

IBM WebSphere Commerce



# Guia de Segurança

*Versão 5.5*



IBM WebSphere Commerce



# Guia de Segurança

*Versão 5.5*

**Nota:**

Antes de utilizar estas informações e o produto por ela suportado, certifique-se de ler a informação em “Avisos” na página 227.

**Primeira Edição (Junho de 2003)**

Esta edição aplica-se ao IBM WebSphere Commerce Versão 5.5 (número do produto 5724-A18) e a todos os releases e modificações subseqüentes até que seja indicado de outra forma em novas edições. Certifique-se de utilizar a edição correta para o nível do produto.

Solicite publicações através de um representante IBM ou uma filial IBM que atende sua localidade.

A IBM agradece os seus comentários. Eles podem ser enviados utilizando o formulário de feedback on-line da documentação do IBM WebSphere Commerce, disponível no seguinte URL:

<http://www.ibm.com/software/commerce/rcf.html>

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.

© Copyright International Business Machines Corporation 2003. Todos os direitos reservados.

# Índice

<b>Sobre este Manual.</b> . . . . .	<b>vii</b>
Resumo das Alterações . . . . .	vii
Navegando por este Manual . . . . .	vii
Convenções Utilizadas neste Manual . . . . .	viii
Variáveis de Caminho . . . . .	ix

## Parte 1. Conceitos de Segurança do WebSphere Commerce . . . . . 1

### Capítulo 1. Introdução ao Modelo de Segurança do WebSphere Commerce . . . 3

Visão Geral . . . . .	3
O que é Autenticação? . . . . .	3
O que é Autorização? . . . . .	3
O que são Diretivas de Controle de Acesso? . . . . .	3
O que é uma Trilha de Auditoria? . . . . .	4
O que é confidencialidade? . . . . .	4
Considerações Gerais sobre Segurança . . . . .	5
Avaliação da Segurança Contínua . . . . .	5
Melhorias de Segurança no WebSphere Commerce 5.5. . . . .	5
Melhorias de Segurança no WebSphere Commerce 5.4. . . . .	5
Melhorias de Segurança no WebSphere Commerce Suite 5.1 Pro Edition. . . . .	9

### Capítulo 2. Autenticação . . . . . 11

Modelo de Autenticação do WebSphere Commerce . . . . .	11
Mecanismos de Desafio . . . . .	12
Mecanismos de Autenticação . . . . .	13
Registro do Usuário . . . . .	13
Credenciais . . . . .	13
Token do WebSphere Commerce . . . . .	14
WebSphere Application Server Token LTPA. . . . .	14
Sign-on Único . . . . .	14
Diretivas de Autenticação. . . . .	14
Diretivas de Contas. . . . .	15
Outras Diretivas Relacionadas a Autenticação . . . . .	16
Diretivas de Sessão . . . . .	16

### Capítulo 3. Conceitos sobre Autorização . . . . . 17

Modelos de Negócios . . . . .	17
Hierarquia Organizacional . . . . .	18
Organização Raiz . . . . .	18
Organizações (Vendedora) . . . . .	19
Organizações (Compradora) . . . . .	19
Grupos de Diretivas . . . . .	20
Assinatura de Grupo de Diretivas . . . . .	20
Diretiva de Controle de Acesso . . . . .	22
Elementos de uma Diretiva de Controle de Acesso . . . . .	22
Conceitos da Diretiva de Controle de Acesso . . . . .	23
Tipos de Diretivas de Controle de Acesso . . . . .	29

Diretivas Especiais de Controle de Acesso Padrão . . . . .	29
Funções . . . . .	29
Funções Mapeadas para Ferramentas do WebSphere Commerce para Cada Amostra de Loja . . . . .	30
Como o Controle de Acesso Impede Ações não Autorizadas . . . . .	34
Verificando a Autorização antes de Executar uma Ação Iniciada pelo Usuário . . . . .	34
Níveis de Controle de Acesso . . . . .	34
Avaliando as Diretivas de Controle de Acesso . . . . .	37
Hierarquia Organizacional . . . . .	37
Usuários . . . . .	37
Funções . . . . .	37
Grupos de Acesso . . . . .	38
Documentos . . . . .	38
Avaliando Diretivas Padrão Agrupáveis . . . . .	38
Avaliando Diretivas de Gabarito Agrupáveis . . . . .	41
Analisando uma Diretiva em Detalhes . . . . .	42
Exemplo 1: Lendo uma Diretiva . . . . .	43
Exemplo 2: Lendo uma Diretiva em XML . . . . .	45
Exemplo 3: Identificando outras Diretivas Associadas a sua Diretiva. . . . .	46

## Parte 2. Administrando a Autenticação de Segurança . . . . . 49

### Capítulo 4. Aprimorando a Segurança do Site. . . . . 51

Consideração de Segurança para o Servidor Web dos IIS (Internet Information Services) . . . . .	52
Exibições de Segurança . . . . .	52
Tempo Limite de Login . . . . .	53
Invalidação de Senha . . . . .	53
Comandos Protegidos por Senha . . . . .	54
Proteção de Scripts entre Sites . . . . .	55
Ativando o Tempo Limite de Login . . . . .	55
Ativando a Invalidação de Senha . . . . .	56
Ativando os Comandos Protegidos por Senha . . . . .	56
Atualizando os Dados Criptografados . . . . .	57
Ativando a Proteção de Script Entre Sites . . . . .	58
Ativando o Log de Acesso . . . . .	60
Configurando uma Diretiva de Contas . . . . .	61
Configurando uma Diretiva de Senhas . . . . .	62
Configurando uma Diretiva de Bloqueio de Contas . . . . .	63
Lançando uma Verificação de Segurança. . . . .	64
Campo de Encrypt PDI do Configuration Manager . . . . .	65
Diretivas de Autenticação Padrão . . . . .	65
Compradores . . . . .	65
Administradores. . . . .	66

### Capítulo 5. Gerenciamento de Sessões 69

Gerenciamento de Sessão Baseado em Cookies . . . . . 69

Utilizando Cookies para Gerenciamento de Sessão . . . . .	70
Regravação de URL . . . . .	71
Utilizando Gerenciamento de Sessões de Regravação de URL . . . . .	71
Gravando Gabaritos JSP para Regravação de URL	72
Gerenciamento de Sessão em Nível de Loja. . . . .	73

**Capítulo 6. Definindo e Alterando Senhas . . . . . 77**

Referência Rápida para IDs do Usuário, Senhas e Endereços da Web . . . . .	77
Alterando a Senha do Configuration Manager. . . . .	79
Definindo a Senha do Administrador do IBM HTTP Server . . . . .	80
Alterando a Senha do Arquivo de Chaves SSL. . . . .	80
Gerando Senhas Criptografadas para o WebSphere Commerce. . . . .	80
Gerando Senhas Criptografadas para o WebSphere Commerce Payments . . . . .	81
Redefinindo uma Conta de Administrador . . . . .	82

**Capítulo 7. Sign-on Único . . . . . 85**

Pré-requisitos. . . . .	85
Ativando Sign-on Único . . . . .	85
Configurar Funções para Usuários SSO . . . . .	86

**Capítulo 8. Administrando os Certificados X.509 . . . . . 87**

Ativando os Certificados X.509 . . . . .	87
Atualizando o Status de Usuários do Certificado X.509 . . . . .	88
Um Cenário de Autenticação Típico . . . . .	89

**Parte 3. Administrando a Autorização de Segurança . . . . . 91**

**Capítulo 9. Uma Introdução ao Controle de Acesso . . . . . 93**

O Que Significa Controle de Acesso para Você. . . . .	93
---	----

**Capítulo 10. Introdução . . . . . 95**

Definindo as Organizações e os Usuários . . . . .	95
Definindo uma Organização Vendedora . . . . .	96
Definindo uma Organização Compradora . . . . .	97
Compreendendo o Controle de Acesso . . . . .	97
O Que É uma Diretiva de Controle de Acesso?	97
Como Funciona uma Diretiva de Controle de Acesso? . . . . .	98
Como Início a Utilização do Controle de Acesso? . . . . .	99

**Capítulo 11. Personalizando as Diretivas de Controle de Acesso Padrão . . . . . 101**

Identificando as Diretivas Afetadas por uma Alteração . . . . .	101
---	-----

Compreendendo o Relacionamento entre as Diretivas Baseadas em Funções e em Nível de Recurso . . . . .	101
Determinando se uma Diretiva é Baseada em Funções ou em Nível do Recurso. . . . .	105
Diretivas Baseadas em Funções . . . . .	105
Diretivas em Nível do Recurso . . . . .	106
Dicas para Alterar Diretivas Padrão . . . . .	107
Depois de Fazer as Alterações na Diretiva . . . . .	107
Testando as Alterações da Diretiva . . . . .	108
Extraindo as Alterações das Diretivas em Arquivos XML . . . . .	108

**Capítulo 12. Personalizando as Diretivas de Controle de Acesso Utilizando a GUI . . . . . 109**

Cenário 1 de Leilões: Removendo a Capacidade dos Administradores de Leilões para Fechar o Lance do Leilão . . . . .	110
Etapas a Serem Executadas . . . . .	110
Cenário 2 de Leilões: Removendo a Habilidade dos Gerenciadores de Leilão em Retirar Lances . . . . .	111
Etapas a Serem Executadas . . . . .	111
Cenário 3 de Leilões: Limitando o Lance do Leilão aos Compradores . . . . .	112
Etapas a Serem Executadas . . . . .	112
Cenário 1 de Contratos: Remover a Habilidade dos Gerenciadores de Contratos em Adicionar ou Excluir Anexos a Contratos. . . . .	114
Etapas a Serem Executadas . . . . .	114
Cenário 2 de Contratos: Permitir que Operadores e Administradores de Contratos Implementem Contratos. . . . .	115
Etapas a Serem Executadas . . . . .	115
Cenário 1 de Pedidos: Permitindo que Apenas Compradores Criem Pedidos . . . . .	116
Etapas a Serem Executadas . . . . .	117
Cenário 2 de Pedidos: Permitindo que Apenas os Administradores de Comprador Modifiquem os Pedidos . . . . .	118
Etapas a Serem Executadas . . . . .	119
Cenário 3 de Pedidos: Permitindo que Aprovadores RMA Aprovelem todas RMAs . . . . .	120
Etapas a Serem Executadas . . . . .	121
Cenário 1 de Associação: Remover a Capacidade dos Usuários de Auto-Registrarem . . . . .	122
Etapas a Serem Executadas . . . . .	123
Cenário 2 de Associação: Permitindo que Apenas Usuários Registrados e Aprovados Alterem suas Informações de Endereço . . . . .	123
Etapas a Serem Executadas . . . . .	124
Cenário 3 de Associação: Permitindo que os Registradores de Membros Registrem Usuários . . . . .	124
Etapas a Serem Executadas . . . . .	125
Cenário 1 de Cupons: Permitindo que Apenas Compradores Resgatem Cupons . . . . .	127
Etapas a Serem Executadas . . . . .	127

Cenário 2 de Cupons: Permitindo que Administradores de Cupons e Gerenciadores de Operações Criem Promoções com Cupons Eletrônicos . . . . .	129
Etapas a Serem Executadas . . . . .	130
Cenário 1 de Aquisição: Permitindo que os Gerentes de Carrinho de Compras Gerenciem o Carrinho de Compras de Aquisição para Pedidos Criados por sua Organização . . . . .	131
Etapas a Serem Executadas . . . . .	131
Cenário 2 de Aquisição: Permitir Administradores de Compradores de Aquisição a Submeter o Carrinho de Compras de Aquisição para Pedidos Criados por sua Organização . . . . .	132
Etapas a Serem Executadas . . . . .	133
Cenário 1 de Estoque: Permitir que os Gerentes do Centro de Distribuição Atualizem os Centros de Distribuição, Mas Não os Exclua . . . . .	134
Etapas a Serem Executadas . . . . .	134
Cenário de Inventário 2: Permitir Apenas Gerenciadores de Logística, Gerenciadores de Operações e Representantes de Contas para Criar, Atualizar ou Excluir Centros de Distribuição . . . . .	135
Etapas a Serem Executadas . . . . .	135
Cenário 1 Inteligência de Negócios: Permitindo que Auditores Exibam os Relatórios de Inteligência de Negócios . . . . .	136
Etapas a Serem Executadas . . . . .	136

**Capítulo 13. Personalizando as Diretivas de Controle de Acesso Utilizando o XML . . . . . 139**

Alterações que Apenas Podem ser Feitas Editando e Carregando Arquivos XML . . . . .	139
Sobre os Arquivos XML para Controle de Acesso	139
Alterando os Arquivos XML . . . . .	141
Protegendo as Exibições . . . . .	142
Protegendo os Comandos do Controlador . . . . .	145
Protegendo os Recursos . . . . .	152
Protegendo os Beans de Dados . . . . .	153
Agrupando Recursos por Atributos . . . . .	155
Definindo Relacionamentos . . . . .	157
Definindo Grupos de Relacionamentos . . . . .	157
Grupos de Acesso . . . . .	160
Diretivas . . . . .	164
Depois de Alterar os Arquivos XML . . . . .	172
Testando suas Alterações . . . . .	172
Carregando suas Alterações no Banco de Dados	172
Carregando suas Alterações de XML no Banco de Dados . . . . .	173
Extraindo Definições da Diretiva e do Grupo de Acesso do Banco de Dados em seus Arquivos XML . . . . .	174

**Parte 4. Segurança de Pagamentos . . . . . 177**

**Capítulo 14. Acesso ao WebSphere Commerce Payments . . . . . 179**

**Capítulo 15. Mantendo a Segurança do WebSphere Commerce Payments . 181**

Protegendo o WebSphere Commerce Payments . . . . .	181
Protegendo Dados Sensitivos . . . . .	181
Protegendo o Banco de Dados . . . . .	182
Dados da Transação . . . . .	182

**Parte 5. Tópicos Variados sobre Segurança . . . . . 183**

**Capítulo 16. Ativando a Segurança do WebSphere Application Server . . . . 185**

Antes de Iniciar . . . . .	186
Ativando a Segurança com um Registro de Usuário LDAP . . . . .	186
Ativando a Segurança com um Registro de Usuário do Sistema Operacional . . . . .	191
Desativando a Segurança EJB do WebSphere Commerce . . . . .	192
Opções de Implementação de Segurança do WebSphere Commerce . . . . .	193
Configuração de Segurança para o Monitor de Cache Dinâmico . . . . .	194
Administrando Instâncias do WebSphere Commerce Através do Configuration Manager . . . . .	194

**Capítulo 17. Ativando o SSL para Produção com o IBM HTTP Server . . 197**

Sobre Segurança . . . . .	197
Configurando um Arquivo de Chaves de Segurança para Produção . . . . .	197
Solicitando um Certificado Seguro de uma Autoridade de Certificação . . . . .	201
Usuários da Equifax . . . . .	201
Usuários da VeriSign . . . . .	201
Recebendo e Definindo seu Arquivo de Chaves de Produção como o Arquivo de Chaves Atual . . . . .	202
Testando o Arquivo de Chaves de Produção . . . . .	203
Consideração sobre SSL para o WebSphere Commerce Payments . . . . .	203
Melhorando a Confidencialidade . . . . .	203
Ativando o SSL no IBM HTTP Server (iSeries) . . . . .	204
Utilizando o SSL com o WebSphere Commerce Payments . . . . .	204

**Capítulo 18. Ativando o SSL para o IBM Directory Server (LDAP). . . . . 207**

Configurando o IBM Directory Server . . . . .	207
Configurando o IBM OS/400 Directory Services na Plataforma iSeries . . . . .	207
Atribuindo e Importando um Certificado Auto Assinado ao WebSphere Application Server . . . . .	208
WebSphere Application Server . . . . .	209
WebSphere Commerce . . . . .	210

**Parte 6. Apêndices . . . . . 211**

**Apêndice. Diretivas e Grupos de Controle de Acesso Padrão . . . . . 213**

Diretivas de Controle de Acesso Padrão . . . . . 213  
Diretivas Baseadas em Funções . . . . . 214  
Diretivas em Nível do Recurso por Área de Negócios . . . . . 217

Grupos de Diretivas de Controle de Acesso Padrão 226

**Avisos . . . . . 227**

Licença de Copyright. . . . . 229  
Marcas Comerciais . . . . . 229



---

## Sobre este Manual

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

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

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

### Importante

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

---

## Resumo das Alterações

Este Guia de Segurança e qualquer versão atualizada desse, estarão disponíveis na Página da Web da Biblioteca Técnica do WebSphere Commerce (<http://www.ibm.com/software/commerce/library/>). Para obter informações adicionais da edição do WebSphere Commerce, consulte as páginas de visão geral:

- Business Edition ([http://www.ibm.com/software/webservers/commerce/wc\\_be/](http://www.ibm.com/software/webservers/commerce/wc_be/))
- Professional Edition ([http://www.ibm.com/software/commerce/wscom/support/wc\\_pe/](http://www.ibm.com/software/commerce/wscom/support/wc_pe/))

Para obter informações de suporte adicionais, consulte a Página de Suporte do WebSphere Commerce (<http://www.ibm.com/software/commerce/support/>).

