comando para submeter um carrinho de compras de procurement. Você utilizará este grupo de ação para definir a nova política em nível do recurso que autoriza os administradores de compradores de procurement a submeter carrinhos de compras de procurement se estiverem na mesma organização que o criador do pedido.

- Crie uma nova política em nível do recurso que autoriza os administradores de compradores de procurement a submeter carrinhos de compras de procurement se eles estiverem na mesma organização que o criador do pedido.

Etapas a Serem Executadas

Identificar o Grupo de Recursos e o Grupo de Ação da Política em Nível do Recurso

1. Procure Procurement, no Apêndice, para localizar a política em nível do recurso que autoriza os gerentes de carrinhos de compras de procurement a gerenciá-los para pedidos. A política é:

   `ProcurementShoppingCartManagersExecuteProcurement ShoppingCartManageOnOrderResource`
2. No Administration Console, clique em **Gerenciamento de Acesso > Políticas**.
3. Localize a política na lista de políticas.
4. Anote o nome do seu grupo de ação — `ProcurementShoppingCartManage`. É necessário atualizar este grupo de ação para remover a ação para submeter carrinhos de compras de procurement.
5. Anote o nome do seu grupo de recursos — `OrderDataResourceGroup`. Você utilizará este grupo de recursos para definir a nova política em nível do recurso.

Atualizar o Grupo de Ação da Política em Nível do Recurso

1. Clique em **Gerenciamento de Acesso > Grupos de Ação**.
2. Na lista de grupos de ação, selecione **ProcurementShoppingCartManage**.
3. Clique em **Alterar** para exibir a página Alterar Grupo de Ação.
4. Na lista Ações Selecionadas, selecione **com.ibm.commerce.me.commands.SubmitShoppingCartCmd**. Você criará um novo grupo de ação com esta ação e utilizará o grupo de ação em sua nova política em nível do recurso.
5. Clique em **Remover**.
6. Clique em **OK**.

Definir um Novo Grupo de Ação

1. Clique em **Gerenciamento de Acesso > Grupos de Ação**.
2. Clique em **Novo** para exibir a página Novo Grupo de Ação.
3. Para Nome, especifique `ProcurementShoppingCartSubmit`.
4. Para Nome de exibição, especifique uma descrição resumida do grupo de ação em seu idioma local.
5. Para Descrição, especifique uma descrição mais longa do que o grupo de ação faz em seu idioma local.
6. Na lista Ações Disponíveis, selecione **com.ibm.commerce.me.commands.SubmitShoppingCartCmd**.
7. Clique em **Incluir** .
8. Clique em **OK**.

Definir a Nova Política

1. Clique em **Gerenciamento de Acesso > Políticas**.
2. Para Exibir, clique em **Organização Raiz** para exibir as políticas em nível do site.
3. Clique em **Novo** para exibir a página Nova Política.

4. Para Nome, especifique:

   `ProcurementBuyerAdministratorsExecuteProcurementShoppingCartSubmitCommands OnOrderResource`
5. Para Nome da Exibição, especifique uma descrição resumida da política em seu idioma local.
6. Para Descrição, especifique uma descrição mais longa do que a política faz em seu idioma local.
7. Para Grupo de Usuários, clique **Localizar** e selecione **ProcurementBuyerAdministrators**.
8. Clique em **OK**.
9. Para Grupo de Recursos, selecione **OrderDataResourceGroup**.
10. Para Grupo de Ação, selecione **ProcurementShoppingCartSubmit**.
11. Para Relacionamento, selecione **sameOrganizationalEntityAsCreator**.
12. Para Tipo de Política, selecione **Política Modelo** para designar a política como uma política de modelo.
13. Clique em **OK**.

Atualizar o Registro da Política de Controle de Acesso com suas Alterações

1. Clique em **Configuração > Registro**.
2. Da lista de registros, selecione **Políticas de Controle de Acesso**.
3. Clique em **Atualizar**.

Cenário 1 de Estoque: Permitir que os Gerentes do Centro de Distribuição Atualizem os Centros de Distribuição, Mas Não os Exclua

Por padrão, os gerentes do centro de distribuição têm permissão para atualizar ou excluir os centros de distribuição associados à sua loja. Em alguns casos, talvez você queira permitir que os gerentes do centro de distribuição atualizem os centros de distribuição, mas não os exclua.

Para efetuar esta alteração, é necessário fazer o seguinte:

- Utilize o Apêndice para localizar a política em nível do recurso que autoriza os gerentes do centro de distribuição a gerenciá-los.
- Remova a ação para excluir um centro de distribuição do grupo de ação da política.

Etapas a Serem Executadas

Remover a Ação para Excluir um Centro de Distribuição

1. Procure Procurement, no Apêndice, para localizar a política em nível do recurso que autoriza os gerentes de carrinhos de compras de procurement a gerenciá-los para pedidos. A política é:

   `FulfillmentCenterManagersForOrgExecuteFulfillmentCenter ManageCommandsOnFulfillmentResource`
2. No Administration Console, clique em **Gerenciamento de Acesso > Políticas**.
3. Localize a política na lista de políticas.
4. Anote o nome de seu grupo de ação—`FulfillmentCenterManage`. É necessário atualizar este grupo de ação para remover a ação para excluir os centros de distribuição.
5. Clique em **Gerenciamento de Acesso > Grupos de Ação.**

6. Na lista de grupos de ação, selecione **FulfillmentCenterManage**.
7. Clique em **Alterar** para exibir a página Alterar Grupo de Ação.
8. Na lista Ações Selecionadas, selecione **com.ibm.commerce.inventory.commands.FulfillmentCenterDeleteCmd**.
9. Clique em **Remover**.
10. Clique em **OK**.

Atualizar o Registro da Política de Controle de Acesso com suas Alterações

1. Clique em **Configuração > Registro**.
2. Da lista de registros, selecione **Políticas de Controle de Acesso**.
3. Clique em **Atualizar**.

Cenário 2 de Estoque: Permitir Apenas que os Gerentes de Logística e de Operações Criem, Atualizem ou Excluam Centros de Distribuição

Por padrão, os gerentes do centro de distribuição têm autorização para criar, atualizar ou excluir os centros de distribuição associados a sua loja. O grupo de acesso do centro de distribuição inclui as funções: vendedor, gerente de logística e gerente de operações. Em alguns casos, talvez você não queira que os vendedores tenham autorização como os gerentes do centro de distribuição.

Para efetuar esta alteração, é necessário fazer o seguinte:

- Utilize o Apêndice para localizar a política em nível do recurso que autoriza os gerentes do centro de distribuição a gerenciá-los.
- Remova a função de vendedores da definição do grupo de acesso `gerentes do centro de distribuição`.

Etapas a Serem Executadas

Remover a Função de Vendedor do Grupo de Acesso

1. Procure Procurement, no Apêndice, para localizar a política em nível do recurso que autoriza os gerentes de carrinhos de compras de procurement a gerenciá-los para pedidos. A política é:

   ```
   FulfillmentCenterManagersForOrgExecuteFulfillmentCenterManage
   CommandsOnFulfillmentResource
   ```

2. No Administration Console, clique em **Gerenciamento de Acesso > Grupos de Acesso**.
3. Na lista de grupos de acesso, selecione **FulfillmentCenterManagersForOrg**.
4. Clique em **Alterar** para exibir a página Alterar Grupo de Acesso.
5. Clique em **Gerenciamento de Acesso > Grupos de Acesso**.
6. Clique em **Alterar** para exibir a página Detalhes.
7. Clique em **Critérios** para exibir a página Critérios.
8. Na lista Funções, selecione **Vendedor**.
9. Clique em **Remover**.
10. Clique em **OK**.

Atualizar o Registro da Política de Controle de Acesso com suas Alterações

1. Clique em **Configuração > Registro**.
2. Da lista de registros, selecione **Políticas de Controle de Acesso**.

3. Clique em **Atualizar**.

Cenário 1 Inteligência de Negócios: Permitindo que Auditores Exibam os Relatórios de Inteligência de Negócios

Por padrão, os visualizadores de relatório de inteligência têm permissão para exibir relatórios de inteligência de negócios para sua loja. Em alguns casos, talvez você possa criar uma nova função chamada `auditor` e autorizar usuários com esta função para exibir relatórios de inteligência de negócios de uma loja.

Aqui está uma visão geral das etapas envolvidas:

- Crie uma nova função e, para ela, um novo grupo de acesso, um novo grupo de recursos e uma nova política baseada em funções.
- Inclua uma nova função no grupo de acesso da política em nível do recurso.
- Defina uma nova função chamada `Auditor`.
- Defina um novo grupo de acesso, chamado `Auditores`, que inclui a função do auditor.
- Inclua a função do auditor ao grupo de acesso da política em nível do recurso que define quem pode exibir relatórios de inteligência de negócios em suas lojas.

Neste cenário, você fará o seguinte:

- Utilize o Apêndice para localizar a política em nível do recurso que permita que os visualizadores do relatório de inteligência de negócios exibam os relatórios de inteligência de negócios.
- Anote o nome da ação no seu grupo de ação. Você deve criar um novo grupo de recursos com esta ação e utilizá-lo na política baseada em funções para a nova função. Tenha em mente que, nas políticas baseadas em funções para ações, o grupo de ação contém apenas uma única ação executar. O grupo de recursos contém as ações (comandos) que podem ser executadas.
- Defina o novo grupo de recursos, chamado `AuditorCommands`, que inclui o comando para exibir os relatórios de inteligência de negócios. Você utilizará este grupo de recursos na política baseada em funções para a função de auditor.
- Defina uma nova política baseada em funções para auditores, que utiliza o grupo de acesso Auditores e o grupo de recursos AuditorCommands.
- Inclua a função de auditor no grupo de acesso para a política em nível do recurso que define quem pode exibir os relatórios de inteligência de negócios em sua loja.

Etapas a Serem Executadas

Definir a Nova Função de Auditor

1. No administration console, clique em **Gerenciamento de Acesso > Funções**.
2. Na página Funções, clique em **Nova**.
3. Para nome, especifique Auditor.
4. Para Descrição, especifique uma descrição da função de auditor em seu idioma local.
5. Clique em **OK**.

Definir um Novo Grupo de Acesso para a Função de Auditor

1. Clique em **Gerenciamento de Acesso > Grupos de Acesso**.

2. Na página Grupos de Acesso, clique em **Novo** para exibir a página Detalhes para o novo grupo de acesso.
3. Para Nome, especifique—Auditores.
4. Para Descrição, especifique uma descrição do grupo de acesso em seu idioma local.
5. Para Organização Pai, selecione Organização Raiz.
6. Clique em **Avançar** para exibir a página Critérios do novo grupo de acesso.
7. Clique em **Baseada em organizações e funções**.
8. Na lista Funções, selecione **Auditor**.
9. Clique em **Incluir** .
10. Clique em **Concluir**.

Identificar as Ações a Serem Utilizadas no Grupo de Recursos para a Política Baseada em Funções da Função de Auditor

1. Procure Inteligência de Negócios, no Apêndice, para localizar a política que autoriza os visualizadores de relatório de inteligência a exibir os relatórios de inteligência de negócios. A política é:

   ```
   IntelligenceReportViewersForOrgExecuteViewBusinessIntelligenceReport
   CommandsOnStoreEntityResource
   ```

2. No Administration Console, clique em **Gerenciamento de Acesso > Políticas**.
3. Para Exibir, selecione **Organização Raiz** para exibir as políticas em nível do site.
4. Localize a política na lista.
5. Anote o nome do grupo de ações da política—`ViewBusinessIntelligenceReport`. Este é o grupo de ação que você deve exibir para identificar as ações para registrar membros.
6. Clique em **Gerenciamento de Acesso > Grupos de Ação**.
7. Na lista de grupos de ação, selecione **ViewBusinessIntelligenceReport**.
8. Clique em **Alterar** para exibir a página Alterar Grupo de Ação.
9. Anote o nome do comando para exibir relatórios de inteligência de negócios—`com.ibm.commerce.bi.commands.BIShowReportCmd`.

Definir o Novo Grupo de Recursos a Ser Utilizado na Política Baseada em Funções para a Função de Auditor

1. Clique em **Gerenciamento de Acesso > Grupos de Recursos** para exibir a página Grupos de Recursos.
2. Clique em **Novo** para exibir a página Geral para o novo grupo de recursos.
3. Para Nome, especifique AuditorCommands.
4. Para Nome de Exibição, especifique uma descrição do grupo de recursos em seu idioma local.
5. Para Descrição, especifique uma descrição mais longa do grupo de recursos em seu idioma local.
6. Clique em **Avançar**.
7. Para Tipo, selecione **Grupo de Recursos Explícito**.
8. Clique em **Avançar** para exibir a página Detalhes para o novo grupo de recursos.
9. Na lista Recursos Disponíveis, selecione **com.ibm.commerce.bi.commands.BIShowReportCmd**.
10. Clique em **Incluir** .

11. Clique em **Concluir**.

Definir a Política Baseada em Funções para a Função do Auditor

1. Clique em **Gerenciamento de Acesso > Políticas**.
2. Na página Políticas, clique em **Novo**.
3. Para Nome, especifique **AuditorsExecuteAuditorCommands**.
4. Para Nome de Exibição, especifique uma descrição da política em seu idioma local.
5. Para Descrição, especifique uma descrição mais longa do que a política faz em seu idioma local.
6. Para Grupos de Usuário, clique em **Localizar** e selecione **Auditores**.
7. Clique em **OK**.
8. Para Grupo de Recursos, selecione **AuditorCommands**.
9. Para Grupo de Ação, selecione **ExecuteCommandActionGroup**.
10. Clique em **OK**.

Incluir a Função de Auditor no Grupo de Acesso da Política em Nível de Recursos

1. Clique em **Gerenciamento de Acesso > Grupos de Acesso.**
2. Na lista dos grupos de acesso, selecione **IntelligenceReportViewersForOrg**.
3. Clique em **Alterar** para exibir a página Alterar Grupo de Acesso.
4. Clique em **Critérios** para exibir a página Critérios do grupo de acesso.
5. Na lista Funções, selecione **Auditor**.
6. Clique em **Para Organização** para especificar que a função deve estar dentro da própria organização de usuários.
7. Clique em **Incluir** .
8. Clique em **OK**.

Atualizar o Registro da Política com suas Alterações

1. Clique em **Configuração > Registro**.
2. Da lista de registros, selecione **Políticas de Controle de Acesso**.
3. **Clique em Atualizar.**

Capítulo 6. Utilizando XML para Personalizar as Políticas de Controle de Acesso

O WebSphere Commerce Administration Console permite fazer alterações simples nas políticas de controle de acesso e suas partes. Para fazer alterações mais sofisticadas, você precisa editar arquivos XML diretamente.

Antes de começar a fazer as alterações nos arquivos XML para o controle de acesso, leia o capítulo sobre o controle de acesso em *IBM WebSphere Commerce Programmer's Guide*. Este capítulo fornece uma visão geral técnica do controle de acesso e explica como criar comandos personalizados, beans de entidade e modelos JSP (JavaServer Pages) que podem ser protegidos pelas políticas de controle de acesso.

Assim que terminar as personalizações de código seguindo as orientações fornecidas no *IBM WebSphere Commerce Programmer's Guide*, você poderá editar os arquivos XML para controle de acesso a fim de estabelecer proteções necessárias.

Alterações que Apenas Podem ser Feitas Editando e Carregando Arquivos XML

As seguintes alterações podem ser feitas apenas ao editar e, em seguida, carregar os arquivos XML apropriados:

- Protegendo um novo comando ou exibição
- Criar ou modificar um relacionamento
- Criar ou modificar um grupo de relacionamentos
- Protegendo um novo recurso
- Criar ou modificar atributos
- Criando ou modificando grupos de acesso utilizando critérios complexos
- Criar ou modificar grupos de recursos utilizando critérios complexos

Sobre os Arquivos XML para Controle de Acesso

Os nomes e as descrições dos arquivos XML, arquivos DTD e arquivos XSL do WebSphere Commerce, para o XML Transformer, são exibidos na tabela a seguir.

Tabela 4. Arquivos XML do WebSphere Commerce para controle de acesso

Nome do arquivo	Descrição
ACUserGroups_de_DE.xmll ACUserGroups_en_US.xml ACUserGroups_es_ES.xml ACUserGroups_fr_FR.xml ACUserGroups_it_IT.xml ACUserGroups_ja_JP.xml ACUserGroups_ko_KR.xml ACUserGroups_pt_BR.xml ACUserGroups_zh_CN.xml ACUserGroups_zh_TW.xml	As definições e descrições do grupo de acesso em cada idioma suportado.
defaultAccessControlPolicies.xml	Arquivo principal contendo as definições das políticas de controle de acesso padrão, grupos de ação, grupos de recursos, relacionamentos, grupos de relacionamentos, ações, categorias de recursos e atributos.
defaultAccessControlPolicies_de_DE.xml defaultAccessControlPolicies_en_US.xml defaultAccessControlPolicies_es_ES.xml defaultAccessControlPolicies_fr_FR.xml defaultAccessControlPolicies_it_IT.xml defaultAccessControlPolicies_ja_JP.xml defaultAccessControlPolicies_ko_KR.xml defaultAccessControlPolicies_pt_BR.xml defaultAccessControlPolicies_zh_CN.xml defaultAccessControlPolicies_zh_TW.xml	Arquivos contendo os nomes de exibição e as descrições para as políticas de controle de acesso padrão, grupos de ação, ações, grupos de recursos, categorias de recursos, relacionamentos e atributos em cada idioma suportado.
ACPoliciesfilter.xml	Arquivo de filtro utilizado na extração de informações de controle de acesso alterado a partir dos bancos de dados.
accesscontrolpolicies.dtd	O arquivo XML das políticas de controle de acesso deve se ajustar a este DTD.
accesscontrolpoliciesnls.dtd	O arquivo XML NLS (national language specific) das políticas de controle de acesso deve se ajustar a este DTD.
ACUserGroups_en_US.dtd	O arquivo XML de grupos de usuários do controle de acesso deve se ajustar a este DTD.

Tabela 4. Arquivos XML do WebSphere Commerce para controle de acesso (continuação)

accesscontrol.xsl	O arquivo de regra de transformação XSL para o arquivo XML das políticas de controle de acesso.
accesscontrolnls.xsl	O arquivo de regra de transformação XSL para o arquivo XML NLS das políticas de controle de acesso (exibe apenas nomes e descrições).
ACUserGroup.xsl	O arquivo de regra de transformação do XSL para os arquivos XML do grupo de acesso.
wcstoacpolicies.xsl	O arquivo de regra de transformação XSL para o arquivo ExtractedACPolicies.xml após extração, para criar o arquivo XML das políticas de controle de acesso.
wcstoacpoliciesnls.xsl	O arquivo de regra de transformação XSL para o ExtractedACPolicies.xml após extração, para criar o arquivo XML NLS das políticas de controle de acesso.
wcstoacusergroup.xsl	O arquivo de regra de transformação XSL para arquivo ExtractedACPolicies.xml após extração, para criar o arquivo XML de grupo de acesso.

Personalizando os Arquivos XML

Protegendo as Exibições

Qualquer exibição chamada diretamente de uma URL ou lançada como um redirecionamento de outro comando precisa de uma política de controle de acesso baseada em função a fim de ser exibida. O exemplo a seguir mostra uma política baseada em função para exibições:

```
<Policy Name="ProductManagersExecuteProductManagersViews"
OwnerID="RootOrganization"
UserGroup="ProductMangers"
ActionGroupName="ProductMangersViews"
ResourceGroupName="ViewCommandResourceGroup">
</Policy>
```

O nome do ResourceGroupe, ViewCommandResourceGroup, indica que isso é uma política baseada em função para exibições. A política indica que usuários no grupo de usuários ProductManagers, podem mostrar as exibições no grupo de ação ProductMangersViews.

A seguir, um exemplo do grupo de ação ProductMangersViews:

```
<ActionGroup Name="ProductManagersViews"
OwnerID="RootOrganization">

<ActionGroupAction Name="ProductImageView"/>
```

```
<ActionGroupAction Name="ProductManufacturerView"/>
<ActionGroupAction Name="ProductSalesTaxView"/>

 </ActionGoup>
```

O exemplo acima lista três ações, `ProductImageView`, `ProductManufacturerView` e `ProductSalesTaxView` que podem ser executadas no grupo de ação `ProductManagerViews`.

A seguir, um exemplo da definição de ação `ProductImageView`:

```
<Action Name="ProductImageView"
CommandName="ProductImageView">
</Action>
```

O atributo `Name`, `ProductImageView`,é utilizado como uma tag para mencionar a ação em qualquer parte no XML como ao associar a ação a um grupo de ação.

Nota: O nome da exibição, armazenado na coluna VIEWNAME da tabela VIEWREG, deve corresponder a `CommandName` na definição da ação. O valor de `CommandName` é armazenado na coluna ACTION da tabela ACACTION. Os atributos `Name` e `CommandName` não devem ser iguais.

Incluindo uma nova Exibição Utilizando as Políticas já Existentes

Para incluir uma nova exibição acessível por funções nas políticas de Exibição baseada em funções existentes, faça o seguinte:

1. Crie uma nova definição de ação no arquivo XML que tem o nome de exibição MyNewView.

   ```
   <Action Name="MyNewView"
   CommandName="MyNewView">
   </Action>
   ```

2. Determine quais funções devem ter acesso a esta exibição e associe a nova ação com os grupos de ação correspondentes no arquivo XML:

   ```
   <ActionGroup Name="ProductManagersViews"
   OwnerID="RootOrganization">

   <ActionGroupAction Name="ProductImageView"/>
   <ActionGroupAction Name="ProductManufacturerView"/>
   <ActionGroupAction Name="ProductSalesTaxView"/>
   <ActionGroupAction Name="MyNewView"/>

   </ActionGroup>
   ```

3. Carregue suas alterações de XML no banco de dados. Para obter mais informações sobre como carregar as alterações de XML, consulte “Carregando suas Alterações no Banco de Dados” na página 102.
4. Atualize o Registro de Políticas de Controle de Acesso no Administration Console.

Uma vez que já existe uma política baseada na função que inclui este grupo de ação, a exibição agora pode ser utilizada.

Incluindo uma Nova Exibição Utilizando uma Nova Política

Para incluir uma nova exibição acessível por uma nova função que não tenha uma política baseada em função existente, faça o seguinte:

1. Crie uma nova definição de ação no arquivo XML que tem o nome de exibição MyNewView.

```
<Action Name="MyNewView
CommandName="MyNewView">
</Action>
```

2. Crie um novo grupo de ação a ser associado com a nova função:

```
<ActionGroupName="XYZViews"
OwnerID="RootOrganization">
</ActionGroup>
```

3. Associe a nova ação com o novo grupo de ações:

```
<ActionGroupName="XYZViews"
OwnerID="RootOrganization">

<ActionGroupAction Name="MyNewView"/>

</ActionGroup>
```

4. Crie uma política que menciona o novo grupo de ação:

```
<Policy Name="XYZExecuteXYZViews"
OwnerID="RootOrganization"
UserGroup="XYZ"
ActionGroupName="XYZViews"
ResourceGroupName="ViewCommandResourceGroup">
</Policy>
```

5. Carregue suas alterações de XML no banco de dados. Para obter mais informações sobre como carregar as alterações de XML, consulte "Carregando suas Alterações no Banco de Dados" na página 102.
6. Atualize o Registro de Políticas de Controle de Acesso no Administration Console.

Agora você pode utilizar sua exibição.

Protegendo os Comandos do Controlador

Todos os comandos do controlador exigem uma política de controle de acesso baseada em função para serem executados. Um comando do controlador ou da tarefa também requer uma política em nível do recurso se o comando estiver fazendo uma verificação no nível do recurso. Para obter mais informações, consulte "Implementando o Controle de Acesso do Nível do Recurso" na página 83. O exemplo a seguir exibe uma política baseada em função para comandos do controlador:

```
<Policy Name="SellersExecuteSellersCmdResourceGroup"
OwnerID="RootOrganization"
UserGroup="Sellers"
ActionGroupName="ExecuteCommandActionGroup"
ResourceGroupName="SellersCmdResourceGroup">
</Policy>
```

O ActionGroupName, `ExecuteCommandActionGroup`, indica que esta é uma política baseada em função para comandos do controlador. A política indica que usuários no grupo de acesso `Sellers` pode executar os comandos no grupo de recursos `SellersCmdResourceGroup`.

A seguir, um exemplo da definição do grupo de recursos `SellersCmdResourceGroup`:

-
```
<ResourceGroup Name="SellersCmdResourceGroup"
OwnerID="RootOrganization">
<ResourceGroupResource Name="com.ibm.contract.commands.Contract
CancelCmdResourceCategory"/>
<ResourceGroupResource Name="com.ibm.contract.commands.Contract
```

```
CloseCmdResourceCategory"/>
<ResourceGroupResource Name="com.ibm.contract.commands.Contract
CreateCmdResourceCategory"/>
</ResourceGroup>
```

O exemplo acima mostra os três recursos a seguir no grupo de recursos, que cada um corresponde a um comando do controlador:

- com.ibm.contract.commands.ContractCancelCmdResourceCategory
- com.ibm.contract.commands.ContractCloseCmdResourceCategory
- com.ibm.contract.commands.ContractCreateCmdResourceCategory

A seguir, uma definição de exemplo de um recurso:

```
<ResourceCategory Name="com.ibm.commerce.contract.commands.Contract
CloseCmdResourceCategory"
ResourceBeanClass="com.ibm.commerce.contract.commands.ContractCloseCmd">

<ResourceAction Name="ExecuteCommand"/>

</ResourceCategory>
```

O atributo Name, com.ibm.commerce.contract.commands.ContractCloseCmdResourceCategory, é utilizado como uma tag para mencionar o recurso no arquivo XML. O Nome ResourceAction ExecuteCommand é utilizado para especificar as ações que podem operar nos recursos. Essas informações são utilizadas no Administration Console ao utilizar as políticas de controle de acesso para preencher a caixa de seleção Ação que corresponde a um determinado recurso. Nesse caso, a ação Execute é especificada. A ação Execute é definida em:

```
<Action Name="ExcecuteCommand
CommandName="Execute">
</Action>
```

Nota: O nome da interface do comando do controlador deve corresponder ao ResourceBeanClass na definição de recursos. O valor de ResourceBeanClass é armazenado na coluna RESCLASSNAME da tabela ACRESCGRY. Esses comandos podem ser utilizados como recursos porque eles ampliam a interface ControllerCommand, que amplia a interface AccCommand que, por sua vez, amplia a interface Protectable. Para obter mais informações sobre estas interfaces, consulte o *IBM WebSphere Commerce Programmer's Guide*.