Para obter informações sobre as últimas alterações feitas no produto, consulte o arquivo READ-ME atualizado do produto, também disponível no Web site acima.

Todas as atualizações deste manual serão resumidas nesta seção.

---

## Navegando por este Manual

Este documento está dividido nas seguintes partes:

- A Parte 1, “Conceitos de Segurança do WebSphere Commerce”, na página 1 discute o modelo de segurança do WebSphere Commerce e fornece uma visão geral conceitual da segurança do WebSphere Commerce. Ela será de interesse daqueles que desejam uma visão geral da segurança do WebSphere Commerce para planejar a segurança em um site do WebSphere Commerce.
- A Parte 2, “Administrando a Autenticação de Segurança”, na página 49 discute as tarefas de administração do WebSphere Commerce referentes à segurança do


site. Esta parte será de interesse daqueles que executam as tarefas de administração relacionadas à segurança do site.

- A Parte 3, “Administrando a Autorização de Segurança”, na página 91 discute as tarefas de autorização do WebSphere Commerce referentes ao controle de acesso. Esta parte será de interesse daqueles que executam as tarefas de autorização de sistema referentes ao controle de acesso no WebSphere Commerce.
- A Parte 4, “Segurança de Pagamentos”, na página 177 discute as tarefas de administração do WebSphere Commerce referentes à segurança do WebSphere Commerce Payments. Esta parte será de interesse daqueles que administram WebSphere Commerce Payments.
- A Parte 5, “Tópicos Variados sobre Segurança”, na página 183 discute as várias tarefas de administração do sistema WebSphere Commerce, como a melhoria da segurança do WebSphere Application Server. Esta parte será de interesse dos administradores do sistema responsáveis pela segurança.

---

## Convenções Utilizadas neste Manual

Este manual utiliza as seguintes convenções de destaque:

<b>Negrito</b>	Indicam comandos ou controles GUI (Interface Gráfica com o Usuário) tais como nomes ou campos, ícones ou opções de menu.
Fonte Monoespaçada	Indica exemplos de texto que você digita exatamente como exibido, nomes de arquivos e caminhos e nomes de diretórios.
<i>Itálico</i>	Utilizados para enfatizar palavras. Itálico também indica nomes que devem ser substituídos pelos valores apropriados para seu sistema.
<i>host_name</i>	O nome completo do host de seu servidor WebSphere Commerce (por exemplo, server.mydomain.ibm.com está completo).
<i>instance_name</i>	O nome da instância WebSphere Commerce com a qual você está trabalhando.
 Windows	A letra representando a unidade na qual você instalou o produto ou o componente que está sendo discutido (por exemplo, C:).
<i>unidade</i>	



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

---

### Importante

Estas seções destacam informações especialmente importantes.

### Atenção

Estas seções destacam informações que visam proteger seus dados.

 **Business** indica informações específicas ao WebSphere Commerce Business Edition.

**Professional** indica informações específicas ao WebSphere Commerce Professional Edition.

**AIX** indica as informações específicas para WebSphere Commerce para AIX.

**400** indica informações específicas do WebSphere Commerce para o IBM @server iSeries 400 (anteriormente chamado de AS/400)

**Linux** indica informações específicas ao WebSphere Commerce para Linux.

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

**Windows** indica informações específicas para WebSphere Commerce para Windows 2000.

## Variáveis de Caminho

Este guia utiliza as seguintes variáveis para representar os caminhos de diretórios:

### *DB2\_installdir*

Essa variável representa o diretório de instalação real do DB2 Universal Database em sua máquina. Os seguintes são os diretórios de instalação padrão para o DB2 Universal Database em vários sistemas operacionais:

<b>AIX</b>	/usr/lpp/db2_08_01
<b>400</b>	Não aplicável (instalado como parte do sistema operacional)
<b>Linux</b>	/opt/IBM/db2/V8.1
<b>Solaris</b>	/opt/IBM/db2/V8.1
<b>Windows</b>	C:\Arquivos de Programas\WebSphere\sql1lib

### *HTTPServer\_installdir*

Essa variável representa o diretório de instalação real do IBM HTTP Server em sua máquina. Os seguintes são os diretórios de instalação padrão do IBM HTTP Server em vários sistemas operacionais:

<b>AIX</b>	/usr/IBMHttpServer
<b>400</b>	Não aplicável (instalado como parte do sistema operacional)
<b>Linux</b>	/opt/IBMHttpServer
<b>Solaris</b>	/opt/IBMHttpServer
<b>Windows</b>	C:\Arquivos de Programas\WebSphere\IBMHTTPServer

### *Oracle\_installdir*

Essa variável representa o diretório de instalação real do Oracle em sua máquina. Os seguintes são os diretórios de instalação padrão do Oracle em vários sistemas operacionais:

<b>AIX</b>	/oracle/u01/app/oracle/product/9.2.0
------------	--------------------------------------

▶ 400	Não aplicável ao OS/400.
▶ Linux	Não aplicável para Linux
▶ Solaris	/opt/oracle/u01/app/oracle/product/9.2.0
▶ Windows	C:\oracle\ora91

### *WAS\_installdir*

Essa variável representa o diretório de instalação real do WebSphere Application Server em sua máquina. Os seguintes são os diretórios de instalação padrão para o WebSphere Application Server em vários sistemas operacionais:

▶ AIX	/usr/WebSphere/AppServer
▶ 400	/QIBM/ProdData/WebAS5/Base
▶ Linux	/opt/WebSphere/AppServer
▶ Solaris	/opt/WebSphere/AppServer
▶ Windows	C:\Arquivos de Programas\WebSphere\AppServer

### *WAS\_userdir*

▶ 400 Esta variável representa o diretório para todos os dados que é utilizado pelo WebSphere Application Server, que pode ser modificado ou precisa ser configurado pelo usuário, em uma máquina do iSeries. O padrão desse diretório é:

▶ 400	/QIBM/UserData/WebAS5/Base/ <i>WAS_instance_name</i>
-------	--

### *WC\_installdir*

Essa variável representa o diretório de instalação real do WebSphere Commerce em sua máquina. Os seguintes são os diretórios de instalação padrão para o WebSphere Commerce em vários sistemas operacionais:

▶ AIX	/usr/WebSphere/CommerceServer55
▶ 400	/QIBM/ProdData/CommerceServer55
▶ Linux	/opt/WebSphere/CommerceServer55
▶ Solaris	/opt/WebSphere/CommerceServer55
▶ Windows	C:\Arquivos de Programas\WebSphere\CommerceServer55

### *WC\_userdir*

▶ 400 Esta variável representa o diretório para todos os dados que é utilizado pelo WebSphere Commerce, que pode ser modificado ou precisa ser configurado pelo usuário em um sistema iSeries. O padrão desse diretório é:

▶ 400	/QIBM/UserData/CommerceServer55
-------	---------------------------------

---

## **Parte 1. Conceitos de Segurança do WebSphere Commerce**

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



---

# Capítulo 1. Introdução ao Modelo de Segurança do WebSphere Commerce

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

---

## Visão Geral

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

### O que é Autenticação?

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

O sistema WebSphere Commerce possui suas próprias senhas para propósitos de administração. Essas senhas devem ser alteradas periodicamente como parte de uma diretiva de segurança em todo o site do WebSphere Commerce. Para obter detalhes sobre como alterar as senhas do sistema WebSphere Commerce, consulte o Capítulo 6, "Definindo e Alterando Senhas", na página 77.

### O que é Autorização?

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

- Para proteger o Enterprise JavaBeans (EJB beans) do WebSphere Commerce contra acesso não autorizado. Esse processo é discutido no Capítulo 16, "Ativando a Segurança do WebSphere Application Server", na página 185.
- Para assegurar que somente partes autorizadas podem executar grupos diferentes de comandos do WebSphere Commerce. Esse processo é discutido na seção em "Controle de Acesso" no documento *WebSphere Commerce Programming Guide and Tutorials*.

### O que são Diretivas de Controle de Acesso?

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

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

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

O modelo de autorização para WebSphere Commerce é baseado na coação das diretivas de controle de acesso. As diretivas de controle de acesso são aplicadas pelo Gerenciador de Diretivas de controle de acesso. Em geral, quando um usuário tenta acessar um recurso que pode ser protegido, o gerenciador de diretivas de controle de acesso primeiro determina quais diretivas de controle de acesso são aplicáveis para esse usuário e, em seguida, com base nas diretivas de controle de acesso aplicáveis, determina se o usuário pode executar a operação solicitada no recurso especificado.

## O que é uma Trilha de Auditoria?

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

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

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

## O que é confidencialidade?

Confidencialidade é o processo de proteger informações sensíveis de serem decifradas por destinatários involuntários. No sistema WebSphere Commerce, a confidencialidade é necessária quando informações sensíveis fluem do navegador do usuário para o servidor WebSphere Commerce, bem como do servidor WebSphere Commerce para o navegador do usuário. Conforme discutido no Capítulo 17, "Ativando o SSL para Produção com o IBM HTTP Server", na página 197, ou uso do SSL fornece confidencialidade para esse cenário.



A confidencialidade é também um requisito forte na área de gerenciamento de sessões. Como o protocolo HTTP (Hypertext Transfer Protocol) não tem informações de estado, um *cookie* é comumente utilizado para identificar continuamente o usuário ao servidor WebSphere Commerce. Se o cookie for roubado, então a conta do usuário ficará comprometida. Isso normalmente é conhecido como *pirataria de sessão*. O WebSphere Commerce impede que a pirataria de sessão utilize recursos exclusivos das especificações de cookie, conforme discutido no Capítulo 5, “Gerenciamento de Sessões”, na página 69.

---

## Considerações Gerais sobre Segurança

### Avaliação da Segurança Contínua

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

### Melhorias de Segurança no WebSphere Commerce 5.5

WebSphere Commerce 5.5 adicionou a assinatura de grupos de diretivas à infra-estrutura de controle de acesso.

No WebSphere Commerce 5.4, uma diretiva era aplicada a recursos pertencentes aos descendentes do proprietário da diretiva. Se organizações diferentes na mesma hierarquia de organizações desejassem níveis diferentes de controle de acesso, o alcance dos níveis diferentes poderia ser difícil. Além disso, se a hierarquia de organizações fosse muito complexa, a compreensão de todas as diretivas aplicadas a uma organização próxima à base da hierarquia poderia ser confusa.

Para facilitar as coisas e torná-las mais explícitas no WebSphere Commerce 5.5, as diretivas foram primeiro agrupadas em grupos de diretivas, com base nos requisitos de negócios e de controle de acesso. Por exemplo, um grupo de diretivas teria as diretivas necessárias para suportar contratos, enquanto o outro teria apenas os usuários registrados para compra. Então, dependendo dos requisitos de negócios e controle de acesso de uma organização, esta assinaria explicitamente os grupos de diretivas adequados. Quando uma organização assina os grupos de diretivas, apenas as diretivas nesses grupos serão aplicadas aos recursos da organização. As diretivas das organizações anteriores não se aplicarão. No entanto, se uma organização não assinar explicitamente os grupos de diretivas, ela herdará a assinatura de diretivas de sua ancestral mais próxima que está assinando.

Para obter uma visão geral desses grupos, consulte a seção sobre “Grupos de Diretiva” no Capítulo 3, “Conceitos sobre Autorização”, na página 17.

### Melhorias de Segurança no WebSphere Commerce 5.4

A seguinte seção lista os aperfeiçoamentos de segurança no WebSphere Commerce 5.4 relacionados ao WebSphere Commerce Suite 5.1 e retidos no WebSphere Commerce 5.5. A maioria desses aprimoramentos foram feitas no release WebSphere Commerce Business Edition 5.1. Eles são geralmente aplicáveis ao:

- Administrador do site do WebSphere Commerce;

- Administrador do sistema;
- Desenvolvedor do WebSphere Commerce.

Observe que às vezes essas funções são alternadas.

## Melhorias para o Administrador do Site

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

### Controle de acesso

- **Estrutura de Controle de Acesso** — Um aperfeiçoamento chave é que uma nova estrutura de controle de acesso foi implementada no WebSphere Commerce 5.4 e retida no WebSphere Commerce 5.5 (juntamente com o aperfeiçoamento do grupo de diretivas no WebSphere Commerce 5.5). Essa nova estrutura utiliza as diretivas de controle de acesso para determinar se um determinado usuário pode executar uma ação específica em um recurso determinado. A nova estrutura de controle de acesso fornece controle de acesso minucioso. Ela funciona em conjunto, mas não substitui o controle de acesso fornecido pelo WebSphere Application Server. A nova estrutura de controle de acesso está descrita em detalhes no Parte 3, “Administrando a Autorização de Segurança”, na página 91.

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

#### Ela é expressiva...

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

#### Ela é hierárquica...

As diretivas de controle de acesso pertencem aos grupos de diretiva. Os grupos de diretiva aos quais uma organização se associa por meio de assinatura também podem ser aplicados implicitamente a suas suborganizações.

#### Ela é personalizável...

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

#### Ela é compacta...

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

- **Script entre sites** — Rejeite qualquer pedido de usuário que contenha atributos ou caracteres designados como não permitidos, utilizando o nó Proteção de Script Entre Sites do WebSphere Commerce Configuration Manager. Está descrito em detalhes no Capítulo 4, “Aprimorando a Segurança do Site”, na página 51.

### Autenticação

- **Armazenamento de senha** — O WebSphere Commerce criptografa e armazena um hash de senhas de uma via utilizando o esquema de hash

SHA-1 no banco de dados do WebSphere Commerce, em vez de armazenar as próprias senhas. Isso assegura que as senhas do usuário não sejam decifradas por outra pessoa, incluindo o administrador do site ou do sistema.