Incluindo um Novo Comando do Controlador Utilizando as Políticas Existentes

Para incluir um novo comando do controlador para ser acessível por funções que têm políticas de comandos do controlador baseadas em funções existentes, faça o seguinte:

1. Crie uma nova definição de recurso no arquivo XML que corresponde ao nome da interface do comando do controlador.

   ```
   <ResourceCategory  Name="com.xyz.commands.MyNewControllerCmdResourceCategory"
   ResourceBeanClass="com.xyz.commands.MyNewControllerCmd">
   <ResourceAction Name="ExecuteCommand"/>
   </ResourceCategory>
   ```

2. Determine quais funções devem ter acesso ao comando e associe o novo recurso aos grupos de recurso correspondentes no arquivo XML:

   ```
    <ResourceGroup Name="SellersCmdResourceGroup"
   OwnerID="RootOrganization">
   <ResourceGroupResource Name="com.ibm.commerce.contract.
   commands.ContractCancelCmdResourceCategory"/>
   ```

```
<ResourceGroupResource Name="com.ibm.commerce.contract.
commands.ContractCloseCmdResourceCategory"/>
<ResourceGroupResource Name="com.ibm.commerce.contract.
commands.ContractCreateCmdResourceCategory"/>

<ResourceGroupResource Name="com.xyz.commands.
MyNewControllerCmdResourceCategory"/>

</ResourceGroup>
```

3. Carregue suas alterações de XML no banco de dados. Para obter mais informações sobre como carregar as alterações de XML, consulte "Carregando suas Alterações no Banco de Dados" na página 102.
4. Atualize o Registro de Políticas de Controle de Acesso no Administration Console.

Uma vez que já existe uma política baseada em função que inclui este grupo de recursos, agora você pode utilizar seu novo comando do controlador, se não estiver fazendo nenhuma verificação no nível do recurso.

Incluindo um Novo Comando do Controlador Utilizando uma Nova Política

Para incluir um novo comando do controlador a ser acessado por uma nova função, que não tenha uma política baseada em função já existente, proceda da seguinte forma:

1. Crie uma nova definição de recurso no arquivo XML que corresponde ao nome da interface do comando do controlador. Consulte "Incluindo um Novo Comando do Controlador Utilizando as Políticas Existentes" na página 82 etapa um, para um exemplo.
2. Crie um novo grupo de recursos a ser associado com a nova função:
   ```
   <ResourceGroup Name="XYZCmdResourceGroup" OwnerID="RootOrganization">
   </ResourceGroup>
   ```
3. Associe o novo recurso ao novo grupo de recursos:
   ```
   <ResourceGroup Name="XYZCmdResourceGroup" OwnerID="RootOrganization">
   <ResourceGroupResource Name="com.xyz.commands.MyNewControllerResourceCategory"/>
   </ResourceGroup>
   ```
4. Crie uma política que menciona seu novo grupo de recursos:
   ```
   <Policy Name="XYZExecuteXYZsCmdResourceGroup"
   OwnerID="RootOrganization"
   UserGroup="XYZ"
   ActionGroupName="ExecuteCommandActionGroup"
   ResourceGroupName="XYZCmdResourceGroup">
   </Policy>
   ```
5. Carregue suas alterações de XML no banco de dados. Para obter mais informações sobre como carregar as alterações de XML, consulte "Carregando suas Alterações no Banco de Dados" na página 102.
6. Atualize o Registro de Políticas de Controle de Acesso no Administration Console.

Agora você pode utilizar seu comando do controlador se não estiver fazendo nenhuma verificação no nível do recurso.

Implementando o Controle de Acesso do Nível do Recurso

Você pode incluir o controle de acesso do nível de recurso para o controlador ou comandos de tarefas. A verificação em nível de recursos é feita no WebSphere Commerce em tempo de execução, com base nos dados retornados pelo método `getResources()` de um comando. A verificação no nível do recurso também pode

ser feita durante a parte do comando performExcecute(), fazendo chamadas diretas ao gerenciador de política de controle de acesso utilizando o método void checkIsAllowed(Object resource, String action) throws ECException. Este método enviará o ECApplicationException se o usuário atual não tiver permissão para executar a ação especificada no recurso especificado.

Nota: Por padrão, o método getResources() retorna nulo, e não será feita nenhuma verificação do nível do recurso.

Você precisa criar uma política em nível do recurso para novos comandos nas seguintes instâncias:

- O novo comando se estende de outro comando que está fazendo uma verificação do nível do recurso.
- O próprio comando faz a verificação do controle de acesso em nível do recurso.

A seguir, um exemplo de uma política em nível de recurso:

```
<Policy
Name="ContractMangersForOrgExecuteContractManageCommandsOnContractResource"
OwnerID="RootOrganization"
UserGroup="ContractManagersForOrg"
ActionGroupName="ContractManage"
ResourceGroupName="ContractDataResourceGroup"
PolicyType="template">
</Policy>
```

Em que:

Name: O nome da política.

PolicyType: O tipo da política. É uma política de modelo e será aplicada dinamicamente na entidade organizacional que possui o recurso e seus ascendentes.

OwnerID: O membro que possui a política. É uma política de exemplo e será alterada dinamicamente para ser a entidade organizacional que possui o recurso e seus ascendentes, uma vez que a política é aplicada pelo Gerenciador de política de controle de acesso.

UserGroup: A política se aplica aos usuários deste grupo. A convenção de nomenclatura de grupos de acesso onde as funções são colocadas em escopo dinamicamente para a entidade organizacional do recurso e seus ascendentes devem anexar ForOrg ao nome do grupo.

ActionGroupName: O nome do grupo de ação que contém as ações a serem executadas no recurso.

ResourceGroupName: O nome do grupo de recursos que contém os recursos no qual agir.

No exemplo acima, o grupo de ação ContractManage contém um conjunto de comandos que agirá no ContractDataResourceGroup. A seguir, um exemplo do grupo de ação que é utilizado na política em nível do recurso acima:

```
<ActionGroupName="ContractManage" OwnerID="RootOrganization">
<ActionGroupActionName="com.ibm.commerce.contract.commands.ContractCancelCmd"/>
<ActionGroupActionName="com.ibm.commerce.contract.commands.ContractCloseCmd"/>
<ActionGroupActionName="com.ibm.commerce.contract.commands.ContractDeleteCmd"/>
</ActionGroup>
```

Os comandos que foram definidos anteriormente como recursos para as políticas baseadas em funções agora são definidos como ações. A seguir, uma amostra de definição de uma ação que faz parte do grupo ContractManage acima.

```
<Action Name="com.ibm.commerce.contract.commands.ContractCloseCmd"
CommandName="com.ibm.commerce.contract.commands.ContractCloseCmd">
</Action>
```

Nota: O valor de CommandName deve corresponder ao nome do comando da interface que está fazendo a verificação do nível do recurso.

A maioria dos comandos funcionam com os beans corporativos. Estes beans geralmente são os recursos que as políticas em nível do recurso estão protegendo. A seguir, um exemplo de uma definição de amostra do grupo de recursos que é utilizado na política de recurso acima:

```
<ResourceGroup Name="ContractDataResourceGroup" OwnerId="RootOrganization">
<ResourceGroupResource Name="com.ibm.commerce.contract.
objects.ContractResourceCategory"/>
</ResourceGroup>
```

Neste exemplo, ContractDataResourceGroup é definido e é composto de um recurso. O recurso é definido da seguinte forma:

```
<ResourceCategory Name="com.ibm.commerce.contract.objects.ContractResourceCategory"
ResourceBeanClass="com.ibm.commerce.contract.objects.Contract"
<ResourceAction Name="com.ibm.commerce.contract.commands.ContractCancelCmd"/>
<ResourceAction Name="com.ibm.commerce.contract.commands.ContractCloseCmd"/>
<ResourceAction Name="com.ibm.commerce.contract.commands.ContractDeleteCmd"/>
 </ResourceCategory>
```

Em que:

Name: Uma tag utilizada para mencionar este recurso em qualquer lugar no arquivo XML.

ResourceBeanClass: A classe que representa o recurso a ser protegido. Esta classe deve implementar a interface Protectable. Se o recurso for um bean corporativo, é a interface remota que deve ampliar a interface Protectable.

ResourceAction: Especifica as ações que estarão operando neste recurso. Estas informações são utilizadas pelo Administration Console ao determinar quais ações são válidas com um recurso particular.

Nota: Para obter mais informações sobre a interface Protectable, consulte o *WebSphere Commerce Programmer's Guide*.

Protegendo os Beans de Dados

Os beans de dados contém informações sobre objetos de negócios e são utilizados para exibir informações sobre o objeto em uma página da web. As páginas da web dinâmicas geralmente são mapeadas para exibições dentro do WebSphere Commerce, e estas exibições são protegidas pelas políticas baseadas em funções. Algumas vezes é necessário para proteger o conteúdo da página da web protegendo seus beans de dados, se existirem.

Quando os beans de dados são preenchidos utilizando o método DataBeanManager.activate(..) , os gerenciadores do bean de dados reforçam o controle de acesso neles. Os beans de dados podem ser protegidos direta ou indiretamente, utilizando a interface Delegator. Os beans de dados protegidos diretamente também implementam a interface Protectable. Se um bean de dados

protegido indiretamente não implementa a interface Delegator ou retorna um valor nulo para o método getDelegate(), ele não é protegido e pode ser exibido por qualquer pessoa.

Nota: Para obter mais informações sobre a interface protectable, consulte o *WebSphere Commerce Programmer's Guide*

A seguir, um exemplo de uma política em nível do recurso para um bean de dados:

```
<Policy Name="AllUsersDisplayOrderDataBeanResourceGroup"
OwnerID="RootOrganization"
UserGroup="AllUsers"
ActionGroupName="DisplayDataBeanActionGroup"
ResourceGroupName="OrderDataBeanResourceGroup"
RelationName="creator">
```

O ActionGroupName, DisplayDataBeanActionGroup, indica que esta política é para beans de dados. Este grupo de ação inclui uma ação Display.

Em que:

Name: O nome desta política.

UserGroup: O grupo de acesso que contém os usuários a quem a política se aplica. Nesse caso, inclui todos os usuários.

ActionGroupName: O valor DisplayDataBeanActionGroup indica que é uma política em nível do recurso para beans de dados.

ResourceGroupName:O nome do grupo de recursos que contém os beans de dados a serem protegidos.

RelationName: O relacionamento que deve ser atendido entre um usuário e o recurso. Nesse caso, o usuário deve ser o criador do recurso de negócio Order.

O OrderDataBeanResourceGroup é definido da seguinte forma:

```
<ResourceGroup Name="OrderDataBeanResourceGroup" OwnerID="RootOrganization">
<ResourceGroupResource Name="com.ibm.commerce.order.beans.
OrderListDataBeanResourceCategory"/>
<ResourceGroupResource Name="com.ibm.commerce.order.beans
.OrderDataBeanResourceCategory"/>
</ResourceGroup>
```

O OrderDataBeanResourceGroup consiste em dois recursos. A seguir, um exemplo de definição de recurso para um Bean de Dados:

```
<ResourceCategory Name="com.ibm.commerce.order.beans.OrderDataBeanResourceCategory"
ResourceBeanClass="com.ibm.commerce.order.beans.OrderDataBean">
<ResourceAction Name="DisplayDataBean"/>
</ResourceCategory>
```

Em que:

Name: Uma tag utilizada para mencionar este recurso no arquivo XML.

ResourceBeanClass: O nome da classe do bean de dados que está sendo protegido diretamente. Esta classe deve implementar a interface Protectable.

`ResourceAction`: Um elemento necessário para a edição da política no Administration Console. Nesse caso, este elemento indica que `Display` é uma ação válida a ser executada neste recurso.

Agrupando Recursos por Atributos

Os grupos de recursos podem ser definidos completamente, utilizando a coluna CONDITIONS na tabela ACRESGRP. A coluna CONDITIONS armazena o documento XML que contém as limitações e os pares de valores de atributos utilizados para os recursos de agrupamento. Este tipo de grupo de recursos é chamado de grupo de recurso implícito e, geralmente, é utilizado quando o nome da classe do recurso não é suficiente. Por exemplo, se uma política de controle de acesso se aplica aos recursos `Order` que possuem um status igual a `P` (pendente) ou `E` (editando por um representante de serviço ao cliente), um grupo de recursos pode ser definido para isso.

Nota: Para agrupar recursos por atributos que não sejam o nome da classe, o recurso deve implementar a interface Groupable. Para obter mais informações sobre a interface Groupable, consulte o *IBM WebSphere Commerce Programmer's Guide*.

A seguir, um exemplo do grupo de recursos `Order`:

```
<ResourceGroup  Name="OrderResourceGroupwithPEStatus"
OwnerID="RootOrganization">
<ResourceCondition>
 <![CDATA[
  <profile>
   <andListCondition>
<orListCondition>
      <simpleCondition>
       <variable name="Status"/>
       <operator name="="/>
       <value data="P"/>
      </simpleCondition>
      <simpleCondition>
       <variable name="Status"/>
       <operator name="="/>
       <value data="E"/>
      </simpleCondition>
 </orListCondition>
      <simpleCondition>
       <variable name="classname"/>
       <operator name="="/>
       <value data="com.ibm.commerce.order.objects.Order"/>
      </simpleCondition>
    </andListCondition>
   </profile>
 ]]>
</ResourceCondition>
</ResourceGroup>
```

Em que:

`Name`: O nome do grupo de recursos armazenado na coluna GRPNAME da tabela ACRESGRP.

`OwnerID`: O proprietário do grupo de recursos. Esta deve ser a organização raiz.

`<ResourceCondition>`: Especifica os dados que serão carregados na coluna CONDITIONS da tabela ACRESGRP, para definir o grupo de recurso.

<![CDATA[...]]>: Significa uma seção de dados de caractere que são utilizados exatamente como são digitados .

<profile>: Um parâmetro obrigatório para todas as condições do recurso.

Um componente essencial da definição do grupo de recurso é o elemento <simpleCondition> que possui name="classname". Este elemento identifica a classe java do recurso ao qual o grupo se aplica. A classe java, com.ibm.commerce.order.objects.Order, pode ser vista no seguinte exemplo:

```
<simpleCondition>
   <variable name="classname"/>
   <operator name="="/>
   <value data="com.ibm.commerce.order.objects.Order"/>
   </simpleCondition>
```

O exemplo a seguir especifica a condição no recurso com.ibm.commerce.objects.order.objects.Order, que o status deve ser igual a P.

```
<simpleCondition>
<variable name="Status"/>
       <operator name="="/>
       <value data="P"/>
   </simpleCondition>
```

No exemplo acima, <variable name="*value*"/> representa os nomes do atributo reconhecidos pelo método getGroupingAttributeValue (String attributeName, GroupContext context)() no recurso. Este método faz parte da interface Groupable. Para obter os objetivos do gerenciamento do Grupo de Recursos Implícitos dentro do Administration Console do WebSphere Commerce, o atributo também deve ser definido na tabela ACATTR e ser associado ao recurso na tabela ACRESATREL. Quando é momento de localizar as políticas aplicáveis para um determinado recurso e ação, esta condição será marcada chamando o método getGroupingAttributeValue(..) , que neste caso passa para Status conforme o parâmetro attributeName.

O <orListCondition>, especifica que as condições dentro deste bloco devem ser aplicadas utilizando um booleano OR. Neste caso, o status é P ou E. O <andListConditon>, especifica que as condições dentro deste bloco devem ser aplicadas utilizando um booleano AND. Neste caso, (Classname = com.ibm.commerce.order.objects.Order) AND (Status = P OR Status=E).

Um exemplo de definição do atributo para preencher a tabela ACATTR é mostrado a seguir:

```
<Attribute Name="Status" Type="String">
</Attribute>
```

O elemento Name é um termo para identificar o atributo e o elemento Type identifica o tipo de dados do atributo. Os valores possíveis do atributo são:

- String
- Integer
- Double
- Currency
- Decimal
- URL
- Image
- Date

A associação de um atributo em um recurso é especificado dentro da definição do Recurso. Por exemplo, o atributo `Status` é associado à `OrderResourceCategory` no exemplo a seguir:

```
<ResourceCategory Name="com.ibm.commerce.order.objects.OrderResourceCategory"
ResourceBeanClass="com.ibm.commerce.order.objects.Order" >

<ResourceAttributes Name="Status"
AttributeTableName="ORDERS"
AttributeColumnName="STATUS"
ResourceKeyColumnName="ORDERS_ID"/>
</ResourceCategory>
```

Em que:

`<ResourceAttributes>`: Um bloco de código que associa um atributo a um recurso.

`AttributeTableName`: O nome da tabela do banco de dados do recurso.

`AttributeColumnName`: O nome da coluna na tabela do recurso que armazena o atributo.

`ResourceKeyColumnName`: O nome da coluna na tabela do recurso que armazena a chave principal.

Definindo Relacionamentos

As políticas de controle de acesso possuem um elemento de relacionamento opcional. Este relacionamento pode ser criado apenas ao carregar um arquivo de política XML com a definição de relacionamento vista abaixo:

```
<Relation Name="value">
 </Relation>
```

A entrada `Name` é o nome do relacionamento utilizado em qualquer política e é incluído na tabela ACRELATION. `Name` corresponde ao parâmetro de relacionamento do método `fulfills()` no recurso protectable.

O seguinte exemplo exibe a definição de um relacionamento chamado `creator`.

```
<Relation Name="creator">
</Relation>
```

Definindo Grupos de Relacionamentos

Os grupos de relacionamentos contêm condições abertas que são as condições para pertencer ao grupo de relacionamento. Se você precisa definir grupos de relacionamentos, será necessário fazê-lo através da definição das informações do grupo de relacionamentos em seu arquivo XML ou através da modificação do arquivo `defaultAccessControlPolicies.xml`, conforme visto abaixo:

```
<RelationGroup
Name="aValue"
OwnerID="aValue">
<RelationCondition><![CDATA[
<profile>
Relationship Chain Open Condition XML
</profile>
]]></RelationCondition>
</RelationGroup>
```

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 ao examinar o número de entradas `<parmeter 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>
```

Em que:

`<parameter name="Relationshiop" value="something">`: Uma cadeia representando o relacionamento entre o usuário e o recurso.

`name` : O parâmetro de relacionamento do método `fulfills()` no recurso protectable.

Quando uma cadeia de relacionamento tem um comprimento de dois ou mais, ela é uma série de dois relacionamentos. A primeira entrada, `<parmeter name= "X" value="Y">`, está entre um usuário e uma entidade organizacional. A última entrada `<parmeter name= "X" value="Y">` está entre uma entidade organizacional e o recurso. As entradas intermediárias `<parmeter name= "X" value="Y">` na cadeia estão entre organizações. 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>
```

Em que:

`aValue1` : Os possíveis valores 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 reproduz uma 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` for `ROLE`, os 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.

`Value3`: 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 for retornada mais de uma entidade organizacional pelo parâmetro de avaliação `aValue1`, esta parte do RELATIONSHIP_CHAIN será satisfatória se pelo menos uma dessas entidades organizacionais satisfizerem o relacionamento especificado pelo parâmetro `aValue2`.

Nota: Para obter mais informações sobre a definição de grupos de relacionamentos, consulte “Definindo Grupos de Relacionamentos” na página 89

Definindo Grupos de Relacionamentos em Cadeia Única

Se como parte de sua política de controle de acesso, você for solicitado a reforçar que um usuário deve pertencer à entidade organizacional que é, por exemplo, BuyingOrganizationalEntity do recurso, será necessário criar um grupo de relacionamento que seja composto de uma cadeia de relacionamento com um comprimento de dois. Isso é mostrado no exemplo a seguir:

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

A cadeia de relacionamento possui um comprimento de dois porque consiste em dois relacionamentos separados. O primeiro relacionamento está entre o usuário e sua entidade organizacional pai. O usuário é o filho neste 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 retorna true se for a entidade organizacional de compra do recurso.

Nota: Para obter mais informações sobre a tag openCondition, consulte o *WebSphere Commerce Accelerator Customization Guide*.

Outro exemplo seria reforçar que o usuário possui a função de Representante de Contas da entidade organizacional que é a entidade organizacional de compra do recurso. Novamente, isso utiliza um grupo de relacionamento 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 o 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. Se isso ocorrer, será retornado o valor true.

O exemplo a seguir mostra como definir este 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>
```

Definindo Grupos de Relacionamentos em Várias Cadeias

Se você precisar compor um grupo de relacionamento que contenha um relacionamento em várias cadeias, será necessário especificar se o usuário deve satisfazer todas as cadeias de relacionamentos, significando que é um cenário AND, ou o usuário deve satisfazer pelo menos uma das cadeias de relacionamentos, o que significa que é um cenário OR.

No exemplo a seguir, o usuário deve ser o criador do recurso e deve pertencer ao BuyingOrganizationalEntity especificado no recurso. A primeira cadeia que

especifica que o usuário deve ser o criador do recurso tem o comprimento de um. A segunda cadeia, que especifica que o usuário deve pertencer ao BuyingOrganizationalEntity especificado no recurso, tem um comprimento de dois.

```
<RelationshipGroup 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>
```

Nota: Se você solicitar que o usuário satisfaça qualquer uma das duas cadeias de relacionamentos, a tag <andListConditon> deve ser alterada para a tag <orListConditon>.

Grupos de Acesso

Os grupos de acesso padrão que fazem parte do WebSphere Commerce são encontrados em arquivos XML específicos para linguagem, como *wc_install_directory*/xml/policies/xml/ACUserGroups_locale.xml. Este arquivo segue o DTD especificado pelo *wc_install_directory*/xml/policies/dtd/ACUserGroups_en_US.dtd.

A seguir, o formato de um elemento do grupo de acesso:

```
<UserGroup Name="value"
OwnerID="value"
Description="value"
<UserCondition>
<![CDATA[
<profile>
Condition XML
</profile>
]]>
</UserCondition>
</UserGroup>
```

Em que:

Name: O nome do grupo de acesso, armazenado na coluna MBRGRPNAME da tabela MBRGRP.

OwnerID: O ID do Membro que possui este grupo de acesso. A combinação Name e OwnerID deve ser exclusiva. Os valores especiais que podem ser utilizados incluem: RootOrganization (-2001) ou DefaultOrganization (-2000).

Description (opcional): Um atributo opcional utilizado para descrever o grupo de acesso.

UserCondition (opcional): Um elemento opcional especificando as condições implícitas da associação neste grupo de acesso. Este critério é armazenado na coluna CONDITIONS da tabela MBRGRPCOND.

`Condition XML`: Utilizando a estrutura da condição, qualquer condição válida dos elementos `orListCondition`, `andListCondition`, `simpleCondition` e `trueConditionCondition`.

Os seguintes nomes de SimpleCondition são suportados para o elemento `UserCondition`:

Tabela 5. Nomes suportados da condição simples

Nome da Variável	Descrição	Operadores Suportados	Valores Suportados	Qualificadores	Valores do Qualificador
`função`	Especifica que o usuário deve ter esta função na tabela MBRROLE·.	= !=	Qualquer valor da coluna NAME na tabela ROLE.	`org` (se não for especificado, o usuário deve ter a função para qualquer organização na tabela MBRROLE.	• `OrgEntityID` : Onde o usuário deve ter a função. • `?`: Quando é utilizado em uma política de modelo.
`registrostatus`	Especifica que o usuário deve ter este status de registro.	= !=	Qualquer valor da coluna REGISTER-TYPE na tabela USERS, como `G` para convidado e `R` para registrado.	none	n/a
`status`	Especifica que o usuário deve ter este estado do membro. Geralmente é utilizado para o status de aprovação do registro.	= !=	Qualquer valor da coluna STATE na tabela MEMBER, como `0` para aprovação de registro pendente, `1` para registro aprovado e `2` para registro rejeitado.	none	n/a
`org`	Especifica que o usuário deve ser registrado nesta organização pai. É armazenado na tabela MBRREL.	= !=	• Qualquer valor de ORGENTITY_ID na tabela ORGENTITY. • `?`- se for uma política de modelo.	none	n/a

Nota: O ? será dinamicamente alterado para a entidade organizacional pertencente ao recurso e subseqüentemente fica ascendente quando a política de modelo for aplicada no tempo de execução. Os grupos de acesso definidos com ? funcionam apenas com as políticas de modelo.

Exemplos de simpleConditions para Grupos de Acesso

Função:

Função sem um Qualificador: O exemplo a seguir exibe uma `função` simpleCondition sem um qualificador; mais comumente utilizado nas políticas baseadas em funções. Neste exemplo o usuário deve ter uma função de Administração de Vendedor para qualquer entidade organizacional.

```
<UserConditon>
<![CDATA[
<profile>
<simpleCondition>
<variable name="role"/>
<operator name="="/>
<value data="Seller Administrator"/>
</simpleCondition>
</profile>
]]>
</UserCondition>
```

Função com um Qualificador: O exemplo a seguir exibe uma `função` simpleCondition com um qualificador; mais comumente utilizado nas políticas em nível de organização. Neste exemplo, o usuário deve ter uma função Vendedor para a entidade organizacional `100`.

```
<UserCondition>
<!CDATA[
<profile>
<simpleCondition>
<variable name="role"/>
<operator name="="/>
<value data="Seller"/>
<qualifier name="org" data="100"/>
<simpleCondition>
</profile>
]]>
</UserCondition>
```

Função com um Qualificador e um Parâmetro: O exemplo a seguir exibe uma `função` simpleCondition com um qualificador e um parâmetro. Funciona apenas em políticas de modelo. Neste exemplo, o usuário deve ter uma função Gerente de Vendas, Gerente de Contas ou Vendedor na entidade organizacional que possui o recurso especificado na política de modelo.