- **Invalidação de Senha** — Solicite aos usuários que alterem suas senhas quando estiverem efetuando login no sistema pela primeira vez, utilizando o nó Invalidação de Senha do WebSphere Commerce Configuration Manager. Está descrito em detalhes no Capítulo 4, “Aprimorando a Segurança do Site”, na página 51.
- **Diretiva de contas** — Configure uma diretiva de contas para o site para definir as diretivas relacionadas às contas em uso, utilizando a página Diretiva de contas do WebSphere Commerce Administration Console. Está descrito em detalhes no Capítulo 4, “Aprimorando a Segurança do Site”, na página 51.
- **Diretiva de senhas** — Configure uma diretiva de senha para o site para controlar as características de seleção de senha de um usuário utilizando a página Diretiva de senhas do WebSphere Commerce Administration Console. Está descrito em detalhes no Capítulo 4, “Aprimorando a Segurança do Site”, na página 51.
- **Diretiva de bloqueio de contas** — Configure uma diretiva de bloqueio de contas para o site para reduzir as chances de uma conta de usuário ficar comprometida utilizando a página Diretiva de bloqueio de contas do WebSphere Commerce Administration Console. Está descrito em detalhes no Capítulo 4, “Aprimorando a Segurança do Site”, na página 51.

#### **Autorização**

**Comandos protegidos por senha** — Solicite aos usuários que digitem suas senhas se estiverem executando pedidos que executam comandos designados, utilizando o nó Comandos Protegidos por Senha do WebSphere Commerce Configuration Manager. Está descrito em detalhes no Capítulo 4, “Aprimorando a Segurança do Site”, na página 51.

#### **Dados criptografados**

**Ferramenta de atualização de banco de dados** — Atualize dados criptografados, como senhas e informações do cartão de crédito bem como chave do comerciante em um banco de dados do WebSphere Commerce, utilizando o nó Ferramenta de Atualização de Banco de Dados do WebSphere Commerce Configuration Manager. Está descrito em detalhes no Capítulo 4, “Aprimorando a Segurança do Site”, na página 51.

#### **Gerenciamento de sessões**

**Tempo limite de login** — Efetue logoff para um usuário que está inativo por um período de tempo estendido e peça que ele efetue logon novamente no sistema, utilizando o nó Tempo Limite de Login. Esse aprimoramento é chamado através do WebSphere Commerce Configuration Manager e está descrito em detalhes no Capítulo 4, “Aprimorando a Segurança do Site”, na página 51.

#### **Log de acesso**

**Log de acesso** — identifica rapidamente qualquer ameaça de segurança contra o WebSphere Commerce ativando o log de acesso. Esse aprimoramento é chamado através do WebSphere Commerce Configuration Manager e está descrito em detalhes no Capítulo 4, “Aprimorando a Segurança do Site”, na página 51.

## Melhorias para o Administrador do Sistema

A seguir, são aperfeiçoamentos de segurança feitos no WebSphere Commerce 5.4 e retidos no WebSphere Commerce 5.5 que geralmente são direcionados a um administrador do site:

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

## Melhorias para o Programador do WebSphere Commerce

Um aperfeiçoamento importante é que uma nova estrutura de controle de acesso foi implementada no WebSphere Commerce 5.4 e retida no WebSphere Commerce 5.5. Essa estrutura utiliza as diretivas de controle de acesso para determinar se um usuário específico tem permissão para executar uma ação específica em um determinado recurso. A nova estrutura de controle de acesso fornece controle de acesso minucioso. Ela funciona em conjunto, mas não substitui o controle de acesso fornecido pelo WebSphere Application Server. A nova estrutura de controle de acesso está descrita em detalhes no Parte 3, “Administrando a Autorização de Segurança”, na página 91.

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

### Ela é expressiva...

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

### Ela é hierárquica...

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

### Ela é personalizável...

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

### Ela é compacta...

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

Para obter informações adicionais sobre considerações de segurança para programadores, consulte o documento *WebSphere Commerce Programming Guide and Tutorials*.

## Melhorias de Segurança no WebSphere Commerce Suite 5.1 Pro Edition

Embora o Commerce Suite 5.1 representasse uma nova arquitetura de e-commerce e fosse uma nova escrita completa do Commerce Suite 4.1 baseado em C++, ele continha todos os recursos de segurança de versões anteriores do WebSphere Commerce Suite, mais os novos aprimoramentos de segurança incluídos. Esses aprimoramentos foram herdados pelo WebSphere Commerce 5.5.

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

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

### Melhorias de Segurança Gerais

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

O algoritmo DES Triplo (padrão de criptografia de dados) padrão na indústria foi utilizado para proteger informações sensíveis no sistema WebSphere Commerce. O pacote que contém o algoritmo DES Triplo é sinalizado digitalmente de forma que se ele tiver sido violado o servidor WebSphere Commerce não poderá ser iniciado. Esses aperfeiçoamentos foram retidos no WebSphere Commerce 5.5.

### Gerenciamento de Sessões

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

### Autenticação

As senhas do sistema e do aplicativo necessárias para o servidor WebSphere Commerce durante a execução foram seguramente criptografadas, utilizando-se uma chave de 128 bits especificada por um comerciante e armazenada nos arquivos de configuração do WebSphere Commerce. As informações sensíveis que aparecem na caixa de entrada de URL dos usuários, foram criptografadas para proteger compradores contra divulgação não autorizada.

### Log

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



---

## Capítulo 2. Autenticação

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

---

### Modelo de Autenticação do WebSphere Commerce

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

- Mecanismos de Desafio
- Mecanismos de Autenticação
- Registro de Usuários

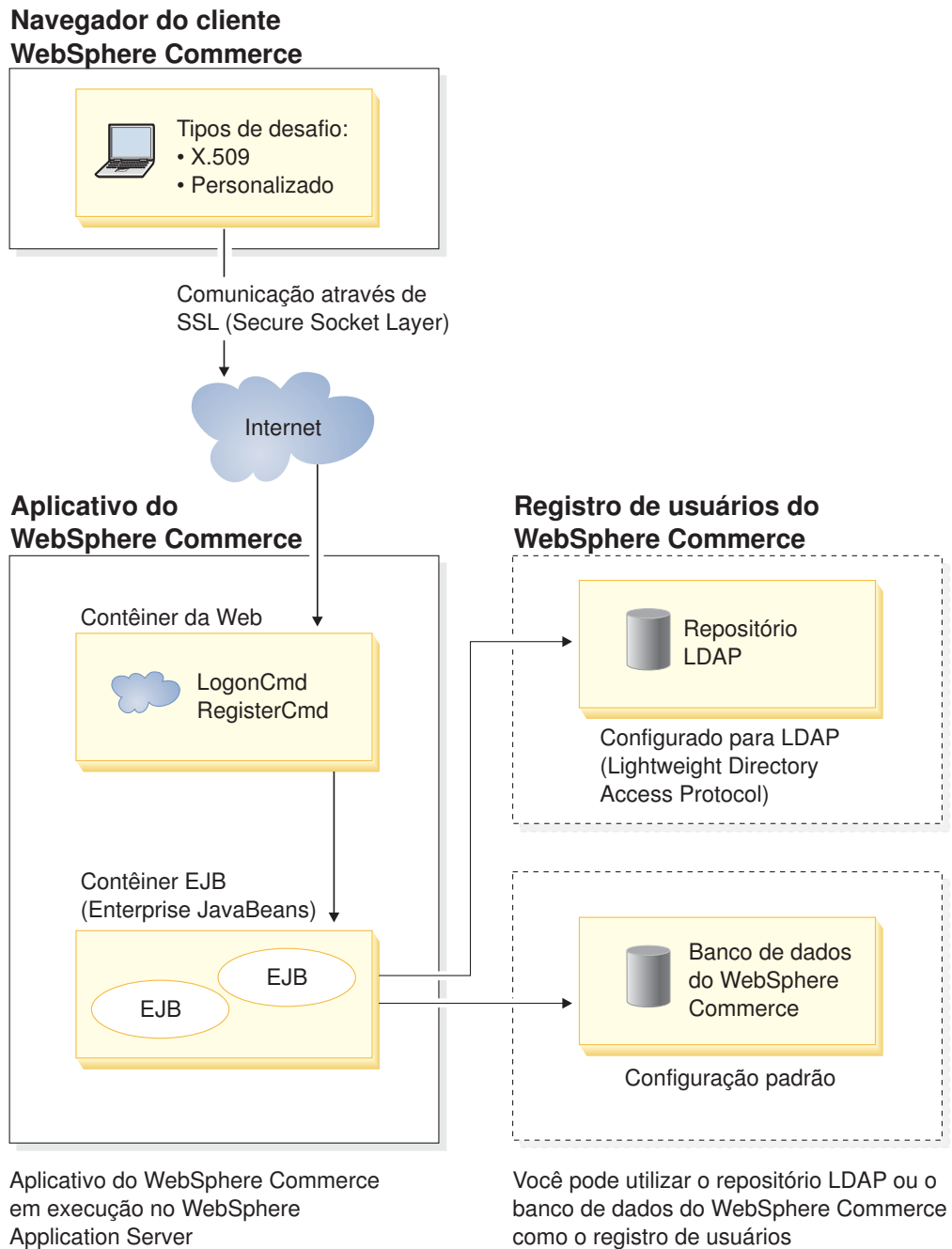


Figura 1. Modelo de Segurança do WebSphere Commerce

## Mecanismos de Desafio

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

### Autenticação baseada em formulário ou personalizada

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



### Autenticação baseada em certificado (certificado X.509)

O mecanismo de desafio de certificado indica que o servidor Web seja configurado para executar autenticação mútua através do SSL. O cliente precisa apresentar um certificado para estabelecer a conexão. Esse certificado é então mapeado para um registro do usuário.

## Mecanismos de Autenticação

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

### Validação de Certificado

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

### Ligação LDAP

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

### Ligação de Bancos de Dados

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

## Registro do Usuário

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

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

O WebSphere Commerce suporta os seguintes provedores LDAP:

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

---

## Credenciais

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

## Token do WebSphere Commerce

O WebSphere Commerce utiliza um cookie de autenticação seguro para gerenciar os dados de autenticação. Um cookie de autenticação somente flui sobre o SSL e recebe uma marca de tempo para segurança máxima. Este cookie é utilizado para autenticar o usuário dentro das conexões SSL sempre que um comando com distinção de maiúsculas e minúsculas for executado, por exemplo oDoPaymentCmd, que pede o número do cartão de crédito do usuário. Há um risco mínimo de que esse cookie seja roubado e utilizado por um usuário não autorizado.

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

## WebSphere Application Server Token LTPA

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

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

---

## Sign-on Único

A filosofia por trás da conexão única do HTTP é preservar a autenticação do usuário para diferentes aplicativos da Web. Seu objetivo é: evitar solicitar várias vezes ao usuário as credenciais de segurança de um determinado domínio de segurança que inclui:

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

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

Para obter as etapas para implementação de sign-on único com o WebSphere Commerce, consulte Capítulo 7, "Sign-on Único", na página 85.

---

## Diretivas de Autenticação

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

## Diretivas de Contas

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

### Diretiva de contas

A página Diretiva de contas do WebSphere Commerce Administration Console permite configurar uma diretiva de contas. Uma diretiva de conta define as diretivas relacionadas à conta, como diretivas de bloqueio de senha e de conta.

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

Para obter informações sobre a criação de diretivas de contas, consulte o “Configurando uma Diretiva de Contas” na página 61.

Consulte também o tópico de referência “Diretivas de Autenticação Padrão” na ajuda on-line do WebSphere Commerce.

### Diretiva de Bloqueio de Contas

A página Diretiva de bloqueio de conta do WebSphere Commerce Administration Console permite configurar uma diretiva de bloqueio de conta para diferentes funções do usuário dentro do WebSphere Commerce. A diretiva de bloqueio de contas desativará uma conta de usuário, se ações maliciosas forem ativadas junto a essa conta, para reduzir as chances que as ações comprometem a conta.

A diretiva de bloqueio de contas aplica os seguintes itens:

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

Para obter informações sobre a criação de diretivas de bloqueio de contas, consulte o “Configurando uma Diretiva de Bloqueio de Contas” na página 63.

### Diretiva de Senha

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

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

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

Para obter informações sobre a criação de diretivas de senhas, consulte o “Configurando uma Diretiva de Senhas” na página 62.

Consulte também o tópico de referência “Diretivas de Autenticação Padrão” na ajuda on-line do WebSphere Commerce.

## Outras Diretivas Relacionadas a Autenticação

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

### Invalidação de Senha

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

Para obter informações sobre o nó Invalidação de Senha, consulte “Ativando a Invalidação de Senha” na página 56.

### Comandos Protegidos por Senha

Utilize o nó Comandos Protegidos por Senha do Configuration Manager para ativar ou desativar o recurso de comandos protegidos por senha. Quando esse recurso é ativado, o WebSphere Commerce requer que os usuários registrados que estejam com logon no WebSphere Commerce informem suas senhas antes de continuar um pedido que executa comandos designados do WebSphere Commerce.

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

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

Para obter informações sobre a utilização do nó Comandos Protegidos por Senha, consulte “Ativando os Comandos Protegidos por Senha” na página 56.

## Diretivas de Sessão

No WebSphere Commerce as diretivas de sessão são incorporadas na diretiva de tempo limite de login.

Com a diretiva de tempo limite de login, o WebSphere Commerce efetuará logoff de um usuário que está inativo por um longo período de tempo e solicitará que ele efetue logon no sistema utilizando o nó Tempo Limite de Login. Esse aprimoramento é chamado através do WebSphere Commerce Configuration Manager e está descrito em detalhes em “Ativando o Tempo Limite de Login” na página 55.

---

## Capítulo 3. Conceitos sobre Autorização

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

A autorização ou o controle de acesso, no WebSphere Commerce é realizado utilizando-se diretivas de controle de acesso. Uma diretiva 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 diretivas de controle de acesso padrão. Essas diretivas 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.

---

### Modelos de Negócios

No WebSphere Commerce 5.4, depois de criar sua instância, o Administrador do Site tinha que tomar as seguintes decisões:

1. A estrutura organizacional apropriada para o site
2. As funções a serem atribuídas a determinadas organizações
3. As diretivas de controle de acesso que seriam necessárias

Após essas decisões, a loja podia ser publicada junto a organização apropriada.

No WebSphere Commerce 5.5, este processo foi simplificado pela criação de modelos de negócios. Um modelo de negócios fornece a estrutura da organização, funções, diretivas de controle de acesso e lojas predefinidas que são desejadas em uma solução específica de e-commerce. Os modelos de negócios podem ser utilizados como o estágio de desenvolvimento como uma base, à qual o conteúdo pode ser adicionado, excluído ou alterado.

Os seguintes modelos de negócios estão disponíveis com o WebSphere Commerce 5.5:

- Direto ao consumidor
- Direto ao B2B
- Cadeia de demanda
- Hospedagem
- Cadeia de fornecimento

Para entender os modelos de negócios e o componente de controle de acesso do WebSphere Commerce, primeiro você deve entender a hierarquia organizacional típica de um site de e-commerce.

**Nota:** Para obter informações adicionais sobre modelos de negócios, consulte o *WebSphere Commerce Fundamentals*.

## 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 vendedora e várias organizações compradoras; 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 vendedora, cada suborganização 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.

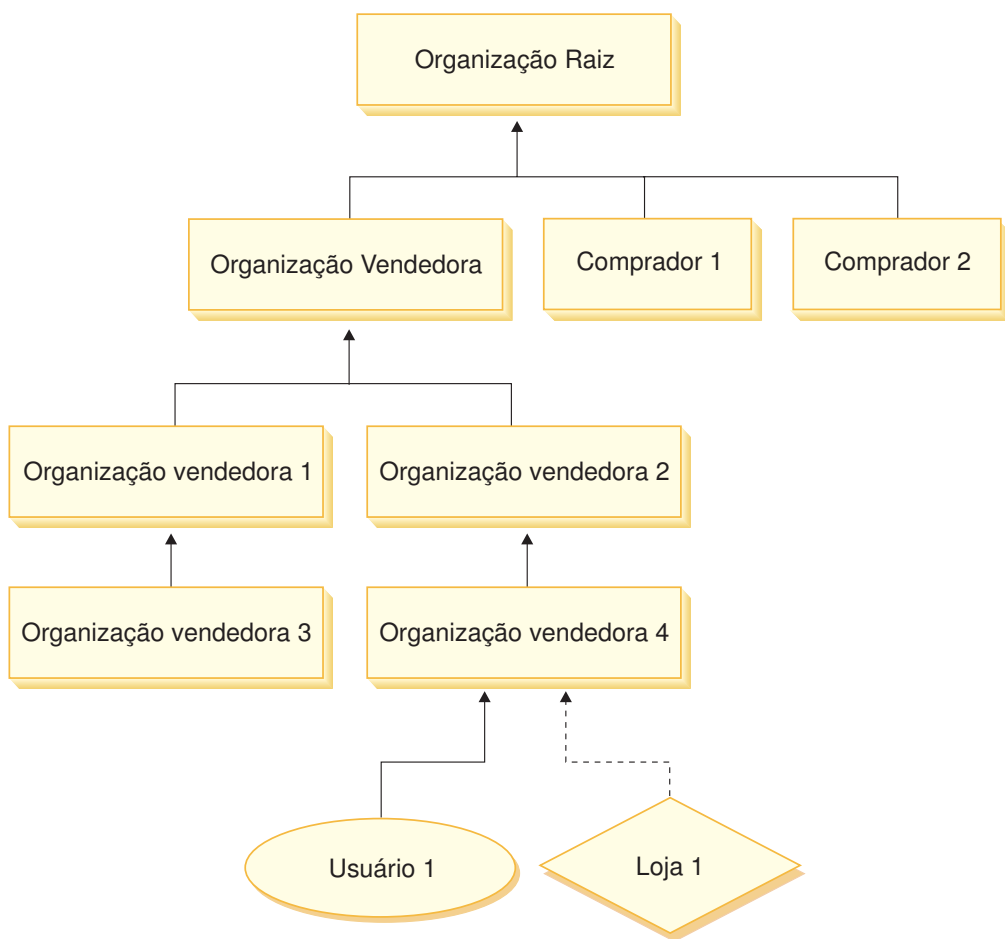


Figura 2. Hierarquia Organizacional de um Site de Business-to-Business

### Organização Raiz

A organização raiz fica na parte superior da hierarquia organizacional. Um Administrador do Site possui acesso de superusuário para executar qualquer operação no 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 às 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 vendedora. Em um site de business-to-business, também há uma ou mais organizações compradoras. O Administrador do Site pode definir as diretivas de controle de acesso da organização vendedora (que possui a loja), bem como as diretivas de controle de acesso de cada organização que compra da loja. Em um site de business-to-consumer, não há organizações compradoras. Os clientes de business-to-consumer são modelados como membros da organização padrão.

## Organizações (Vendedora)

Nos sites de business-to-business e de business-to-consumer, o Administrador do Site cria um vendedor no nível superior. Sob essa organização vendedora, 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 diretivas de controle de acesso especiais para uma organização vendedora e atribui um Administrador da Vendedora para gerenciar essa organização. O Administrador da Vendedora registra usuários e atribui a eles funções diferentes para ajustar as necessidades de negócio da organização, de acordo com as diretivas de controle de acesso pertencentes a essa organização.

As responsabilidades do Administrador da Vendedora são resumidas desta forma:

- Crie suborganizações 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 suborganizações.
- Crie usuários.
- Atribua funções a usuários.

## Organizações (Compradora)

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

As responsabilidades do Administrador da compradora são resumidas desta forma:

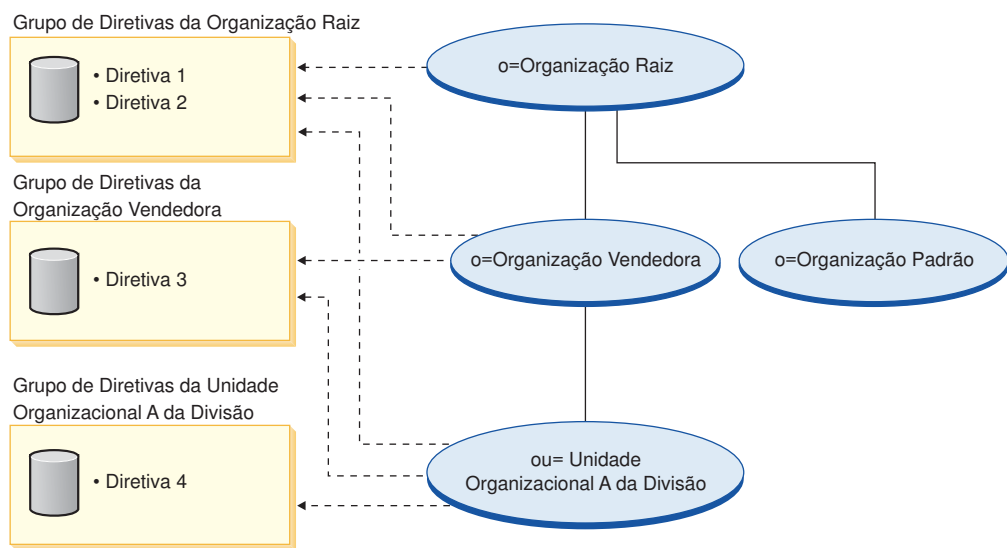
- Criar e administrar suborganizações dentro de uma organização compradora. Opcionalmente, defina quais processos na organização requerem aprovação. Essa etapa é necessária somente em um site business-to-business.

- Atribua funções às suborganizações.
- Crie usuários.
- Atribua funções a usuários.

**Nota:** Observe que o Administrador do Site pode modificar e gerenciar as diretivas de controle de acesso da organização compradora, se adequado. Para obter informações adicionais sobre as tarefas do Administrador do Site, consulte a ajuda on-line do WebSphere Commerce.

## Grupos de Diretivas

O WebSphere Commerce 5.5 suporta vários modelos de negócios e cada um desses modelos possui seu próprio conjunto de diretivas de controle de acesso. Para agrupar os conjuntos de diretivas nos modelos, foram criados grupos de diretivas. As diretivas são atribuídas explicitamente a grupos de diretivas apropriados e, em seguida, as organizações podem assinar um ou mais desses grupos. Por exemplo, no diagrama a seguir, a Organização Vendedora é assinante do Grupo de Diretivas da Organização Vendedora e do Grupo de Diretivas da Organização Raiz.



As diretivas são atribuídas aos grupos de diretivas. Por exemplo, no diagrama anterior, a Diretiva 1 e a Diretiva 2 são atribuídas ao Grupo de Diretivas da Organização Raiz, a Diretiva 3 é atribuída ao Grupo de Diretivas da Organização Vendedora e a Diretiva 4 é atribuída ao Grupo de Diretivas da Unidade Organizacional A da Divisão.

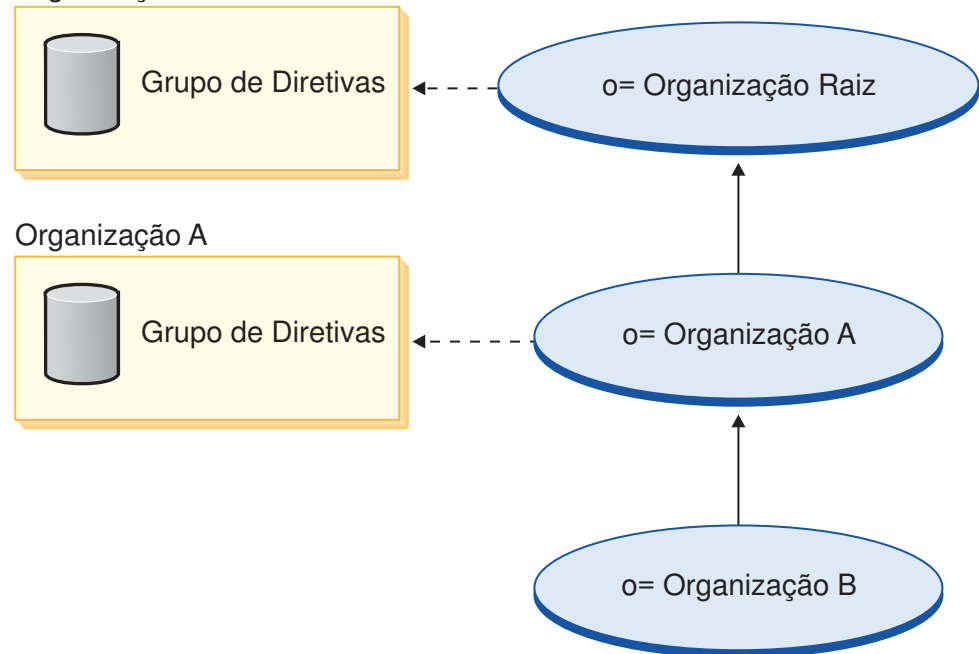
## Assinatura de Grupo de Diretivas

Em versões anteriores do WebSphere Commerce, uma diretiva aplicada a todos os recursos pertencentes aos descendentes da organização proprietária dessa diretiva. Por exemplo, se a Organização A tinha uma determinada diretiva e era pai da Organização B, então a Organização B, implicitamente, também tinha essa diretiva. No WebSphere Commerce 5.5, as organizações agora podem ser assinantes de grupos de diretivas. No WebSphere Commerce 5.5, se a Organização B não for assinante de nenhum dos grupos de diretivas, a estrutura de controle de acesso começará pesquisando a hierarquia de organizações até encontrar uma organização que seja assinante de pelo menos um grupo de diretivas. Se a organização pai imediata da Organização B, Organização A, for assinante de um grupo de diretivas, a pesquisa será parada e as diretivas serão aplicadas às Organizações A e



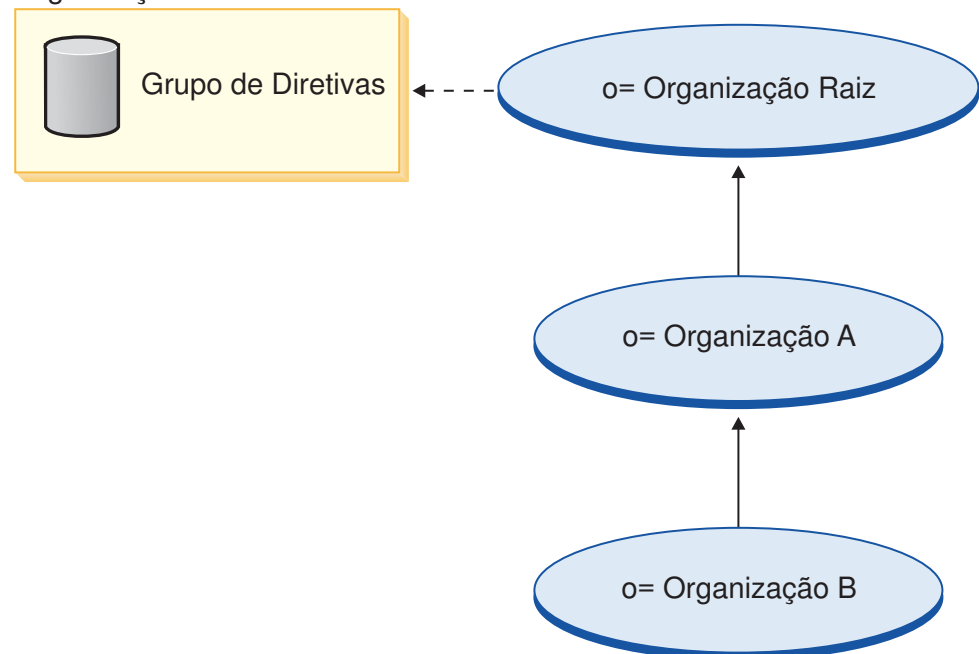
B. Isso pode ser visto no diagrama a seguir.

Organização Raiz



Se a Organização A não for assinante de um grupo de diretivas, a pesquisa continuará até a hierarquia de organizações, até que seja encontrada uma organização com uma assinatura. Isso é visto no diagrama a seguir, no qual a Organização Raiz é assinante de um grupo de diretivas. As diretivas nesse grupo se aplicam à Organização B e à Organização A.

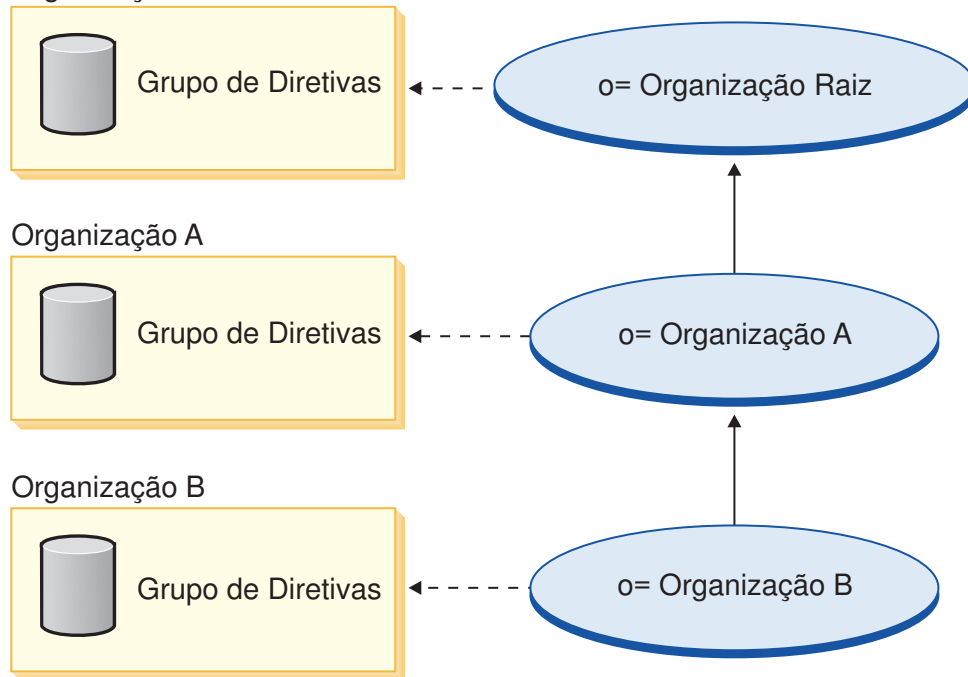
Organização Raiz



Se a Organização B for assinante de um grupo de diretivas, a pesquisa será parada na Organização B. Portanto, apenas as diretivas no grupo de diretivas da

Organização B serão aplicadas à Organização B.

Organização Raiz



---

## Diretiva de Controle de Acesso

Uma diretiva 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 diretivas de controle de acesso, os usuários não têm acesso a nenhuma das funções do sistema. Para compreender as diretivas 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 Diretiva de Controle de Acesso

Uma diretiva de controle de acesso consiste em quatro elementos:

#### Grupo de Acesso

O grupo de usuários ao qual a diretiva se aplica.

#### Grupo de Ações

Um grupo de ações executadas pelo usuário nos recursos.

#### Grupo de Recursos

Os recursos controlados pela diretiva. 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 diretiva 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 Diretiva de Controle de Acesso

As diretivas 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 diretivas de controle de acesso, os usuários não têm acesso a nenhuma das funções de seu site.

Cada diretiva de controle de acesso tem o seguinte formato:

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

Os elementos na diretiva 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 aos tipos de grupos 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 diretiva 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 adicionar 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 da Vendedora e um grupo de acesso correspondente chamado Administradores da Vendedora. Um Administrador do Site utiliza o WebSphere Commerce Administration Console para criar, manter e excluir grupos de acesso para um site. Um Administrador do Site, Administrador da Compradora, Administrador da Vendedora ou Gerenciador de Canais utiliza o WebSphere Commerce Organization Administration Console para atribuir funções a usuários ou para explicitamente atribuir usuários a grupos de acesso.