```
<UserCondition><!CDATA[
<profile>
<orListCondition>
<simpleCondition>
<variable name="role"/>
<operator name="="/>
<value data="Sales Manager"/>
<qualifier name="org" data="?"/>
</simpleCondition>
<simpleCondition>
<variable name="role"/>
<operator name="="/>
<value data="Account Representative"/>
<qualifier name="org" data="?"/>
</simpleCondition>
<simpleCondition>
<variable name="role"/>
<operator name="="/>
<value data="Seller"/>
<qualifier name="org" data="?"/>
```

```
</simpleCondition>
</orListCondition>
</profile/>
]]></UserCondition>
```

RegistrationStatus: O exemplo a seguir exibe uma simpleCondition registrationStatus. Neste exemplo, o usuário deve ser registrado (USERS.REGISTERTYPE = R).

```
<UserCondition><!CDATA[
<profile>
<simpleCondition>
<variable name="registrationStatus"/>
<operator name="="/>
<value data="R"/>
</simpleCondition>
</profile>
]]></UserCondition>
```

Status: O exemplo a seguir exibe uma simpleCondition status. Neste exemplo, o usuário deve ter tido o registro aprovado. (MEMBER.STATUS = 1)

```
<UserCondition><![CDATA[
<profile>
<simpleCondition>
<variable name="status"/>
<operator name="="/>
<value data="1"/>
</simpleCondition>
</profile>
]]></UserCondition>
```

Org: O exemplo a seguir exibe uma simpleCondition org. Neste exemplo, o usuário deve ser registrado na entidade organizacional 100. Na tabela MBRREL, o usuário deve ter o valores de ANCESTOR_ID = 100, e SEQUENCE = 1.

```
<UserCondition><![CDATA[
<profile>
<simpleCondition>
<variable name="org"/>
<operator name="="/>
<value data="100"/>
</simpleCondition>
</profile>
]]>
</UserCondition>
```

Políticas

O arquivo *wc_install_directory*/xml/policies/xml/defaultAccessControlPolicies.xmldefine as políticas de controle de acesso padrão que são enviadas fora da caixa. Ele segue o DTD especificado por: *wc_install_directory*/xml/policies/dtd/accesscontrolpolicies.dtd.

A seguir, o modelo de um elemento de política:

```
<Policy Name="value"
OwnerId="value"
UserGroup="value"
UserGroupOwner="value"
ActionGroupName="value"
ResourceGroupName="value"
PolicyType="value"
```

```
RelationName="value"
RelationGroupName="value"
RelationGroupOwner="value"
</Policy>
```

Em que:

`Name`: O nome da política. É carregado na coluna POLICYNAME da tabela ACPOLICY. O `Name` e o `OwnerID` juntos devem ser exclusivos.

`OwnerID`: O ID do membro da entidade organizacional que possui a política. Este será carregado na coluna `member_id` da tabela ACPOLICY. O `OwnerID` e o `Name` juntos devem ser exclusivos. Há dois valores especiais que são reconhecidos pela ferramenta de transformador, são `RootOrganization: -2001` e `DefaultOrganization: -2000`

`UserGroup`: O nome do grupo de acesso especificado na coluna MBRGRPNAME da tabela MBRGRP. Este é carregado na coluna `mbrgrp_id` da tabela ACPOLICY. Os grupos de acesso padrão são definidos no arquivo `wc_install_directory/xml/policies/xml/ACUserGroups_language.xml`.

`UserGroupOwner`: O ID do membro que possui o Grupo de Acesso. Isso é necessário quando o grupo de acesso pertence a um membro que não seja o proprietário da política. Se isso não for especificado, é assumido que o grupo de acesso pertence ao membro que é especificado pelo atributo `OwnerID`.

`ActionGroupName`: O nome do grupo de ação especificado na coluna GROUPNAME da tabela ACACTGRP. É utilizado para obter o ID do grupo de ação correspondente (ACACTGRP_ID) que será armazenado na tabela ACPOLICY. As políticas baseadas em funções para comandos do controlador têm o `ActionGroupName` definido como `ExecuteCommandActionGroup`. As políticas para os beans de dados têm o `ActionGroupName` definido como `DisplayDatabeanActionGroup`.

`ResourceGroupName`: O nome do Grupo de Recursos, especificado na coluna GRPNAME da tabela ACRESGRP. É utilizado para obter o ID do grupo de recursos correspondente (ACRESGRP_ID) que será armazenado na tabela ACPOLICY. As políticas baseadas em funções para exibições têm o `ResoureGroupName` definido como `ViewCommandResourceGroup`.

`PolicyType`: O tipo da política. Os valores válidos são `template` (POLICYTYPE será definido como 1 na tabela ACPOLICY). Se este atributo não for especificado, o valor do tipo da política permanecerá inalterado. (Por padrão, o valor desta coluna é nulo. Qualquer valor diferente de 1 implica em um tipo de política não-modelo). Para obter mais informações sobre os tipos de políticas, consulte Capítulo 3, “Conceitos de Controle de Acesso” na página 9.

`RelationName (opcional)`: O nome do Relacionamento, conforme especificado na coluna RELATIONNAME da tabela ACRELATION. Se for especificado, será utilizado para obter o ID do relacionamento correspondente (ACRELATION_ID) que será armazenado na tabela ACPOLICY.

`RelationGroupName (opcional)`: O nome do Grupo de Relacionamentos, conforme especificado na coluna GRPNAME da tabela ACRELGRP. Se este atributo for especificado, o `RelationName` não deve ser especificado, já que o Grupo de Relacionamentos tem precedência.

RelationGroupOwner: O ID do membro que possui o Grupo de Relação. Este atributo é necessário apenas se o atributo RelationGroupName for especificado e se o valor do atributo OwnerID não for RootOrganization; neste caso, RelationGroupOwner deverá ser especificado como RootOrganization (-2001).

Exemplos da Política

Políticas Baseadas em Funções:

Para Comandos do Controlador: Neste exemplo, os usuários pertencentes ao grupo de acesso AllUsers podem executar os comandos do controlador que fazem parte do grupo de recursos AllUserCmdResourceGroup.

```
<Policy Name="AllUsersExceuteAllUserCmdResourceGroup"
OwnerID="RootOrganization"
UserGroup="AllUsers"
ActionGroupName="ExecuteCommandActionGroup"
ResourceGroupName="AllUserCmdResourceGroup">
</Policy>
```

Para Exibições: Neste exemplo, os usuários pertencentes ao grupo de acesso MarketingManagers podem executar as exibições pertencentes ao grupo de ação MarketingManagersViews.

```
<Policy Name="MarketingManagersExecuteMarketingManagersViews"
OwnerID="RootOrganization"
UserGroup="MarketingManagers"
ActionGroupName="MarketingManagersViews"
ResourceGroupName="ViewCommandResourceGroup">
</Policy>
```

Políticas em Nível do Recurso:

Para Comandos: Neste exemplo, os usuários pertencentes ao grupo de acesso RegisteredApprovedUsers podem executar as ações especificadas pelo grupo de ação CouponRedemption nos recursos especificados pelo CouponWalletResourceGroup, contanto que os usuários preencham o relacionamento creator com respeito ao recurso.

```
<Policy Name="RegisteredApprovedUsersExecuteCouponRedemptionCommandsOn
WalletResource"
OwnerID="RootOrganization"
UserGroup="RegisteredApprovedUsers"
ActionGroupName="CouponRedemption"
ResourceGroupName="CouponWalletResourceGroup"
RelationName="creator">
</Policy>
```

Para Beans de Dados: Neste exemplo, os usuários pertencentes ao grupo de acesso AllUsers podem Exibir os beans de dados especificados pelo grupo de recursos UserDatabeanResourceGroup, contanto que os usuários preencham o relacionamento owner com respeito ao recurso.

```
<Policy Name="AllUsersDisplayUserDatabeanResourceGroup"
OwnerID="RootOrganization"
UserGroup="AllUsers"
ActionGroupName="DisplayDatabeanActionGroup"
ResourceGroupName="UserDatabeanResourceGroup"
RelationName="owner">
</Policy>
```

Políticas Modelo: Neste exemplo, os usuários pertencentes ao grupo de acesso MembershipAdministratorsForOrg, podem executar as ações especificadas pelo grupo de ação ApproveGroupUpdate nos recursos especificados pelo OrganizationDataResourceGroup.

```
<Policy Name=MembershipAdministratorsForOrgExecuteApproveGroupUpdateCommands
OnOrganizationResource"
OwnerID="RootOrganization"
UserGroup="MembershipAdministratorsForOrg"
ActionGroupName="ApproveGroupUpdate"
ResourceGroupName="OrganizationDataResourceGroup"
PolicyType="template">
</Policy>
```

Quando esta política modelo é aplicada, o proprietário da política será dinamicamente alterado de RootOrganization para a entidade organizacional que possui o recurso e subseqüentemente, suas entidades organizacionais ascendentes, e incluindo a Organização Raiz. Examinar a definição do grupo de acesso MembershipAdministratorsForOrg revelaria a seguinte condição da associação:

```
<UserCondition><![CDATA[
<profile>
<orListCondition>
<simple condition>
<variable name="role"/>
<operator name="="/>
<value data="Buyer Administrator"/>
<qualifier name="org" data="?"/>
</simpleCondition>
<simpleConditon>
<variable name="role"/>
<operator name="="/>
<value data="Seller Administrator"/>
<qualifier name="org" data="?"/>
</simpleConditon>
</orListCondtion>
</profile>
]]></UserCondition>
```

Nota: O simpleCondition da função é qualificado por org = **?**. Este **?** é dinamicamente substituído junto ao proprietário da política, conforme explicado acima. Este comportamento dinâmico está disponível apenas para políticas modelo. Assim, neste exemplo, os usuários que têm a função Administrador do Comprador ou Administrador do Vendedor para a entidade organizacional que possui o recurso, satisfaz a condição da associação neste grupo de acesso.

Dados da Política Traduzíveis

A seguir, um modelo dos elementos do controle de acesso traduzível que, no mínimo, deve ser definido no arquivo defaultAccessControlPolicies_*locale*.xml.

```
<?xml version="1.0" encoding="ISO-8859-1" standalone="no" ?>
<!--The following TRANSLATABLE access control elements should
 be defined in this file:
<Attribute_nls>
<Action_nls>
<Relation_nls>
<ResourceCategory_nls>
<ActionGroup_nls>
<ResourceGroup_nls>
<Policy_nls>-->
<!DOCTYPE PoliciesNLS SYSTEM "../dtd/accesscontrolpoliciesnls.dtd">
```

```
<PoliciesNLS LanguageID="value">


 <!--Inserir definições do elemento de controle de acesso aqui -->
 </PoliciesNLS>
```

O atributo `LanguageID` é uma cadeia que corresponde à linguagem dos dados específicos do local. Os valores válidos do `LanguageID` são:

- en_US
- fr_FR
- de_DE
- it_IT
- es_ES
- pt_BR
- zh_CN
- zh_TW
- ko_KR
- ja_JP

Dados da Política não Traduzíveis

A seguir, um modelo de um arquivo de política personalizada contendo dados não traduzíveis:

```
  <?xml version="1.0" encoding="ISO-8859-1" standalone="no" ?>

<!DOCTYPE Policies SYSTEM "../dtd/accesscontrolpolicies.dtd">

<!--Os seguintes elementos do controle de acesso NON-TRANSLATABLE
 devem ser definidos neste arquivo:

<Attribute>
<Action>
<ResourceCategory>
<Relation>
<RelationGroup>
<ActionGroup>
<ResourceGroup>
<Policy-->
<Policies>

 <!--Inserir definições do elemento de controle de acesso aqui -->
 </Policies>
```

Dados Específicos do Locale

Os seguintes dados opcionais específicos do locale podem ser carregados para oferecer descrição adicional aos elementos do controle de acesso definidos no arquivo XML não traduzível. Os dados padrão específicos do locale podem ser encontrados no seguinte endereço:

wc_install_directory\xml\policies\xml\
defaultAccessControlPolicies_*locale*.xml

Por exemplo, `defaultAccessControlPolicies_en_US.xml`.

Atributo: O exemplo a seguir define as informações adicionais sobre o elemento do atributo:

```
<Atrribute_nls AttributeName="Status"
DisplayName_nls="Status attribute"
Description_nls="Resource status attribute"
/>
```

Em que:

`AttributeName`: O nome do atributo. Este valor é armazenado na coluna ATTRNAME da tabela ACATTR.

`DisplayName_nls`: O nome de exibição do atributo. Este valor é armazenado na coluna DISPLAYNAME da tabela ACATTRDESC.

`Description_nls`: Uma descrição opcional do atributo. Este valor é armazenado na coluna DESCRIPTION da tabela ACATTRDESC.

Ação: O exemplo a seguir define as informações do elemento de ação adicional:

```
<Action_nls ActionName="OrderAdjustmentButton"
DisplayName_nls="Order Adjustment Button View"
Description_nls="The view for loading buttons in the order adjustment page
 when placing an order from Commerce Acclerator"
/>
```

Em que:

`ActionName`: O nome da ação. Este valor é armazenado na coluna ACTION da tabela ACACTION.

`DisplayName_nls`: O nome de exibição da ação. Este valor é armazenado na coluna DISPLAYNAME da tabela ACACTDESC.

`Description_nls`: Uma descrição opcional da ação. Este valor é armazenado na coluna DESCRIPTION da tabela ACACTDESC.

Relação: O exemplo a seguir define as informações adicionais do elemento de relação:

```
<Relation_nls RelationName="creator"
DisplayName_nls="creator"
Description_nls="creator"
/>
```

Em que:

`RelationName`: O nome do relacionamento. Este valor é armazenado na coluna RELATIONNAME da tabela ACRELATION.

`DisplayName_nls`: O nome de exibição do relacionamento. Este valor é armazenado na coluna DISPLAYNAME da tabela ACRELDESC.

`Description_nls`: Uma descrição opcional do relacionamento. Este valor é armazenado na coluna DESCRIPTION da tabela ACRELDESC.

Categoria de Recursos: O exemplo a seguir define as informações adicionais da categoria de recursos:

```
<ResourceCategory_nls ResourceCategoryName="com.ibm.commerce.
catalog.objects."InterestItemList"
DisplayName_nls="Interest Item List"
Description_nls="Interest Item List command"
/>
```

Em que:

ResourceCategoryName: O nome da categoria de recursos. Este valor é armazenado na coluna RESCLASSNAME da tabela ACRESCGRY.

DisplayName_nls: O nome de exibição da categoria de recursos. Este valor é armazenado na coluna DISPLAYNAME da tabela ACRSCGDES.

Description_nlsUma descrição opcional da categoria de recursos. Este valor é armazenado na coluna DESCRIPTION da tabela ACRSCGDES.

Grupo de Ação: O exemplo a seguir define as informações adicionais do grupo de ação:

```
<ActionGroup_nls ActionGroupName="DoEverything"
DisplayName_nls="Do Everything"
Description_nls="Permits access to all Actions"
/>
```

Em que:

ActionGroupName: O nome do grupo de ação. Este valor é armazenado na coluna GROUPNAME da tabela ACACTGRP.

DisplayName_nls: O nome de exibição do grupo de ação. Este valor é armazenado na coluna DISPLAYNAME da tabela ACACGPDESC.

Description_nls: Uma descrição opcional do grupo de ação. Este valor é armazenado na coluna DESCRIPTION da tabela ACACGPDESC.

Grupo de Recursos: O exemplo a seguir define as informações adicionais do grupo de recursos:

```
<ResourceGroup_nls ResourceGroupName="AllResourceGroup"
DisplayName_nls="All Resources Group"
Description_nls="All Resources"
/>
```

Em que:

ResourceGroupName: O nome do grupo de recursos. Este valor é armazenado na coluna GRPNAME da tabela ACRESGRP.

DisplayName_nls: O nome de exibição do grupo de recursos. Este valor é armazenado na coluna DISPLAYNAME da tabela ACRESGPDES.

Description_nls: Uma descrição opcional do grupo de recursos. Este valor é armazenado na coluna DESCRIPTION da tabela ACRESGPDES.

Política: O exemplo a seguir define as informações da política:

```
<Policy_nls PolicyName="SiteAdministratorsCanDoEverything"
OnwerID="RootOrganization"
DisplayName_nls="Site Administrators Can Do Everything"
Description_nls="Policy that allows Site Administrators to do everything"
/>
```

Em que:

PolicyName: O nome da política de controle de acesso. Este valor é armazenado na coluna POLICYNAME da tabela ACPOLICY.

`OwnerID`: O ID do membro da entidade organizacional que possui esta política.

`DisplayName_nls`: O nome de exibição da política. Este valor é armazenado na coluna DISPLAYNAME da tabela ACPOLDESC.

`Description_nls`: Uma descrição opcional da política. Este valor é armazenado na coluna DESCRIPTION da tabela ACPOLDESC.

Depois de Alterar os Arquivos XML

Testando suas Alterações

Para obter informações sobre como testar suas alterações, consulte "Depois de Fazer as Alterações na Política" na página 45.

Carregando suas Alterações no Banco de Dados

Se você fizer alterações na política trabalhando diretamente com arquivos XML, você deverá carregar os arquivos XML alterados novamente nos bancos de dados. É importante manter a consistência entre os arquivos XML e as informações de controle de acesso nos bancos de dados por diversos motivos:

- Quando você cria uma instância do WebSphere Commerce, a política e as definições do grupo de acesso são carregadas a partir dos arquivos XML.
- Se quiser implementar as mesmas políticas de controle de acesso em uma segunda instância do WebSphere Commerce, poderá fazer isso copiando os arquivos XML para o diretório adequado antes de criar a segunda instância.
- Os arquivos XML oferecem uma maneira conveniente de exibir e editar diretamente suas políticas e partes de componentes; portanto, manter os arquivos atualizados é essencial.

Carregando suas Alterações de XML no Banco de Dados

O processo de carregamento lê os arquivos XML que contêm as informações da política de controle de acesso e as definições do grupo de acesso e carrega-os nos bancos de dados apropriados. A política e as informações do grupo de acesso contidas nos arquivos XML são carregadas na instalação; no entanto, você deve carregar novamente os arquivos se fizer alterações neles.

Nota: Se você criar arquivos XML personalizados, será necessário copiá-los no diretório *<wc_install_directory>*`/xml/policies/xml` para carregá-los nos bancos de dados.

Para 400: se você criar arquivos XML personalizados, deverá utilizar o caminho completo para o DTD em seu arquivo. Os DTDs das políticas de controle de acesso estão localizados em `/QIBM/ProdData/WebCommerce/xml/policies/dtd`.

Para carregar os grupos de acesso e as políticas de controle de acesso, execute os seguintes comandos.

Para NT 2000

1. Do diretório *<wc_install_directory>*`\bin`, execute os seguintes arquivos de comandos conforme necessário na ordem listada aqui:
   - Para carregar as definições do grupo (acesso) de usuário, execute o arquivo de comando **acugload**. **Sintaxe**: acugload.cmd *<database name> <database user*

> *<database user password>* < *UserGroups xml file>* **Exemplo** : acugload mall dbuser dbusrpwd ACUserGroups_en_US.xml

- Para carregar o arquivo de políticas de controle de acesso principal, execute o arquivo de comando **acpload**. **Sintaxe:** acpload.cmd *<database name>* *<database user>* *<database user password>* *<Policies xml file>* **Exemplo**: acpload mall dbuser dbusrpwd defaultAccessControlPolicies.xml
- Para carregar os nomes de exibição e o arquivo de descrições, execute o arquivo de comando **acpnlsload**. **Sintaxe:** acpnlsload.cmd *<database name>* *<database user>* *<database user password>* *<NLS Policies xml file>* **Exemplo**: acpnlsload mall dbuser dbusrpwd defaultaccesscontrolpolicies_en_US.xml

2. Verifique os arquivos de log **acugload.log**, **acpload.log,** e **acpnlsload.log** em *<wc_install_directory>*\logs à procura de erros.

Para AIX Solaris Linux

O ID do usuário do banco de dados deve ter autoridade de leitura/gravação/execução para os diretórios *<wc_install_directory>*/xml/policies, *<wc_install_directory>*/bin and *<wc_install_directory>*/properties/utilities, bem como seus subdiretórios e arquivos.

1. Efetuar login como o ID do usuário do banco de dados.
2. Do diretório *<wc_install_directory>*/bin, execute os seguintes scripts de shell, conforme for necessário na ordem listada aqui:

1. Para carregar as definições do grupo (acesso) de usuário, execute o script de shell **acugload**. **Sintaxe:** acugload.sh *<database name>* *<database user >* *<database user password>* *<UserGroups xml filename>* **Exemplo**: acugload mall dbuser dbusrpwd ACUserGroups_en_US.xml
2. Para carregar o arquivo de políticas de controle de acesso principal, execute o seguinte script de shell **acpload**. **Sintaxe:** acpload.sh *<database name>* *<database user>* *<database user password>* *<Policies xml filename>* **Exemplo**: acpload mall dbuser dbusrpwd defaultAccessControlPolicies.xml
3. Para carregar os nomes de exibição e o arquivo de descrições, execute o script de shell acpnlsload. **Sintaxe:**acpnlsload.sh *<database name>* *<database user>* *<database user password>* *<NLS Policies xml filename>* **Exemplo**: acpnlsload mall dbuser dbusrpwd defaultaccesscontrolpolicies_en_US.xml

Verifique os arquivos de log acugload.log, acpload.log e acpnlsload.log em *<wc_install_directory>*/logs à procura de erros.

Nota: Após ter executado estes scripts, será necessário verificar os arquivos de log, pois qualquer erro que possa ocorrer durante a execução destes scripts não aparecerá na linha de comandos.

Para 400

Na linha de comandos, execute os seguintes comandos conforme necessário na ordem especificada.

- Para carregar as definições do grupo (acesso) do usuário, execute o comando LODWCSUG. **Sintaxe:** LODWCSUG DATABASE(*<database name>*) SCHEMA(*<schema_name>*) PASSWD(*<instance_password>*) INSTROOT(*<instance_root>*) INFILE(*<full path for XML file>*)
- Para carregar o arquivo de políticas de controle de acesso principal, execute o comando LODWCSAC. **Sintaxe:** LODWCSAC DATABASE (<database name>)

SCHEMA (<schema_name>) PASSWD (<instance_password>) INSTROOT (<instance_root>) INFILE (*<full path for XML file>*)

- Para carregar os nomes de exibição e o arquivo de descrições, execute o comando `LODWCSACD`. **Sintaxe:** LODWCSACD DATABASE(*<database name>*) SCHEMA(*<schema_name>*) PASSWD (< *instance_password*>) INSTROOT(*<instance_root* >) INFILE(*<full path to XML file*>)

Extraindo Definições da Política e do Grupo de Acesso do Banco de Dados em seus Arquivos XML

O processo de extração lê as informações da política e do grupo de acessos nos bancos de dados do controle de acesso e gera arquivos que capturam as informações no formato XML.

Para NT 2000

1. Do diretório `<wc_install_directory>\bin`, execute o seguinte comando `acpextract`:

   ```
   acpextract.cmd <database name> <database user> <database user password>
   ACPoliciesfilter.xml
   ```

   Por exemplo,

   ```
   acpextract.cmd mall dbuser dbusrpwd ACPoliciesfilter.xml
   ```

   Os seguintes arquivos são criados:

   - `ExtractedACPolicies.xml`: Este arquivo contém dados extraídos pelo comando `Extract` para o critério do filtro determinado.
   - `ExtractedACPolicies.dtd`: O DTD para o arquivo `ExtractedACPolicies.xml`.
   - `AccessControlUserGroups.xml`: O arquivo que contém as definições do grupo de acesso.
   - `AccessControlPolicies.xml`: O arquivo que contém as informações da política de controle de acesso independente da linguagem.
   - `AccessControlPolicies_LOCALE.xml`: O arquivo das políticas de controle de acesso dependente de linguagem que contém os nomes de exibição e descrições.
2. Verifique o arquivo de log `<wc_install_directory>\logs\acpextract.log`para quaisquer erros de processamento que possa ter ocorrido.

Para AIX Solaris Linux

1. Efetuar login como o ID do usuário do banco de dados.
2. Do diretório `<wc_install_directory>\bin`, execute o seguinte script de shell `acpextract`:

   ```
   acpextract.sh <database name> <database user>
   <database user password> ACPoliciesfilter.xml
   ```

   Por exemplo,

   ```
   acpextract.sh mall dbuser dbusrpwd ACPoliciesfilter.xml
   ```

   Os seguintes arquivos são criados:

   - `ExtractedACPolicies.xml`: Este arquivo contém dados extraídos pelo comando `Extract` para o critério do filtro determinado.
   - `ExtractedACPolicies.dtd`: O DTD para o arquivo `ExtractedACPolicies.xml` .

- AccessControlUserGroups.xml: O arquivo que contém as definições do grupo de acesso.
- AccessControlPolicies.xml: O arquivo que contém as informações da política de controle de acesso independente da linguagem.
- AccessControlPolicies_LOCALE.xml: O arquivo das políticas de controle de acesso dependente de linguagem que contém os nomes de exibição e descrições.

3. Verifique o arquivo de log <*wc_install_directory*>\logs\acpextract.logpara quaisquer erros de processamento que possa ter ocorrido.

Para ▶ 400

1. Da linha de comandos, execute o seguinte comando EXTWCSAC:

```
EXTWCSAC DATABASE (<database name>)
 SCHEMA (<schema_name>) PASSWD (<database user>)
INSTROOT (<instance_root>) FILTER (<input filter XML file>) OUTDIR
 (<output directory
 for new files>)
```

   Os seguintes arquivos são criados no diretório especificado, utilizando o parâmetro OUTDIR:
   - ExtractedACPolicies.xml: Este arquivo contém dados extraídos pelo comando Extract para o critério do filtro determinado.
   - ExtractedACPolicies.dtd: O DTD para o arquivo ExtractedACPolicies.xml .
   - AccessControlUserGroups.xml: O arquivo que contém as definições do grupo de acesso.
   - AccessControlPolicies.xml: O arquivo que contém as informações da política de controle de acesso independente da linguagem.
   - AccessControlPolicies_LOCALE.xml: O arquivo das políticas de controle de acesso dependente de linguagem que contém os nomes de exibição e descrições.

Apêndice. Políticas de Controle de Acesso Padrão

O Apêndice lista as políticas padrão fornecidas com o WebSphere Commerce. Elas são organizadas nas seguintes categorias:

- **Políticas baseadas em funções:** As políticas baseadas em funções para cada função padrão. Essas políticas também são mencionadas como políticas em nível de comandos porque elas definem quem pode executar cada comando.
- **Políticas em nível do recurso:** As políticas em nível do recurso, agrupadas por área de negócios. Essas políticas definem as ações que um grupo de usuários pode executar em recursos específicos. Em cada área de negócios, as políticas são organizadas pelo tipo de recurso que elas regulam:
  - **Recursos de dados** - objetos de negócios que podem ser manipulados como um pedido ou um lance.
  - **Recursos de bean de dados** - contém informações sobre os objetos de negócios. Os Beans de dados são utilizados para exibir informações de objeto em uma página na Web.

Tabela 6.

Políticas	**Iniciando na página**
Políticas baseadas em funções	"Políticas Baseadas em Funções" na página 108
Políticas em nível do recurso por área de negócios:	"Políticas em Nível do Recurso por Área de Negócios" na página 109
Pedidos	"Pedidos" na página 109
Comércio (contratos)	"Comércio (Contratos)" na página 110
Aprovações	"Aprovações" na página 111
Leilões	"Leilões" na página 111
Inteligência de negócios	"Inteligência de Negócios" na página 111
Associação	"Associação" na página 112
Administration console de comprador	"Administration Console de Comprador" na página 112
Campanhas	"Campanhas" na página 112
Catálogo	"Catálogo" na página 113
Conectividade e notificação	"Conectividade e Notificação" na página 113
Procurement	"Procurement" na página 114
Cupons	"Cupons" na página 114
Perfil de cliente	"Perfil de Cliente" na página 114
Descontos	"Descontos" na página 114
Estoque	"Gerenciamento de Estoque" na página 115
Estoque Programado	"Estoque Programado" na página 115
Gerenciamento de Estoque	"Gerenciamento de Estoque" na página 115
Gerenciamento de pedidos	"Gerenciamento de Pedidos" na página 116
Pagamento	"Pagamento" na página 117

Tabela 6. (continuação)

As páginas do Administration console para editar políticas, grupos de acesso, grupos de recursos e grupos de ação	"Páginas do Administration Console para Editar Políticas, Grupos de Acesso, Grupos de Recursos e Grupos de Ação" na página 117
Consultor de Produtos	"Consultor de Produto" na página 117
RFQ	"RFQ" na página 117
Regras	"Regras" na página 118
Programador	"Programador" na página 118

Políticas Baseadas em Funções

Tabela 7.

AccountRepresentativesExecuteAccountRepresentativesCmdResourceGroup
AccountRepresentativesExecuteAccountRepresentativesViews
AllUsersExecuteAllUserCmdResourceGroup
AllUsersExecuteAllUsersViews
BecomeUserCustomerServiceGroupExecutesBecomeUserCmdsResourceGroup
BuyerAdministratorsExecuteBuyerAdminstratorsViews
BuyerAdministratorsExecuteBuyerAdminstratorsCommands
BuyerApproversExecuteBuyerApproversCmdResourceGroup
BuyerApproversExecuteBuyerApproversViews
Buyers(buy-side)ExecuteBuyers(buy-side)CommandsResourceGroup
Buyers(buy-side)ExecuteBuyers(buy-side)Views
Buyers(sell-side)ExecuteBuyers(sell-side)CommandsResourceGroup
Buyers(sell-side)ExecuteBuyers(sell-side)Views
CategoryManagersExecuteCategoryManagersCmdResourceGroup
CategoryManagersExecuteCategoryManagersView
CustomerServiceRepresentativesExecuteCustomerServiceRepCmdResourceGroup
CustomerServiceRepresentativesExecuteCustomerServiceRepresentativeView
CustomerServiceSupervisorsExecuteCustomerServiceSupervisorCmdResourceGroup
CustomerServiceSupervisorsExecuteCustomerServiceSupervisorViews
CustomersExecuteCustomersViews
GuestsExecuteGuestUsersCmdResourceGroup
LogisticsManagersExecuteLogisticsManagersCmdResourceGroup
LogisticsManagersExecuteLogisticsManagersViews
MarketingManagersExecuteMarketingManagerCmdResourceGroup
MarketingManagersExecuteMarketingManagersViews
OperationsManagersExecuteOperationsManagersCmdResourceGroup
OperationsManagersExecuteOperationsManagersView
PickPackersExecutePickPackersCmdResourceGroup
PickPackersExecutePickPackersViews
ProcurementBuyersExecuteProcurementBuyersCmdResourceGroup

Tabela 7. (continuação)

ProductManagersExecuteProductManagersCmdResourceGroup
ProductManagersExecuteProductManagersViews
ReceiversExecuteReceiversCmdResourceGroup
ReceiversExecuteReceiversViews
ReturnsAdministratorsExecuteReturnsAdministratorsCmdResourceGroup
ReturnsAdministratorsExecuteReturnsAdministratorsViews
SalesManagersExecuteSalesManagersCmdResourceGroup
SalesManagersExecuteSalesManagersViews
SellerAdministratorsExecuteSellerAdministratorsCommands
SellerAdministratorsExecuteSellerAdministratorsViews
SellersExecuteSellersCmdResourceGroup
SellersExecuteSellersView
SiteAdministratorsCanDoEverything
StoreAdministratorsExecuteStoreAdministratorsCmdResourceGroup
StoreAdministratorsExecuteStoreAdministratorViews

Políticas em Nível do Recurso por Área de Negócios

Pedidos

Tabela 8.

Recursos de Dados	
Pedido	AllUsersExecuteOrderCreateCommandsOnStoreResource
	AllUsersExecuteOrderPrepareCommandsOnOrderResource
	AllUsersExecuteOrderProcessOnOrderResource
	AllUsersExecuteOrderReadCommandsOnOrderResource
	AllUsersExecuteOrderWriteCommandsOnOrderResource
	AllUsersExecuteReturnAgainstOrderOnOrderResource
	AllUsersExecuteScheduledOrderCancelOnOrderResource
	OrderManagersForOrgExecuteOrderManageCommandsOnOrderResource
Lista de Requisições	AllUsersExecuteRequisitionListCreateCommandsOnStoreEntityResource
	AllUsersExecuteRequisitionListExclusiveProcessCommands OnPrivateRequisitionListResource
	AllUsersExecuteRequisitionListExclusiveReadCommandsOn PrivateRequisitionListResource
	AllUsersExecuteRequisitionListSharedProcessCommandsOn SharedRequisitionListResource
	AllUsersExecuteRequisitionListSharedReadCommandsOn SharedRequisitionListResource
	AllUsersExecuteRequisitionListWriteCommandsOn RequisitionListResource

Tabela 8. (continuação)

Item de Interesse	AllUsersExecuteInterestItemReadCommandsOnInterestItemListResource
	AllUsersExecuteInterestItemWriteCommandsOnInterestItemListResource
RMA (Autorização para Devolução de Mercadorias)	AllUsersExecuteRMACreateCommandsOnStoreResource
	AllUsersExecuteRMAProcessCommandsOnRMAResource
	AllUsersExecuteRMAReadCommandsOnRMAResource
	AllUsersExecuteRMAWriteCommandsOnRMAResource
	RMAApproversForOrgExecuteRMAApproveCommandsOnRMAResource
	RMADisposersForOrgExecuteRMADisposeCommandsOnRMAResource
	RMAManagersForOrgExecuteRMAManageCommandsOnRMAResource
	RMAReceiversForOrgExecuteRMAReceiveCommandsOnRMAResource
	StoreAdministratorsForOrgExecuteRMACreditCommandsOnStoreEntityResource
DataBeans	
Pedido	AllUsersDisplayApprovalsOrderDataBeansResourceGroup
	AllUsersDisplayOrderDatabeanResourceGroup
Lista de Requisições	AllUsersDisplaySharedRequisitionListDataBeansIfSame OrganizationalEntityAsCreator
Item de Interesse	AllUsersDisplayInterestItemDatabeanResourceGroup
RMA	AllUsersDisplayRMADatabeanResourceGroup

Comércio (Contratos)

Tabela 9.

Recurso de Dados	
Contrato	ContractAdministratorsForOrgExecuteContractCreateCommandsOn MemberResource
	ContractAdministratorsForOrgExecuteContractManageCommandsOn ContractResource
	ContractOperatorsForOrgExecuteContractDeployCommandsOn ContractResource
	ContractOperatorsForOrgExecuteContractSubmitCommandsOn ContractResource
	ContractViewersExecuteContractDisplayCommandsOnContractResource
Política de Negócios	BusinessPolicyAdministratorsForOrgExecuteBusinessPolicy CreateCommandsOnStoreResoure
	BusinessPolicyAdministratorsForOrgExecuteBusinessPolicy ManageCommandsOnBusinessPolicyResourcee
DataBeans	AccountHandlersDisplayTradingDatabeanResourceGroup

Aprovações

Tabela 10.

Recursos de Dados	
	AllUsersExecuteAllUsersActionGroupCommandsOnOrderResource
	AllUsersExecuteApproveCommandsOnApprovalResource
	AllUsersExecuteCancelApproveCommandsOnApprovalResource

Leilões

Tabela 11.

Recursos de Dados	
Leilão	AuctionAdministratorsForOrgExecuteAdminRetractBidCommands OnAuctionResource
	AuctionAdministratorsForOrgExecuteAuctionCreateCommands OnStoreEntityResource
	AuctionAdministratorsForOrgExecuteAuctionManageCommands OnAuctionResource
Estilo de Leilão	AuctionAdministratorsForOrgExecuteAuctionStyleCreateCommands OnStoreEntityResource
	AuctionAdministratorsForOrgExecuteAuctionStyleManageCommands OnAuctionStyleResource
Regra de Controle de Lances	AuctionAdministratorsForOrgExecuteBidControlRuleCreateCommands OnStoreEntityResource
	AuctionAdministratorsForOrgExecuteBidControlRuleManageCommands OnBidControlRuleResource
Lance	RegisteredApprovedUsersExecuteBidCreateCommandsOnAuctionResource
	RegisteredApprovedUsersExecuteBidManageCommands OnBidResourcesTheyOwn
AutoBid	RegisteredApprovedUsersExecuteAutoBidCreateCommands OnAuctionResource
	RegisteredApprovedUsersExecuteAutoBidManageCommands OnAutoBidResourcesTheyOwn
DataBeans	AuctionDatabeanOwnersDisplayAuctionDatabeans

Inteligência de Negócios

Tabela 12.

Recursos de Dados	
	BusinessAnalystsForOrgExecuteViewContext ListCommandsOnStoreEntityResource
	IntelligenceReportViewersForOrgExecuteViewBusinessIntelligenceReport CommandsOnStoreEntityResource

Associação

Tabela 13.

Recursos de Dados	
Usuário	GuestsExecuteUserSelfRegistrationCommandsOnOrganizationResource
	MembershipAdministratorsForOrgExecuteUserAdminRegistration CommandsOnOrganizationResource
	MembershipAdministratorsForOrg ExecuteUserAdminUpdateCommandsOnUserResource
	NonRejectedUsersExecuteUserSelfRegistration ContinuationCommandsOnUserResource
Organização	MembershipAdministratorsForOrgExecute OrgEntityRegistrationCommandsOnOrganizationResource
	MembershipAdministratorsForOrgExecuteOrg EntityUpdateCommandsOnOrganizationResource
Endereço	MembershipAdministratorsForOrg ExecuteAddressManageCommandsOnMemberResource
	NonRejectedUsersExecuteAddressManageCommandsOn UserResource
Função	MembershipAdministratorsForOrgExecute RoleManageCommandsOnUserResource
	OrganizationRoleAdministratorsExecute RoleManageCommandsOnOrganizationResource
Grupo de Membros	MemberGroupAdministratorsForOrgExecute MemberGroupCreateCommandsOnMemberResource
	MemberGroupManagersForOrgExecute MemberGroupManageCommandsOnMemberGroupResource
DataBeans	MembershipAdministratorsForOrgDisplay OrganizationDatabeanResourceGroup
	MembershipViewersForOrgDisplayMembershipDatabeanResourceGroup

Administration Console de Comprador

Tabela 14.

Recursos de Dados	
Grupo de Aprovação	MembershipAdministratorsForOrgExecute ApproveGroupUpdateCommandsOnOrganizationResource
Grupo de Membros	MembershipAdministratorsForOrgExecute MemberGroupMemberUpdateCommandsOnMemberGroupResource
	MembershipAdministratorsForOrgExecute MemberGroupMemberUpdateCommandsOnUserResource

Campanhas

Tabela 15.

Recursos de Dados	

Tabela 15. (continuação)

	CampaignManagersForOrgExecute CampaignRelatedCreateCommandsOnStoreEntityResource