*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 MBRGRPCOND. 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. Além disso, como vários grupos de acesso podem referir-se ao mesmo atributo do usuário, a atribuição de um atributo a um usuário pode, implicitamente, incluir esse usuário a vários grupos de acesso. 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 dentro um conjunto possível de funções para determinada organização pertenceria ao grupo de acesso.

*Grupo de Acesso Explícito:* É possível adicionar 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 diretivas baseadas em funções para comandos controladores, a ação é Execute e o recurso é o comando sendo executado. Em diretivas 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, nas diretivas dos beans de dados, a ação Exibir é utilizada para permitir a ativação dos 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 do WebSphere Commerce Administration Console e através do XML. Grupos de ações são armazenados na tabela AACTGRP. Ações estão associadas com grupos de ação na tabela AACTACTGP.

### **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 informações adicionais sobre a interface `Protectable`, consulte o Guia do Programador do *IBM WebSphere Commerce*.

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

### **Recursos**

Os recursos são quaisquer objetos no sistema que precisam ser protegidos. Por exemplo RFQs, leilões, usuários e pedidos são alguns dos recursos do WebSphere Commerce que precisam ser protegidos. Cada recurso tem um proprietário. A propriedade do recurso é utilizada para determinar quais diretivas de controle de acesso aplicam-se a ele. As diretivas de controle de acesso têm um proprietário, que é uma entidade organizacional. Uma diretiva é aplicada apenas aos recursos pertencentes à mesma entidade organizacional que assina um grupo de diretivas que contém a diretiva. Se a organização que possui o recurso não assinar o grupo de diretivas, então as diretivas nos grupos de diretivas assinados pela organização predecessora mais próxima serão aplicadas.

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

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

- Utilize a organização que possui a loja que está atualmente no contexto do comando.

- Se não houver nenhuma loja no contexto do comando, utilize a Organização Raiz como a proprietária.

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

Se um bean de dados precisa ser protegido e pode existir por si só, deve ser diretamente protegido. Se a existência de um bean de dados depende da existência de um outro bean de dados, então ele deve delegar para outro bean de dados por motivo de proteção. Um exemplo de bean dados que deve ser diretamente protegido é o bean de dados `Order`. Um exemplo de bean de dados que deve ser indiretamente protegido é o bean de dados `OrderItem`, pois ele não pode existir sem o bean de dados `Order`. Consulte o *WebSphere Commerce Programming Guide and Tutorials* para obter informações adicionais 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 de 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 informações adicionais, consulte o *WebSphere Commerce 5.4 - Guia do Programador*.

## Grupos de Recursos

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

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

**Grupos de Recursos Implícitos:** Os grupos de recursos implícitos definem recursos que correspondem a um determinado conjunto de atributos. Um desses atributos deve ser o nome da classe do Java. Outros atributos podem incluir `status`, `ID` da loja, `preço`, etc. Por exemplo, você poderia criar um grupo de recursos implícito que inclua todos os pedidos que possuem `status` pendentes (`ORDERS.STATUS=P`). Os grupos de recursos implícitos geralmente são utilizados para agrupar recursos que serão utilizados em diretivas 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 diretiva de controle de acesso, utilizando a coluna ACRELATION\_ID da tabela ACPOLICY. Ao avaliar uma diretiva 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 diretivas 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 diretiva 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 diretiva declara que o usuário deve ser o criador ou o submissor 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 de compra 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 relacionamentos consiste em uma ou mais condições abertas RELATIONSHIP\_CHAIN, agrupadas por 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 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.

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 de uma entidade organizacional tiver sido retornada pela avaliação do parâmetro aValue1, esta parte de RELATIONSHIP\_CHAIN será atendida se pelo menos uma destas entidades organizacionais atender 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 diretiva. Para obter informações adicionais sobre como definir grupos de relacionamentos, consulte “Definindo Grupos de Relacionamentos” na página 157.



## Tipos de Diretivas de Controle de Acesso

Existem dois tipos de diretivas de controle de acesso:

- Diretivas padrão agrupáveis (tipo de diretiva -2)
- Diretivas de gabarito agrupáveis (tipo de diretiva -3)

As diretivas de gabarito agrupáveis e padrão agrupáveis devem pertencer a um grupo de diretivas para serem aplicadas no sistema. Uma diretiva padrão agrupável é aplicada uma vez em organizações que são assinantes de um grupo de diretivas que contém a diretiva.

As diretivas de gabarito agrupáveis são naturalmente dinâmicas porque possuem um grupo de acesso que é colocado em escopo quando o sistema está em execução na organização que possui o recurso. Por exemplo, quando este tipo de diretiva é aplicada a um recurso pertencente à Organização XYZ, ele verifica se o usuário desempenhou uma das funções especificadas para a Organização XYZ ou seus ascendentes.

## Diretivas Especiais de Controle de Acesso Padrão

As diretivas a seguir requerem algumas explicações extras:

- Site Administrators Can Do Everything (SiteAdministratorsCanDoEverything)
- BecomeUser Customer Service Group Executes Become User Commands on customer's behalf  
(BecomeUserCustomerServiceGroupExecutesBecomeUserCmdsResourceGroup)

SiteAdministratorsCanDoEverything é uma diretiva padrão especial que concede acesso de super-usuário aos administradores com a função Administrador de Site. Nesta diretiva, 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.

A diretiva

BecomeUserCustomerServiceGroupExecutesBecomeUserCmdsResourceGroup é uma diretiva especial que permite a determinados usuários administrativos executar comandos especificados em nome de outros usuários. Essa diretiva é necessária, por exemplo, quando um cliente solicita a um representante de atendimento ao cliente que crie um pedido em seu nome. Nesse caso, o representante de atendimento ao cliente está apto a executar o comando, tal como se o cliente mesmo estivesse executando o comando.

---

## Funções

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

Todas as funções no WebSphere Commerce são estendidas a uma organização. Por exemplo, um usuário utiliza a função Gerenciador de Produtos para a Organização X. Nesse caso, a Organização X deve suportar a função Gerenciador de Produtos. Em geral, uma organização deve suportar uma função antes de poder atribuí-la a qualquer usuário para essa organização. As diretivas 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 suborganizações.

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

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

- Funções de operações técnicas
- Funções de marketing
- Funções operacionais
- Funções de atendimento ao cliente
- Funções de relacionamento de negócios
- Funções de gerenciamento e comercialização de produtos

No WebSphere Commerce 5.5, cada função é associada a um ou mais modelos de negócios. Em cada modelo, uma função pode executar algumas tarefas seletivas utilizando as ferramentas Commerce Accelerator, o Administration Console e o Organization Administration Console. Para obter informações adicionais sobre modelos de negócios, consulte o *WebSphere Commerce - Fundamentos*.

O gráfico a seguir exibe o acesso que cada função possui a cada uma das ferramentas. Antes de atribuir funções aos usuários, assegure-se de ter as informações corretas sobre quais restrições de acesso são aplicáveis a essa função.

## Funções Mapeadas para Ferramentas do WebSphere Commerce para Cada Amostra de Loja

*Tabela 1. Funções Mapeadas para Ferramentas do WebSphere Commerce*

Funções	Exemplos	Ferramentas
Representante de Conta	<ul style="list-style-type: none"><li>• B2B direto: ToolTech</li></ul>	<ul style="list-style-type: none"><li>• Accelerator</li></ul>
Administrador da Compradora	<ul style="list-style-type: none"><li>• B2B direto: ToolTech</li></ul>	<ul style="list-style-type: none"><li>• Organization Administration Console</li></ul>
Aprovador do Comprador	<ul style="list-style-type: none"><li>• B2B direto: ToolTech</li></ul>	<ul style="list-style-type: none"><li>• Organization Administration Console</li></ul>
Comprador (lado da venda)	<ul style="list-style-type: none"><li>• Consumidor direto: Fashion Flow</li><li>• B2B direto: ToolTech</li></ul>	<ul style="list-style-type: none"><li>• Accelerator</li></ul>
Comprador (Lado da Compra)	<ul style="list-style-type: none"><li>• B2B direto: ToolTech</li><li>• Hospedagem: Loja hospedada</li><li>• Cadeia de suprimentos: Loja hospedada do fornecedor</li></ul>	Esta função está disponível nas amostras, mas não possui acesso a nenhuma ferramenta específica.

Tabela 1. Funções Mapeadas para Ferramentas do WebSphere Commerce (continuação)

Funções	Exemplos	Ferramentas
Gerente de Categorias	<ul style="list-style-type: none"> <li>• Consumidor direto: FashionFlow</li> <li>• B2B direto: ToolTech</li> <li>• Cadeia de demanda: Loja hospedada, Loja de recursos do catálogo,</li> <li>• Hospedagem: Loja hospedada, Loja de recursos do catálogo</li> <li>• Cadeia de suprimentos: Loja de recursos do catálogo, Loja hospedada do fornecedor</li> </ul>	<ul style="list-style-type: none"> <li>• Accelerator</li> </ul>
Gerenciador de Canais	<ul style="list-style-type: none"> <li>• Cadeia de demanda: Hub de canais</li> <li>• Hospedagem: Hub de hospedagem</li> <li>• Cadeia de suprimentos: Diretório da loja</li> </ul>	<ul style="list-style-type: none"> <li>• Accelerator</li> <li>• Organization Administration Console</li> </ul>
Representante de Atendimento ao Cliente	<ul style="list-style-type: none"> <li>• Consumidor direto: Fashion Flow</li> <li>• B2B direto: ToolTech</li> </ul>	<ul style="list-style-type: none"> <li>• Accelerator</li> </ul>
Supervisor de Assistência ao Cliente	<ul style="list-style-type: none"> <li>• Consumidor direto: Fashion Flow</li> <li>• B2B direto: ToolTech</li> </ul>	<ul style="list-style-type: none"> <li>• Accelerator</li> </ul>
Gerente de Logística	<ul style="list-style-type: none"> <li>• B2B direto: ToolTech</li> <li>• Cadeia de suprimentos: Loja hospedada do fornecedor</li> </ul>	<ul style="list-style-type: none"> <li>• Accelerator</li> </ul>
Gerente de Marketing	<ul style="list-style-type: none"> <li>• Consumidor direto: Fashion Flow</li> <li>• B2B direto: ToolTech</li> <li>• Cadeia de demanda: Hub de canais, Loja hospedada, Loja de recursos de fachada da loja do revendedor</li> <li>• Hospedagem: Loja hospedada, Loja de recursos de fachada da loja hospedada</li> </ul>	<ul style="list-style-type: none"> <li>• Accelerator</li> </ul>
Gerente de Operações	<ul style="list-style-type: none"> <li>• Consumidor direto: Fashion Flow</li> <li>• Cadeia de demanda: Loja hospedada</li> <li>• Hospedagem: Loja hospedada</li> </ul>	<ul style="list-style-type: none"> <li>• Accelerator</li> </ul>

Tabela 1. Funções Mapeadas para Ferramentas do WebSphere Commerce (continuação)

Funções	Exemplos	Ferramentas
Coletor	<ul style="list-style-type: none"> <li>• Consumidor direto: Fashion Flow</li> <li>• B2B direto: ToolTech</li> </ul>	<ul style="list-style-type: none"> <li>• Accelerator</li> </ul>
Comprador de Aquisições	<ul style="list-style-type: none"> <li>• B2B direto: ToolTech</li> <li>• Cadeia de suprimentos: Loja hospedada do fornecedor</li> </ul>	Esta função está disponível nas amostras, mas não possui acesso a nenhuma ferramenta específica.
Administrador da Compradora de Aquisições	<ul style="list-style-type: none"> <li>• B2B direto: ToolTech</li> <li>• Cadeia de suprimentos: Loja hospedada do fornecedor</li> </ul>	Esta função está disponível nas amostras, mas não possui acesso a nenhuma ferramenta específica.
Gerente de Produtos	<ul style="list-style-type: none"> <li>• Consumidor direto: Fashion Flow</li> <li>• B2B direto: ToolTech</li> </ul>	<ul style="list-style-type: none"> <li>• Accelerator</li> </ul>
Receptor	<ul style="list-style-type: none"> <li>• Consumidor direto: Fashion Flow</li> <li>• B2B direto: ToolTech</li> </ul>	<ul style="list-style-type: none"> <li>• Accelerator</li> </ul>
Cliente Registrado	<ul style="list-style-type: none"> <li>• Consumidor direto: Fashion Flow</li> <li>• B2B direto: ToolTech</li> <li>• Cadeia de demanda: Hub de canais, Loja hospedada</li> <li>• Hospedagem: Hub de hospedagem, Loja hospedada</li> <li>• Cadeia de suprimentos: Diretório de loja, Loja hospedada do fornecedor</li> </ul>	Esta função está disponível nas amostras, mas não possui acesso a nenhuma ferramenta específica.
Administrador de Devoluções	<ul style="list-style-type: none"> <li>• Consumidor direto: Fashion Flow</li> <li>• B2B direto: ToolTech</li> </ul>	<ul style="list-style-type: none"> <li>• Accelerator</li> </ul>
Gerente de Vendas	<ul style="list-style-type: none"> <li>• B2B direto: ToolTech</li> <li>• Cadeia de suprimentos: Loja hospedada do fornecedor</li> </ul>	<ul style="list-style-type: none"> <li>• Accelerator</li> </ul>

Tabela 1. Funções Mapeadas para Ferramentas do WebSphere Commerce (continuação)

Funções	Exemplos	Ferramentas
Vendedor	<ul style="list-style-type: none"> <li>• Consumidor direto: Fashion Flow</li> <li>• B2B direto: ToolTech</li> <li>• Cadeia de demanda: Loja hospedada</li> <li>• Hospedagem: Loja hospedada</li> <li>• Cadeia de suprimentos: Loja hospedada do fornecedor</li> </ul>	<ul style="list-style-type: none"> <li>• Accelerator</li> </ul>
Administrador da Vendedora	<ul style="list-style-type: none"> <li>• Consumidor direto: Fashion Flow</li> <li>• B2B direto: ToolTech</li> <li>• Cadeia de demanda: Hub de canais, Loja hospedada</li> <li>• Hospedagem: Hub de hospedagem, Loja hospedada</li> <li>• Cadeia de suprimentos: Diretório de loja, Loja hospedada do fornecedor</li> </ul>	<ul style="list-style-type: none"> <li>• Organization Administration Console</li> </ul>
Administrador do Site (Organização Raiz)	<ul style="list-style-type: none"> <li>• Consumidor direto: Fashion Flow</li> <li>• B2B direto: ToolTech</li> <li>• Cadeia de demanda: Hub de canais, Loja hospedada, Loja de recursos do catálogo, Loja de recursos de fachada da loja do revendedor</li> <li>• Hospedagem: Hub de hospedagem, Loja hospedada, Loja de recursos do catálogo, Loja de recursos de fachada da loja hospedada</li> <li>• Cadeia de suprimentos: Diretório da loja, Loja hospedada do fornecedor, Loja de recursos do catálogo, Loja de recursos do fornecedor</li> </ul>	<ul style="list-style-type: none"> <li>• Accelerator</li> <li>• Organization Administration Console</li> <li>• Administration Console</li> </ul>

**Notas:**

1. O Administrador do Site é a única função com acesso ao Administration Console.

2. Para obter informações adicionais sobre as funções específicas e os menus de cada ferramenta a que eles têm acesso, consulte o arquivo "Funções" na ajuda on-line do WebSphere Commerce Production.
3. Para obter informações adicionais sobre cada loja de exemplo, consulte "Lojas" no Ajuda On-line do WebSphere Commerce Production and Development

---

## Como o Controle de Acesso Impede Ações não Autorizadas

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

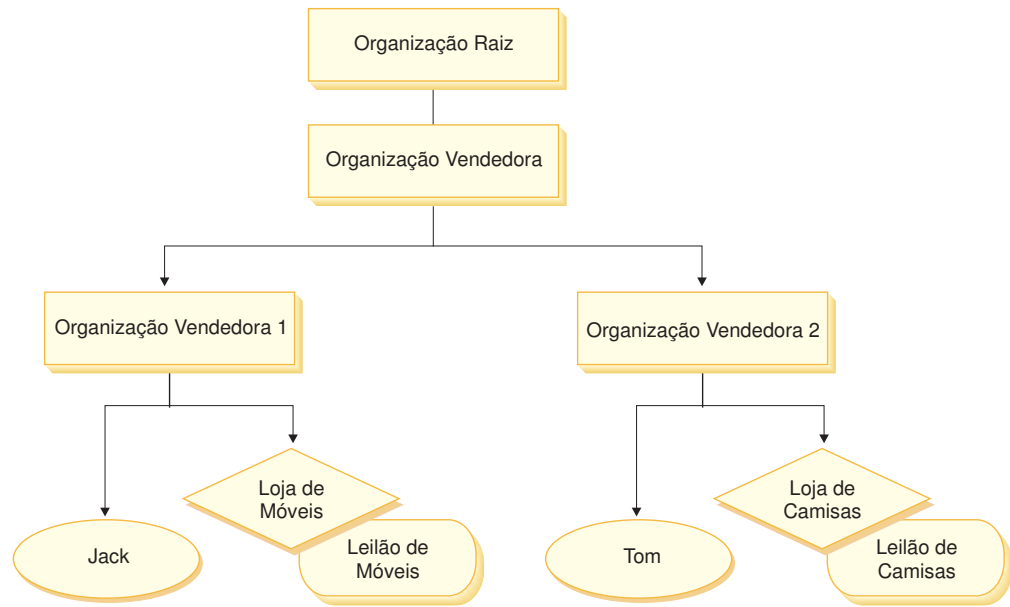
### Verificando a Autorização antes de Executar uma Ação Iniciada pelo Usuário

O *Gerenciador de Diretivas* 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 diretivas de controle de acesso são especificadas no formato XML. Durante a criação da instância, as diretivas padrão e os grupos de diretivas são carregados nas tabelas de banco de dados apropriadas. 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 Diretivas 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 diretivas do XML, o armazenamento em cache do controle de acesso precisa ser atualizado. Isso pode ser feito atualizando o registro apropriado no WebSphere Commerce Administration Console. Se os dados da diretiva foram alterados, então o registro das Diretivas de Controle de Acesso deve ser atualizado. Se os dados do grupo de diretivas foram alterados, então o registro dos Grupos de Diretivas de Controle de Acesso deve ser atualizado. Iniciando novamente o WebSphere Commerce também resultará em uma atualização do cache.

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

### Níveis de Controle de Acesso

Existem dois níveis amplos de controle acesso no WebSphere 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 diretiva de controle de acesso, Vendedores podem executar comandos de vendedores. Nesta diretiva, 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.

#### Controle de Acesso de Nível de Comando para Comandos do Controlador:

Sempre que um comando do controlador for executado, uma diretiva 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 do URL ou quando é o resultado de um redirecionamento a partir de um comando, ela deve ter uma diretiva de controle de acesso. Tal diretiva 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 diretiva de nível de comando apropriada, na tabela `ACPOLICY`.

## Controle de Acesso em Nível de Recurso ou Baseado na Instância

As diretivas de controle de acesso em nível de recurso ou da instância fornecem controle de acesso gradual, determinando quem pode executar qual comando em quais recursos. O exemplo anterior de uma diretiva de controle de acesso baseado na função, que permite que os Vendedores modifiquem os leilões, pode ser ajustado de forma adequada para que o controle de acesso em nível de recurso seja: Vendedores podem modificar leilões pertencentes à organização pela qual exercem a função. Em 35, Jack tem a função de vendedor para a Organização Vendedora 1. Tom tem a função de vendedor para a Organização Vendedora 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 diretiva de controle de acesso em nível de recurso subsequente 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, ..)`

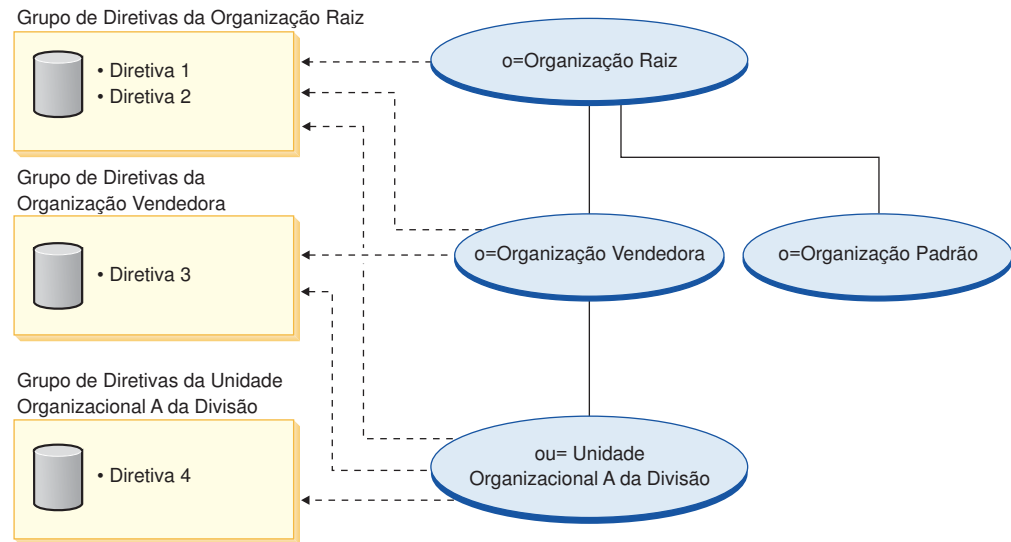
**Controle de Acesso de Nível de Recurso para Beans de Dados:** Conforme explicado acima, as exibições são protegidas por diretivas de nível de comando, que geralmente são baseadas em funções. Por exemplo, a diretiva de nível de comando pode determinar que um Administrador da Vendedora tenha acesso a 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 da Vendedora. 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 diretiva que conceda ao usuário atual a autoridade para executar a ação `Display` no recurso de beans de dados.



## Avaliando as Diretivas de Controle de Acesso

Esta seção pode ser utilizada como um guia para avaliar as diretivas de controle de acesso. Nesta seção, você é apresentado a um cenário e guiado através de um exemplo de como avaliar diretivas de controle de acesso padrão e de gabarito agrupáveis. Cada seção começa com uma descrição de diretivas relacionadas e cenários utilizando cada diretiva. Para obter informações adicionais sobre diretivas padrão agrupáveis e de gabarito agrupáveis, consulte “Tipos de Diretivas de Controle de Acesso” na página 29.

O seguinte diagrama exibe graficamente o cenário:



## Hierarquia Organizacional

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

- Organização Raiz
- Organização Vendedora
- Organização Padrão
- Unidade da Organização da Divisão A

As linhas inteiras no diagrama indicam propriedade, as linhas pontilhadas indicam assinaturas. Como você pode ver, a Organização Raiz é pai da Organização Vendedora e da Organização Padrão. A Organização Vendedora é pai da Unidade da Organização da Divisão A.

## Usuários

No diagrama, Don e Emily estão registrados na Organização Vendedora. Abe, Billy e Carol estão registrados na Unidade da Organização da Divisão A. O usuário Guest 1 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 Vendedora. Abe tem a função de aprovador para a Unidade da Organização da Divisão A.

## Grupos de Acesso

Os seguintes grupos de acesso são utilizados neste cenário:

- Usuários registrados: Esse grupo inclui implicitamente todos os usuários que estão registrados em pelo menos uma organização no site.
- Aprovadores para Vendedor: Este grupo inclui implicitamente todos os usuários que têm a função de aprovadores para a Organização Vendedora.
- Aprovadores para a Divisão A: Esse grupo inclui implicitamente todos os usuários que têm a função de aprovador para a Unidade da Organização da 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 Vendedora podem atualizar documentos pertencentes às duas organizações, Divisão A e Vendedora.

## Avaliando Diretivas Padrão Agrupáveis

Esta seção o conduz pelas diretivas padrão agrupáveis e pelos cenários que os avaliarão.

### Diretivas de controle de acesso relacionadas à atualização de documento

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

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

#### Diretiva 1:

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

Essa é uma diretiva padrão agrupável baseada em função que faz parte do grupo de diretivas da Organização Raiz, que a Organização Raiz, a Organização Vendedora e a Unidade Organizacional A da Divisão estão assinando. Nesta diretiva, os usuários registrados podem executar os comandos Atualizar Documento.

#### Diretiva 2:

[Usuários Registrados, Atualizar Grupo de Ação de Documento, documento, criador ]  
Essa é uma diretiva padrão agrupável de nível do recurso que faz parte do grupo de diretivas da Organização Raiz, que a Organização Raiz, a Organização Vendedora e a Unidade Organizacional A da Divisão estão assinando. Nesta diretiva, os usuários registrados podem atualizar um documento se forem os criadores daquele documento.

#### Diretiva 3:

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

Esta é uma diretiva de nível de recurso padrão agrupável que faz parte do grupo de diretivas da Organização Vendedora da qual a Organização Vendedora e a Unidade Organizacional A da Divisão é assinante. Nesta diretiva, os aprovadores para o Vendedor podem atualizar documentos que pertencem ao Vendedor.

#### **Diretiva 4:**

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

Essa é uma diretiva ao nível de recurso de padrão agrupável que faz parte do grupo de diretivas da Unidade da Organização da Divisão A que a Divisão A está assinando. Nesta diretiva, 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. Portanto, apenas as diretivas pertencentes aos grupos de diretivas assinados pela Organização Raiz serão utilizados para avaliar se o usuário tem acesso em nível de comando: as diretivas 1 e 2 fazem parte do grupo de diretivas que a Organização Raiz está assinando.
2. A Diretiva 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. Como a Divisão A assina os grupos de diretivas, todas as diretivas pertencentes a esses grupos de diretivas serão aplicados: diretivas 1, 2, 3 e 4.
2. A Diretiva 2 concede acesso desde que Billy seja um membro do grupo de acesso Usuários Registrados, esteja executando a ação de comando Atualizar Documento no recurso de documento e atenda o relacionamento de criador do documento.

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

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

*Comando - verificação de nível:*

1. Não existe nenhum ID de loja especificado, então o proprietário do comando é definido como Organização Raiz. Portanto, apenas as diretivas pertencentes aos grupos de diretivas assinados pela Organização Raiz serão utilizados para avaliar se o usuário tem acesso em nível de comando: as diretivas 1 e 2 pertencem à Organização Raiz.
2. A Diretiva 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. Como a Divisão A assina os grupos de diretivas, todas as diretivas pertencentes a esses grupos de diretivas serão aplicados: diretivas 1, 2, 3 e 4.
2. A Diretiva 3 concede acesso desde que Don seja membro do grupo de acesso Aprovadores para Vendedor e esteja executando a ação do comando Atualizar Documento no recurso do documento.

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

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

*Comando - verificação de nível:*

1. Não existe nenhum ID de loja especificado, então o proprietário do comando é definido como Organização Raiz. Portanto, apenas as diretivas pertencentes aos grupos de diretivas assinados pela Organização Raiz serão utilizados para avaliar se o usuário tem acesso em nível de comando: as diretivas 1 e 2 pertencem à Organização Raiz.
2. A Diretiva 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 Vendedora. Como a Organização Vendedora assina os grupos de diretivas, todas as diretivas pertencentes a esses grupos de diretivas serão aplicados: diretivas 1, 2, e 3.
2. A diretiva 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: Usuário Guest 1 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. Portanto, apenas as diretivas pertencentes aos grupos de diretivas assinados pela Organização Raiz serão utilizados para avaliar se o usuário tem acesso em nível de comando: as diretivas 1 e 2 pertencem à Organização Raiz.
2. A Diretiva 1 NÃO concede acesso, visto que o usuário Guest 1 NÃO é 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

Como o usuário Guest 1 falhou na verificação do nível de comando, ele não pode atualizar seu próprio documento.

## Avaliando Diretivas de Gabarito Agrupáveis

Esta seção baseia-se na configuração mostrada no diagrama a seguir.

### Diretivas de controle de acesso relacionadas à atualização de documento

Nesta configuração, as diretivas de controle de acesso 1 e 2 ainda se aplicam, porém, as diretivas de padrão agrupáveis 3 e 4 são agora substituídos pela diretiva de gabarito agrupável 5. Para obter informações adicionais sobre as diretivas 1 e 2, consulte “Avaliando Diretivas Padrão Agrupáveis” na página 38.

#### Diretiva 5:

[Aprovadores para Organização, Atualizar Grupo de Ação de Documento, documento, - ]  
Essa é uma diretiva ao nível de recurso de gabarito agrupável. Ela é parte do grupo de diretivas da Organização Raiz, que a Organização está assinando. As diretivas de gabarito agrupáveis aplicam-se dinamicamente à organização que possui o recurso durante o tempo de execução. Essas diretivas utilizam, tipicamente, grupos de acesso parametrizados. Nesse caso, o seguinte grupo de acesso com parâmetros é utilizado:

- Aprovadores para Organização: Este grupo inclui implicitamente todos os usuários que têm a função de aprovador para a organização que possui o recurso dos documentos ou para organizações de predecessores.

### Cenários

Os cenários a seguir são baseados na configuração mostrada no diagrama anterior, que possui apenas um grupo de diretivas. O grupo de diretivas da Organização Raiz inclui as diretivas 1, 2 e 5.

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

*Comando - verificação de nível:*

1. Não existe nenhum ID de loja especificado, então o proprietário do comando é definido como Organização Raiz. Portanto, apenas as diretivas pertencentes aos grupos de diretivas assinados pela Organização Raiz serão utilizados para avaliar se o usuário tem acesso em nível de comando: as diretivas 1, 2 e 5.
2. A Diretiva 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. A Divisão A não assina nenhum grupo de diretivas, portanto, a estrutura de controle de acesso começará a pesquisar a hierarquia da organização até encontrar uma organização que assine pelo menos um grupo de diretivas. A organização pai imediata da Divisão A, a Organização Vendedora, também não assina grupos de diretivas. Continuando na hierarquia da organização, a Organização Raiz é alcançada. Essa organização assina um grupo de diretivas, portanto, suas diretivas podem ser aplicadas: às diretivas 1, 2 e 5.
2. A diretiva de gabarito agrupável 5 é aplicada à organização que possui o recurso: Divisão A. O grupo de acesso com parâmetros, Aprovadores para Organização, é estendido dinamicamente para o contexto de recurso atual de tal forma que verificará se o usuário atende a condição de grupo de acesso da organização que possui o recurso ou seus ascendentes. Nesse caso, Don é um aprovador para a Organização Vendedora (um ascendente da Divisão A),

portanto, ele atende as condições do grupo de acesso. Como ele está executando a ação do comando Atualizar Documento no recurso de documento, os outros elementos da diretiva 5 também são atendidos, portanto, a verificação de diretiva ao nível de recurso é transmitida.