	CampaignManagersForOrgExecute CampaignUpdateCommandsOnCampaignResource
	CampaignManagersForOrgExecute CollateralUpdateCommandsOnCollateralResource
	CampaignManagersForOrgExecute EMarketingSpotUpdateCommandsOnEMarketingSpotResource
	CampaignManagersForOrgExecute InitiativeUpdateCommandsOnInitiativeResource
DataBeans	CampaignManagersForOrgDisplayCampaignDatabeanResourceGroup

Catálogo

Tabela 16.

Recursos de Dados	
	CatalogEntryManagersForOrgExecute CatalogEntryManageCommandsOnCatalogEntryResource
	CatalogEntryManagersForOrgExecute CatalogEntryRelationManageCommandsOnCatalogResource
	CatalogEntryManagersForOrgExecute StoreCatalogEntryManageCommandsOnStoreEntityResource
	CatalogGroupManagersForOrgExecute CatalogGroupManageCommandsOnCatalogGroupResource
	CatalogGroupManagersForOrgExecute ProductSetAddCommandsOnCatalogResource
	CatalogGroupManagersForOrgExecute ProductSetManageCommandsOnProductSetResource
	CatalogManagersForOrgExecute CatalogManageCommandsOnCatalogResource
	CatalogManagersForOrgExecute StoreCategoryManageCommandsOnCatalogResource
DataBeans	CatalogGroupManagersForOrgDisplay CatalogGroupDataBeansResourceGroup
	ProductAdministratorsForOrgDisplayProductDataBeansResourceGroup

Conectividade e Notificação

Tabela 17.

Recursos de Dados	
	BackendOrderAdministratorsForOrgExecute BackendOrderStatusCreateCommandsOnOrderDataResource
	BackendPickPackersForOrgExecute BackendPickPackListCommandsOnFulfillmentCenterDataResource
	StoreAdministratorsForOrgExecute MessagingAdminCommandsOnStoreEntityResource

Tabela 17. (continuação)

DataBeans	StoreAdministratorsForOrgDisplayMessagingDataBeans

Procurement

Tabela 18.

Recursos de Dados	
	ProcurementAdministratorsForOrgExecute ProcurementAuthenticationAndRegistrationOnOrderDataResource
	ProcurementShoppingCartManagersExecute ProcurementShoppingCartManageOnOrderResource

Cupons

Tabela 19.

Recursos de Dados	
	CouponAdministratorsForOrgExecute CouponPromotionCreateCommandsOnStoreEntityResource
	CouponAdministratorsForOrgExecuteCouponPromotionDeleteCommands OnCouponPromotionResource
	RegisteredApprovedUsersExecute CouponDeleteCommandsOnCouponWalletResource
	RegisteredApprovedUsersExecute CouponRedemptionCommandsOnCouponWalletResource
	StoreAdministratorsForOrgExecute ScheduledCouponCmdsOnStoreResource
DataBeans	CouponAdministratorsForOrgDisplayECouponPromotionListBeans

Perfil de Cliente

Tabela 20.

Recursos de Dados	
	CustomerProfileEditorsForOrgExecute SegmentManageCommandsOnStoreEntityResource
DataBeans	CustomerProfileEditorsForOrgDisplay SegmentationDatabeansResourceGroup

Descontos

Tabela 21.

Recursos de Dados	
	DiscountAdministratorsForOrgExecute DiscountAssociateCommandsOnCalculationCodeResource

Tabela 21. (continuação)

	DiscountAdministratorsForOrgExecute DiscountCreateCommandsOnStoreEntityResource
	DiscountAdministratorsForOrgExecute DiscountDeployCommandsOnCalculationCodeResource
DataBeans	DiscountViewersForOrgDisplayDiscountDatabeans

Gerenciamento de Estoque

Tabela 22.

Recursos de Dados	
	ExpectedInventoryManagersForOrgExecute InventoryManageCommandsOnStoreEntityResource
	FulfillmentCenterManagersForOrgExecute FulfillmentCenterCreateCommandsOnOrganizationResource
	FulfillmentCenterManagersForOrgExecute FulfillmentCenterManageCommandsOnFulfillmentResource
	InventoryAdjustersForOrgExecute InventoryAdjustCommandsOnStoreEntityResource
	PickBatchInventoryManagersForOrgExecuteReleaseReadyShipCommands OnFulfillmentCenterResource
	PickPackGeneratorsForOrgExecute PickPackGenerateCommandsOnFulfillmentCenterResource
	ReturnReasonsManagersForOrgExecute ReturnReasonsCommandsOnStoreEntityResource
	VendorInventoryManagersForOrgExecute VendorCreateCommandsOnStoreEntityResource
	VendorInventoryManagersForOrgExecute VendorManageCommandsOnVendorResource
DataBeans	StoreAdministratorsForOrgDisplay OrderFulfillmentStatusDataBeansResourceGroup

Estoque Programado

Tabela 23.

Recursos de Dados	
	StoreAdministratorsForOrgExecute InventoryScheduledCommandsOnStoreEntityResource

Gerenciamento de Estoque

Tabela 24.

DataBeans	
	ExpectedInventoryManagersForOrgDisplay ExpectedInventoryDataBeansResourceGroup

Tabela 24. (continuação)

	FulfillmentCenterManagersForOrgDisplay FulfillmentCenterDataBeansResourceGroup
	PickBatchInventoryManagersForOrgDisplay PickBatchInventoryDataBeansResourceGroup
	ProductFindInventoryManagersForOrgDisplay ProductFindInventoryDataBeansResourceGroup
	ReceiverOrderManagersForOrgDisplay ReceiverOrderManagementDataBeansResourceGroup
	ReturnReasonsManagersForOrgDisplay ReturnReasonsOrderManagementDataBeansResourceGroup
	ReturnsAdminOrderManagersForOrgDisplay ReturnsAdminOrderManagementDataBeansResource
	SuperUserOrderManagersForOrgDisplay SuperUserOrderManagementDataBeansResourceGroup
	VendorInventoryManagersForOrgDisplay VendorInventoryDataBeansResourceGroup

Gerenciamento de Pedidos

Tabela 25.

Recursos de Dados	
	CustomerOrderManagersExecute CustomerServiceCustomerWriteCommandsOnUserResource
	CustomerOrderManagersForDefaultOrgExecute CustomerServiceCustomerWriteCommandsOnUse
	CustomerOrderManagersForOrgExecute CustomerServiceOrderCreateCommandsOnStoreEntityResource
	CustomerOrderManagersForOrgExecute CustomerServiceOrderWriteCommandsOnOrderResource
	CustomerOrderManagersForOrgExecute CustomerServiceReturnCreateCommandsOnStoreEntity
	CustomerOrderManagersForOrgExecute CustomerServiceReturnWriteCommandsOnRMAResource
DataBeans	CustomerOrderManagersDisplay CustomerUserManagementDatabeans
	CustomerOrderManagersForDefaultOrgDisplay CustomerUserManagementDatabeans
	CustomerOrderManagersForOrgDisplay CustomerOrderManagementDatabeans
	LogisticsManagersForOrgDisplay OrdersAndReturnsListsDatabeans
	ReturnsManagersForOrgDisplayReturnsListsDatabean
	UserOrderManagersDisplayUserDatabeans
	UserOrderManagersForDefaultOrgDisplayUserDatabeans

Pagamento

Tabela 26.

Recursos de Dados	
	AccountAdministratorsForOrgExecute AccountManageCommandsOnAccountResource
	AccountManagersForOrgExecute AccountCreateCommandsOnOrganizationResource
	AccountViewersForOrgExecute PaymentSummaryGenerateCommandsOnAccountResource
	AccountViewersForOrgExecute StorePaymentAdminCommandsOnStoreEntityResource
	AllUsersExecutePaymentOrderWrite CommandsOnOrderResource

Páginas do Administration Console para Editar Políticas, Grupos de Acesso, Grupos de Recursos e Grupos de Ação

Tabela 27.

Recursos de Dados	
	DescendantStoreAdministratorsExecute ACViewPoliciesForOrgActionsOnOrganizationResource
	StoreAdministratorsForOrgExecute ACPolicyCreateCommandsOnOrganizationResource
	StoreAdministratorsForOrgExecute ACPolicyEditCommandsOnACPolicyResource
	StoreAdministratorsForOrgExecute ACViewApplicablePoliciesActionsOnOrganizationResource
	StoreAdministratorsForOrgExecute ACViewPoliciesForUpdateActionsOnOrganizationResource
DataBeans	StoreAdministratorsForOrgExecute UserGroupSearchViews

Consultor de Produto

Tabela 28.

DataBeans	
	ProductAdvisorStatisticiansForOrgDisplay ProductAdvisorStatisticsDatabeans
	SalesAssistantStatisticiansForOrgDisplay SalesAssistantStatisticsDatabeans

RFQ

Tabela 29.

Recursos de Dados	

Tabela 29. (continuação)

	RFQAdministratorsAdministerRFQs
	RFQAdministratorsManageRFQResponses
	RFQBuyersEvaluateRFQResponsesForRFQsTheyOwn
	RFQBuyersForOrgExecuteRFQCreate CommandsOnStoreEntityDataResourceGroup
	RFQBuyersManageRFQResourcesTheyOwn
	RFQBuyersManageRFQResponsesForRFQsTheyOwn
	RFQSalesManagersExecuteRFQResponse ManageCommandsOnRFQResponseResource
	RFQSalesManagersForOrgCreateRFQResponse
DataBeans	RFQBuyersDisplayRFQDataBeanResourceGroupTheyOwn
	RFQBuyersDisplayRFQResponseDataBeans ViewabletoRFQOwnerResourceGroup
	RFQSalesViewersDisplayRFQDataBeanResourceGroup
	RFQSalesViewersDisplayRFQResponseDataBeanResourceGroup

Regras

Tabela 30.

Recursos de Dados	
	StoreAdministratorsForOrgExecutePersonalization RuleServiceAdministrationCommandsOnStoreEntityResource
DataBeans	StoreAdministratorsForOrgDisplay PersonalizationRuleServiceAdministrationDataBeanResource

Programador

Tabela 31.

Recursos de Dados	
	StoreAdministratorsForOrgExecute ScheduledJobManageCommandsOnStoreEntityResource
	StoreAdministratorsForOrgExecute ScheduledJobManageCommandsOnUserResource
DataBeans	StoreAdministratorsForOrgDisplay SchedulerDataBeansResourceGroup

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 apresentados 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.

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

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

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
Tokio 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 o(s) produto(s) e/ou programa(s) descrito(s) 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 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
Avenida Pasteur, 138/146
Botafogo
CEP: 22290-240
Rio de Janeiro - RJ

Tais informações podem estar disponíveis, sujeitas a termos e condições apropriados, 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 qualquer outro contrato equivalente.

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 do desempenho, compatibilidade ou quaisquer outras reivindicações relacionadas à produtos não-IBM. Dúvidas sobre os recursos de produtos não-IBM devem ser encaminhadas diretamente a seus fornecedores.

Estas informações contém exemplos de dados e relatórios utilizados nas operações diárias de negócios. Para ilustrá-los ao máximo possível, os exemplos incluem nomes de indivíduos, empresas, marcas e produtos. Todos estes nomes são fictícios e qualquer semelhança aos nomes e endereços utilizados por uma empresa de negócios real é mera coincidência.

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.

Licença de Copyright

Estas informações contêm exemplos de programas aplicativos no idioma de origem, ilustrando as técnicas de programação em diversas plataformas operacionais. O Cliente pode copiar, modificar e distribuir estes programas de exemplo de qualquer maneira sem pagamento à IBM, com objetivos de desenvolvimento, utilização, marketing ou distribuição de programas aplicativos em conformidade com a interface de programação de aplicativo para a plataforma operacional para qual os programas de exemplo são gravados. Estes exemplos não foram testados completamente em todas as condições. A IBM, portanto, não pode garantir a confiabilidade, manutenção ou função destes programas. O Cliente pode

copiar, modificar e distribuir estes programas de exemplo de qualquer maneira sem pagamento à IBM com objetivos de desenvolvimento, utilização, marketing ou distribuição de programas aplicativos em conformidade com as interfaces de programação de aplicativo da IBM.

Marcas

Os termos a seguir são marcas da International Business Machines Corporation nos Estados Unidos e/ou em outros países:

DB2 DB2 Universal Database

IBM WebSphere

Lotus, Domino e Go Webserver são marcas da Lotus Development Corporation nos Estados Unidos e/ou em outros países.

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

Pentium™ é uma marca da Intel Corporation nos Estados Unidos e/ou em outros países.

Solaris Operating Environment, JDBC, Java™, e todas as marcas baseadas em Java são marcas ou marcas registradas da Sun Microsystems, Inc. nos Estados Unidos e em outros países.

Blaze Advisor, Blaze Expert, Blaze Presenter, Blaze Accessor, Blaze Enterprise, OOScript e Smartlets são marcas da Blaze Software, Inc. nos Estados Unidos e/ou em outros países.

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

Imagens de cartão de crédito, marcas e nomes comerciais fornecidos neste produto devem ser utilizados apenas pelos comerciantes autorizados pelo proprietário da marca do cartão de crédito para aceitar pagamento por cartão de crédito.