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

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

*Comando - verificação de nível:*

1. Não existe nenhum ID de loja especificado, então o proprietário do comando é definido como Organização Raiz. Portanto, apenas as diretivas pertencentes aos grupos de diretivas assinados pela Organização Raiz serão utilizados para avaliar se o usuário tem acesso em nível de comando: as diretivas 1, 2 e 5.
2. A Diretiva 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 Vendedora. A Organização Vendedora não assina nenhum grupo de diretivas, portanto, a estrutura de controle de acesso começará a pesquisar a hierarquia da organização até encontrar uma organização que assine pelo menos um grupo de diretivas. Continuando na hierarquia da organização, a Organização Raiz é alcançada. Essa organização assina um grupo de diretivas, portanto, suas diretivas podem ser aplicadas: às diretivas 1, 2 e 5.
2. A diretiva de gabarito agrupável 5 é aplicada à organização que possui o recurso: Divisão de Vendedores. O grupo de acesso com parâmetros, Aprovadores para Organização, é estendido dinamicamente para o contexto de recurso atual de tal forma que verificará se o usuário atende a condição de grupo de acesso da organização que possui o recurso ou seus ascendentes. Nesse caso, Abe é um aprovador para a Unidade da Organização da Divisão A (um descendente da Organização Vendedora), portanto, ele não atende as condições do grupo de acesso.

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.

---

## Analizando uma Diretiva em Detalhes

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

```
AuctionAdministratorsForOrgExecuteAuctionManageCommandsOnAuctionResource
```

**Nota:** Essa é uma diretiva de nível do recurso. Seu tipo de diretiva é gabarito agrupável.

No primeiro exemplo, aprenderemos como ler a diretiva utilizando o WebSphere Commerce Organization Administration Console, como identificar suas partes e

como entender o que a diretiva significa. O segundo exemplo analisará a diretiva 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 diretiva está relacionada com outras diretivas. Compreender dependências entre diretivas é um pré-requisito importante para fazer alterações para acessar as diretivas de controle ou criar novas.

## Exemplo 1: Lendo uma Diretiva

Neste exemplo, utilizaremos o WebSphere Commerce Organization Administration Console para procurar uma diretiva e identificar as partes que a definem. Também utilizaremos essas peças para formar uma descrição geral da diretiva.

### Analizando a Diretiva no Organization Administration Console

1. Efetue login no WebSphere Commerce Organization Administration Console. No menu Gerenciamento de Acesso, selecione **Diretivas**.
2. Selecione a Organização Raiz a partir do quadro de listagem, visto que a Organização Raiz possui a maioria das diretivas de controle de acesso padrão.
3. Na página Diretivas, role pela lista de diretivas e localize a seguinte diretiva: `AuctionAdministratorsForOrgExecuteAuctionManageCommandsOnAuctionResource`  
Observe que você pode rolar pela lista de diretivas utilizando a barra de rolagem, bem como utilizando os links **Primeiro**, **Anterior**, **Avançar** e **Último**.

### Exibindo as partes da diretiva

1. Selecione a diretiva 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 diretiva. 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 informações adicionais sobre os comandos, consulte a seção de referência na documentação de ajuda on-line.

Observe que você também pode acessar a mesma lista de ações a partir da página Diretivas clicando em **Exibir ações**.

4. Para retornar para a página de diretivas, selecione qualquer uma das ações e clique em **Exibir Diretivas**.
5. Selecione a diretiva novamente, mas agora clique em **Exibir Grupo de Membros** para ver o grupo de membros (de acesso) utilizado nesta diretiva.
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 **Crítérios**. Na página de Crítérios, 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 Crítérios sem fazer quaisquer alterações. No menu Gerenciamento de Acesso, selecione **Diretivas** novamente. Localize a seguinte diretiva:  
AuctionAdministratorsForOrgExecuteAuctionManageCommandsOnAuctionResource
11. Selecione a diretiva e Clique em **Exibir Recursos**. Na página Recursos, você verá o recurso com `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 Diretivas clicando em **Exibir Grupo de Recursos** e detalhando para recursos individuais.
12. Selecione agora **Diretivas** no menu Gerenciamento de Acesso, e localize a seguinte diretiva:  
AuctionAdministratorsForOrgExecuteAuctionManageCommandsOnAuctionResource
13. Selecione a diretiva e clique em **Alterar**. Na página Alterar Diretiva, examine o menu drop down em **Relacionamento** . Observe que o relacionamento é definido como nenhum. Isso significa que a diretiva não tem um relacionamento.
14. Clique em **Cancelar** e **OK** para a caixa de diálogo.

### Compreendendo o que a Diretiva significa

Agora que nós identificamos as partes individuais desta diretiva, podemos começar a juntá-las para entender o que a diretiva faz. Primeiro, sabemos que a diretiva 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 Diretivas e detalhando para o nível de detalhamento. Por último, podemos dizer que a diretiva não inclui um relacionamento entre o grupo de acesso e os recursos.

Reunindo tudo, podemos concluir que esta diretiva 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 diretiva começa com o nome do grupo designado de usuários, AuctionAdministratorForOrg. A notação, ForOrg, indica que essa é uma diretiva de gabarito agrupável. AuctionManageCommands descreve o grupo de ações e AuctionResource descreve o grupo de recursos.

---

## Exemplo 2: Lendo uma Diretiva em XML

As diretivas 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 diretiva no the 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 Diretivas 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 diretiva de controle de acesso do banco de dados para o arquivo XML.

Essa é a aparência de uma diretiva 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="groupable Template">
</Policy>
```

Aqui, a diretiva é definida por:

Name: O nome da diretiva.

OwnerID: A organização na qual a diretiva se aplica.

UserGroup: O grupo de acesso.

ActionGroupName: O grupo de ações.

ResourceGroupName: O grupo de recursos.

PolicyType: O tipo de diretiva, como padrão agrupável ou de gabarito agrupável.

O arquivo que contém todas as diretivas 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 diretiva de controle de acesso padrão no arquivo de controle de acesso padrão precisa ter sua descrição correspondente atualizada

emdefaultAccessControlPolicies\_en\_US.xml. No entanto, recomendamos que as alterações feitas nos arquivos XML sejam reservadas para usuários avançados.

### Exemplo 3: Identificando outras Diretivas Associadas a sua Diretiva

Neste último exemplo, examinaremos como uma diretiva de controle de acesso pode ser dependente de outras diretivas.

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

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

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

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

#### Analizando as funções associadas com a diretiva

1. Efetue login no WebSphere Commerce Administration Console e localize a diretiva de nível de recurso na página Diretivas. Utilizando o mesmo exemplo, sabemos que a diretiva que desejamos é a seguinte:

`AuctionAdministratorsForOrgExecuteAuctionManageCommandsOnAuctionResource`

.

2. Identifique o grupo de acesso associado à diretiva. 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.

#### Analizando as diretivas baseadas na função para cada função

1. Mude para o Apêndice no final deste manual e localize o cabeçalho da seção, Diretivas Baseadas em Funções. Você utilizará o Apêndice para localizar cada diretiva baseada em função associada a uma função.
2. Localize a diretiva `Buyers(sell-side)ExecuteBuyers(sell-side)CommandsResourceGroup`. Esta diretiva está associada à função Compradores (lado de vendas). Sabemos isso porque `Buyers(sell-side)` é o prefixo da diretiva.
3. Localize o restante das diretivas baseadas em funções associadas a funções Compradores (lado de vendas), Gerente de Categorias, Gerente de Produtos e Vendedores, utilizando seus prefixos para identificar as diretivas 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 diretiva baseada em funções permite que os usuários com aquela função executem determinados comandos ou exibições do controlador. Para ver quais ações e recursos estão associados a uma diretiva baseada em funções, procure a diretiva na página Diretivas no WebSphere Commerce Organization Administration Console, utilizando o mesmo procedimento do Exemplo 1.

### **Porque é Importante Identificar Dependências entre Diretivas**

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

No Parte 3, “Administrando a Autorização de Segurança”, na página 91, você aprenderá mais sobre as diretivas 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.



---

## **Parte 2. Administrando a Autenticação de Segurança**

Esta parte descreve as tarefas de autenticação de segurança que normalmente podem ser executadas pelo administrador do site do WebSphere Commerce.



---

## Capítulo 4. Aprimorando a Segurança do Site

Para aprimorar a segurança do seu site do WebSphere Commerce, você pode ativar qualquer um dos seguintes recursos no WebSphere Commerce Configuration Manager:

- Efetue logoff como um usuário que está inativo por um período estendido e solicite que ele efetue logon no sistema novamente, utilizando o nó Tempo Limite de Login. Para obter detalhes, consulte “Ativando o Tempo Limite de Login” na página 55.
- Solicite aos usuários que alterem suas senhas quando estiverem efetuando login no sistema pela primeira vez, utilizando o nó Invalidação de Senha. Para obter detalhes, consulte “Ativando a Invalidação de Senha” na página 56.
- Solicite aos usuários que digitem suas senhas se estiverem executando pedidos que executam comandos designados, utilizando o nó Comandos Protegidos por Senha. Para obter detalhes, consulte “Ativando os Comandos Protegidos por Senha” na página 56.
- Atualize dados criptografados, como senhas e informações do cartão de crédito, bem como a chave do comerciante em um banco de dados WebSphere Commerce, utilizando o nó Ferramenta de Atualização do Banco de Dados. Para obter detalhes, consulte “Atualizando os Dados Criptografados” na página 57.
- Rejeite qualquer pedido de usuário que contenha atributos ou caracteres designados como não permitidos, utilizando o nó Proteção de Script Entre Sites. Para obter detalhes, consulte “Ativando a Proteção de Script Entre Sites” na página 58.
- Identifique rapidamente todas as ameaças de segurança contra o WebSphere Commerce ativando o log de acesso. Para obter detalhes, consulte “Ativando o Log de Acesso” na página 60.

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

- Configure uma diretiva de contas para o site para definir as diretivas relacionadas às contas em uso, utilizando a página Diretiva de contas. Para obter detalhes, consulte “Configurando uma Diretiva de Contas” na página 61.
- Configure uma diretiva de senha para que seu site controle as características de seleção de senha de um usuário utilizando a página Diretiva de senhas (somente se os usuários estiverem autenticados junto ao banco de dados do WebSphere Commerce). Para obter detalhes, consulte “Configurando uma Diretiva de Senhas” na página 62.
- Configure uma diretiva de bloqueio de contas para que seu site reduza as chances de uma conta de usuário ficar comprometida, utilizando a página Diretiva de bloqueio de contas (somente se os usuários estiverem autenticados junto ao banco de dados do WebSphere Commerce). Para obter detalhes, consulte “Configurando uma Diretiva de Bloqueio de Contas” na página 63.
- Lance um programa de segurança que verifica e exclui arquivos temporários do WebSphere Commerce que podem conter exposições de segurança potenciais utilizando a página Lançar verificação de segurança. Para obter detalhes, consulte “Lançando uma Verificação de Segurança” na página 64.

Para obter informações adicionais sobre conceitos relacionados, consulte os seguintes tópicos na ajuda on-line do WebSphere Commerce:

- Configuration Manager
- Arquivo de configuração do WebSphere Commerce
- Administration Console
- Segurança

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

- Ativar o Configuration Manager
- Abrir o Administration Console

---

## Consideração de Segurança para o Servidor Web dos IIS (Internet Information Services)

### Atenção

Se estiver utilizando o servidor Web dos IIS com o WebSphere Commerce, é necessário estar ciente da seguinte consideração de segurança e considerar a ação recomendada para minimizar qualquer exposição de segurança de seus dados do WebSphere Commerce.

**Problema:** Para o servidor Web dos IIS, leia a permissão em um Diretório Virtual que fornece acesso ao código fonte dos arquivos JSP. Para evitar o download do código fonte do JSP, é necessário separar fisicamente o conteúdo estático do conteúdo dinâmico de suas páginas da Web, se estiver utilizando o servidor Web dos IIS. Isso porque a segurança dos IIS é baseada na localização do diretório, em vez de no tipo de arquivo. Sob a configuração padrão dos IIS, os arquivos de imagem e JSP estão localizados sob um alias único. Você deve utilizar a configuração padrão apenas para fins de teste.

**Solução:** Para proteger todos os recursos da Web, o conteúdo dinâmico deve ser acessado utilizando um Diretório Virtual com permissões somente de execução (não leitura), enquanto o conteúdo estático deve ser movido a um Diretório Virtual diferente, com permissão somente de leitura. Para obter informações adicionais sobre como definir as permissões em um Diretório Virtual, consulte as instruções nas informações de ajuda dos IIS. Também é recomendável consultar a documentação atual da Microsoft Corporations sobre correções de segurança e diretivas de configuração.

---

## Exibições de Segurança

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

- Tempo limite de login (consulte “Tempo Limite de Login” na página 53)
- Invalidação de senha (consulte “Invalidação de Senha” na página 53)
- Comandos protegidos por senha (consulte “Comandos Protegidos por Senha” na página 54)
- Proteção de script entre sites (consulte “Proteção de Scripts entre Sites” na página 55)

Para obter informações gerais sobre a criação de exibições e o desenvolvimento da fachada da loja, consulte o *WebSphere Commerce Store Development Guide*.



## Tempo Limite de Login

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

### `LoginTimeoutErrorView`

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

*Tabela 2. Atributos de `LoginTimeoutErrorView`*

<code>ECConstants.EC_LOGIN_TIMEOUT_ERROR_MSGCODE</code>	1	O tempo de expiração está definido com valor errado.
	2	O tempo de logon está definido com o valor errado.
	3	Tempo de expiração ou logon definido com o valor errado.

### `ReLogonFormView`

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

Não existem atributos para `ReLogonFormView`.

*Tabela 3. Atributos de Formulário de `ReLogonFormView`*

<code>ECUserConstants.EC_UREG_LOGONID</code>	O ID de logon do usuário.
<code>ECUserConstants.EC_UREG_LOGON_PASSWORD</code>	A senha de logon do usuário.
<code>ECUserConstants.EC_RELOGIN_URL</code>	O URL que será exibido se as credenciais fornecidas forem inválidas. Na maioria dos casos, será o nome dessa exibição.
<code>ECConstants.EC_STORE_ID</code>	O identificador da loja.
<code>ECConstants.EC_URL</code>	O URL que é exibido quando as credenciais inseridas pertencem a um usuário diferente. Na maioria dos casos, deve ser uma home page da loja ou a mesmo URL que foi utilizado em uma página de logon da loja.

## Invalidação de Senha

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

### `ChangePassword`

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

*Tabela 4. Atributos de `ChangePassword`*

<code>ECConstants.EC_PASSWORD_EXPIRED_FLAG</code>	1	A senha do usuário expirou. Esse atributo é necessário para distinguir essa exibição da exibição utilizada para o recurso de alteração de senha, pois elas são iguais. A exibição para a alteração de senha poderá ser chamada por um usuário e a JSP (JavaServer Pages) atribuída a essa exibição deverá ser o mesmo para ambos os casos. A JSP deve procurar esse atributo para decidir o que exibir.
	<code>null</code>	O atributo não está em um URL. Esse é o comportamento normal de alteração de senha.

**Tabela 4. Atributos de ChangePassword (continuação)**

ECUserConstants.EC_UREG_LOGONID	O ID de logon do usuário atual.
ECConstants.EC_LOGIN_RETURN_URL	O URL o qual o navegador é redirecionado após uma alteração de senha bem-sucedida. Esse URL será transmitido para um comando de ação com o nome ECConstants.EC_URL.

**Tabela 5. Atributos de Formulário de ChangePassword**

ECUserConstants.EC_UREG_LOGONID	O ID de logon do usuário. O ID de logon atual foi passado para a exibição.
ECUserConstants.EC_UREG_LOGON_PASSWORDOLD	A senha antiga.
ECUserConstants.EC_UREG_LOGON_PASSWORD	A nova senha.
ECUserConstants.EC_UREG_LOGON_PASSWORDVERIFY	A verificação da nova senha.
ECConstants.EC_URL	O URL no qual os usuários são redirecionados após uma alteração de senha bem-sucedida. O valor foi passado para a exibição.
ECUserConstants.EC_RELOGIN_URL	O URL no qual o navegador foi redirecionado se a alteração de senha não tiver sido bem-sucedida.

## Comandos Protegidos por Senha

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

### PasswordReEnterErrorView

Essa exibição é utilizada nos seguintes cenários:

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

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

**Tabela 6. Atributos de PasswordReEnterErrorView**

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

### PasswordReEnterFormView

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

**Tabela 7. Atributos de PasswordReEnterFormView**

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

**AÇÃO:** O URL é transmitido como um parâmetro chamado:

**Tabela 8. Atributos de Formulário de PasswordReEnterFormView**

ECConstants.EC_PASSWORD_REREQUEST_PASSWORD1	A primeira senha.
ECConstants.EC_PASSWORD_REREQUEST_PASSWORD2	A segunda senha.

## Proteção de Scripts entre Sites

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

### **ProhibitedAttrsErrorView**

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

### **ProhibitedCharacterErrorView**

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

### **ProhibCharEncodingErrorView**

Igual à exibição `ProhibitedCharacterErrorView` acima.

---

## Ativando o Tempo Limite de Login

**Nota:** Para utilizar o recurso de segurança de tempo limite de login para uma loja, você precisa definir as exibições `LoginTimeoutErrorView` e `ReLogonFormView` para a loja conforme descrito em “Tempo Limite de Login” na página 53.

Utilize o nó Tempo Limite de Login do Configuration Manager para ativar ou desativar o recurso de tempo limite de login. Quando este recurso for ativado, um usuário do WebSphere Commerce que esteja inativo por um longo período de tempo terá seu logoff efetuado no sistema e será solicitado para que efetue login novamente. Se o usuário efetuar login subsequentemente com êxito, o WebSphere Commerce executa o pedido original feito pelo usuário. Se o login do usuário falhar, o pedido original será descartado e o usuário permanecerá com logoff no sistema.

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

Para ativar este recurso:

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

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

---

## Ativando a Invalidação de Senha

**Nota:** Para utilizar o recurso de segurança de invalidação de senha, você precisa definir a exibição ChangePassword para sua loja conforme descrito em “Invalidação de Senha” na página 53.

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

1. Ative o Configuration Manager e vá para o nó de Invalidação de Senha para sua instância da seguinte maneira: **WebSphere Commerce** > *host\_name* > **Lista de Instâncias** > *instance\_name* > **Propriedades da Instância** > **Invalidação da Senha**
2. Para ativar o recurso de invalidação de senha, clique na caixa de opções **Ativar**.
3. Para aplicar suas alterações no Configuration Manager, clique em **Aplicar**.
4. Depois de atualizar com êxito a configuração de sua instância, você receberá uma mensagem indicando uma atualização com êxito.
5. No WebSphere Application Server Administration Console, pare e inicie novamente a instância de servidor do WebSphere Commerce.

---

## Ativando os Comandos Protegidos por Senha

**Nota:** Para utilizar o recurso de segurança de comandos protegidos por senha, você precisa definir as exibições PasswordReEnterErrorView e PasswordReEnterFormView para sua loja conforme descrito em “Comandos Protegidos por Senha” na página 54.

Utilize o nó Comandos Protegidos por Senha do Configuration Manager para ativar ou desativar o recurso de comandos protegidos por senha. Quando esse recurso é ativado, o WebSphere Commerce requer que os usuários registrados que estejam com logon no WebSphere Commerce informem suas senhas antes de continuar um pedido que executa comandos designados do WebSphere Commerce.

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

Para ativar este recurso:

1. Ative o Configuration Manager e vá para o nó de Comandos Protegidos por Senha para sua instância da seguinte maneira: **WebSphere Commerce** > *host\_name* > **Lista de Instâncias** > *instance\_name* > **Propriedades da Instância** > **Comandos Protegidos por Senha**
2. Na guia Geral:
  - a. Para ativar o recurso de comandos protegidos por senha, clique em **Ativar**.
  - b. Digite o número de repetições no campo Repetições. (O número padrão de repetições é 3).

3. Na guia Avançado:
  - a. Selecione na lista um comando do WebSphere Commerce que deseja proteger na janela Lista de Comandos Protegidos por Senha e clique em **Adicionar**. O comando selecionado é listado na janela Lista Atual Protegida por Senha.
  - b. Se desejar desativar a proteção por senha para qualquer comando do WebSphere Commerce, selecione o comando na janela da Lista Atual de Comandos Protegidos por Senha e clique em **Remover**.
4. Para aplicar suas alterações no Configuration Manager, clique em **Aplicar**.
5. Depois de atualizar com êxito a configuração de sua instância, você receberá uma mensagem indicando uma atualização com êxito.
6. No WebSphere Application Server Administration Console, pare e inicie novamente a instância de servidor do WebSphere Commerce.

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

---

## Atualizando os Dados Criptografados

Utilize a Ferramenta de Atualização do Banco de Dados disponível no Nó Banco de Dados do Configuration Manager para alterar a chave do comerciante e atualizar todos os dados criptografados (por exemplo, senhas ou números de cartões de crédito) em um ou mais bancos de dados do WebSphere Commerce de uma determinada instância. Para utilizar a ferramenta:

1. Ative o Configuration Manager e vá para a sua entrada de banco de dados específica, da seguinte maneira: **WebSphere Commerce** > *host\_name* > **Lista de Instâncias** > *instance\_name* > **Propriedades da Instância** > **Banco de Dados** > *database\_name*
2. Clique com o botão direito do mouse em *database\_name* e selecione **Executar Ferramenta de Atualização de Banco de Dados**
  - Selecione **Atualizar todos os bancos de dados para essa instância** para migrar dados criptografados para todos os bancos de dados da instância selecionada.
 

▶ 400

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

Ações	Parâmetros	Ação Necessária
-------	------------	-----------------

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

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

---

## Ativando a Proteção de Script Entre Sites

**Nota:** Para utilizar o recurso de segurança de script entre sites para uma loja, é necessário definir as exibições `ProhibitedAttrsErrorView`, `ProhibitedCharacterErrorView` e `ProhibCharEncodingErrorView` para a loja conforme descrito em “Proteção de Scripts entre Sites” na página 55.

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

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

Para ativar este recurso:

1. Ative o Configuration Manager e vá para o nó de Proteção de Script Entre Sites para a sua instância da seguinte forma: **WebSphere Commerce** > *host\_name* > **Lista de Instâncias** > *instance\_name* > **Propriedades da Instância** > **Proteção de Script Entre Sites**

2. Utilize a guia Geral para ativar o recurso de proteção cruzada de script do site, da seguinte forma:
  - a. Clique em **Ativar**.
  - b. Para adicionar atributos que deseja rejeitar para comandos do WebSphere Commerce, clique com o botão direito do mouse na tabela Atributos Proibidos e selecione **Adicionar linha**. Digite o atributo que você deseja rejeitar. Você só pode especificar um atributo por linha.
  - c. Para remover atributos da tabela Atributos Proibidos, destaque e clique com o botão direito do mouse na linha que contém o atributo na tabela e selecione **Excluir linha**.
  - d. Para adicionar cadeias que deseja rejeitar para os comandos do WebSphere Commerce, clique no botão direito na tabela Caracteres Proibidos e selecione **Adicionar linha**. Adicione a cadeia que você deseja rejeitar. Você só pode especificar uma cadeia por linha.
  - e. Para remover caracteres da tabela Caracteres Proibidos, destaque e clique com o botão direito do mouse na linha que contém o caracter na tabela Caracteres Proibidos e selecione **Excluir linha**.

**Nota:** As seguintes cadeias são especificadas por padrão nos campos de caracteres proibidos. Essas cadeias são mais comumente utilizadas como tags de script em ataques maliciosos a scripts entre sites:

- <SCRIPT
- &lt;SCRIPT
- <% e &lt;%

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

Você também pode remover atributos específicos de um comando, selecionando o atributo e clicando em **Remover**.

4. Para aplicar suas alterações no Configuration Manager, clique em **Aplicar**.
5. Depois de atualizar com êxito a configuração de sua instância, você receberá uma mensagem indicando uma atualização com êxito.
6. No WebSphere Application Server Administration Console, pare e inicie novamente a instância de servidor do WebSphere Commerce.

#### **Notas:**

1. Quando os comandos forem excluídos da proteção de script entre sites, os valores de atributos especificados serão codificados através da codificação de símbolos em HTML. Por exemplo, o comando `cmd1?user=<Thomas>` é codificado como `ascmd1?user=&#60;Thomas&#62;`
2. Quando você especifica a cadeia nos campos de caracteres proibidos, saiba que:

- Uma determinada seqüência de caracteres pode fazer com que a cadeia seja convertida para um único caractere em conformidade com os padrões de codificação do URL. Por exemplo, a cadeia `<%bb` será convertida em uma cadeia `<X` em que `X` é um único caractere que tem um valor de representação hexadecimal HEX 'bb' (decimal 187). Nesse caso, a cadeia `<%bb` não será capturada pela proteção de script entre sites, se tiver passado em um URL.
- Uma determinada seqüência de caracteres pode fazer com que a conversão da cadeia falhe, se eles não estiverem em conformidade com os padrões de codificação do URL. Por exemplo, a cadeia `<%gg` fará com que a conversão falhe, pois HEX 'gg' não é uma representação válida de valor hexadecimal. Nesse caso, a cadeia `<%gg` provocará uma exceção, resultando em nenhuma resposta ao pedido de URL que contém tal cadeia, independente da proteção de script entre sites estar ativada.

**Exemplo:** Considere os seguintes exemplos:

- Cadeias proibidas: `<SCRIPT`, `<%`  
Atributos proibidos: `mycomment`, `description`

Comando	Status
<code>cmd1?description=Available...</code>	rejeitado
<code>cmd2?userid=Thomas...</code>	aceito
<code>cmd3?mycomment=&lt;SCRIPT&gt;...</code>	rejeitado
<code>cmd4?password=&lt;%...%&gt;...</code>	rejeitado

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

Comando	Status
<code>cmd1?text=&lt;SCRIPT&gt;...</code>	aceito
<code>cmd1?text=&lt;%...%&gt;...</code>	aceito
<code>cmd1?txt=&lt;SCRIPT&gt;...</code>	rejeitado
<code>cmd1?txt=&lt;%..%&gt;...</code>	rejeitado

## Ativando o Log de Acesso

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

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

- Nome do Host do cliente
- ID do thread que está executando o comando;
- ID do usuário do cliente;
- Hora em que ocorreu o evento;



- Comando que foi executado;
- Loja para qual o comando foi executado;
- Recurso no qual a operação foi executada;
- Resultado da verificação de controle de acesso.

Para ativar o log de acesso, faça o seguinte:

1. Ative o Configuration Manager.
2. Selecione o **Nome do Host** > **Instância** > **Instance\_List** e então abra a pasta **Componentes**.
3. Selecione **AccessLoggingEventListener**.
4. No painel Geral, ative a caixa de opção **Ativar Componente**.
5. Selecione o painel Avançado e ative **Iniciar**.
6. Clique em **Aplicar**.
7. Saia do Configuration Manager.
8. Inicie Novamente o WebSphere Application Server.

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

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

em que:

- *aa* é um valor inteiro especificando o número máximo de entradas que serão registradas na memória antes das entradas serem gravadas no banco de dados. Geralmente, um número mais alto resultará em melhor desempenho com relação ao registro de acesso. O valor padrão é 32.
  - *bbbb* é true ou false. Um valor true significa que todos os pedidos recebidos estão registrados. Um valor false significa que somente as violações de acesso estão registradas. Para evitar registro excessivo ou desnecessário, um valor false é recomendado. Utilize true somente quando você suspeitar de problemas de autenticação ou contravenção de segurança em seu site. O valor padrão é false.
3. Quando tiver concluído as atualizações, salve o arquivo *instance.xml* da instância do WebSphere Commerce.
  4. Inicie Novamente o WebSphere Application Server.

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

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

---

## Configurando uma Diretiva de Contas

A página Diretiva de Contas do WebSphere Commerce Administration Console permite configurar uma diretiva de contas. Essa página lista todas as diretivas de conta existentes, incluindo qualquer das predefinidas fornecidas com o WebSphere Commerce por padrão. Uma diretiva de conta define as diretivas relacionadas à conta, como diretivas de bloqueio de senha e de conta. Nesta página é possível:

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

Para criar uma nova diretiva de contas:

1. Abra o WebSphere Commerce Administration Console.
2. No menu drop down Segurança do Administration Console, clique em **Diretiva de Contas**.
3. Na página Diretiva de Contas, clique em **Novo** para criar uma nova diretiva de contas.
4. Digite o nome da diretiva de contas no campo Nome (por exemplo, my\_account\_policy).
5. No menu Diretiva de Senhas, selecione uma diretiva de senhas preexistente.
6. No menu Diretiva de bloqueio de contas, selecione uma diretiva de bloqueio de contas preexistente.
7. Clique em **OK**.

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

Consulte também “Diretivas de Autenticação Padrão” na página 65 para obter informações adicionais.

---

## Configurando uma Diretiva de Senhas

A página Diretiva de Senha do WebSphere Commerce Administration Console permite controlar a seleção de senha de um usuário para definir as características da senha e assegurar que esteja de acordo com a diretiva de segurança de seu site. Essa página lista todos as diretivas de senha existentes, incluindo qualquer das predefinidas fornecidas com o WebSphere Commerce por padrão.

Uma diretiva de senhas define os atributos com os quais a senha deve estar de acordo. A diretiva de senha reforça as seguintes condições:

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

Para criar uma nova diretiva de senha:

1. Abra o WebSphere Commerce Administration Console.
2. No menu drop down Segurança do Administration Console, clique em **Diretiva de Senhas**.
3. Na página Diretiva de Senhas, clique em **Novo** para criar uma nova diretiva de senhas.
4. Digite um nome para a diretiva de senhas no campo Nome (por exemplo, `my_password_policy`).
5. Atualize o seguinte conforme necessário para modificar todos os valores a partir do valor padrão para compradores:
  - **O ID do usuário e senha podem coincidir?** Define se o ID do usuário e senha podem ser idênticos ou não. Selecione *Sim* ou *Não* na lista.
  - **Máximo de tipos de caracteres consecutivos.** Define a ocorrência máxima de caracteres consecutivos em uma senha. O valor mínimo é 2 caracteres consecutivos. Por exemplo, com um valor 2, um usuário não pode digitar uma senha como `aaabc`.
  - **Máximo de instâncias de qualquer caracter.** Define o número máximo de vezes que o mesmo caracter pode aparecer em uma senha. O valor mínimo é 1 instância de um caracter. Por exemplo, com um valor 2, um usuário não pode digitar uma senha como `abcaabc`.
  - **Tempo de vida máximo das senhas.** Define o período de tempo, em dias, que uma senha pode existir. O valor mínimo é 1 dia. Após esse período de tempo, o usuário será solicitado a alterar sua senha.
  - **Número mínimo de caracteres alfabéticos.** Define o número mínimo de caracteres alfabéticos que precisam estar em uma senha. O valor mínimo é 0 caracteres alfabéticos.
  - **Número mínimo de caracteres numéricos.** Define o número mínimo de caracteres numéricos que precisam estar em uma senha. O valor mínimo é 0 caracteres numéricos.
  - **Comprimento mínimo de senha.** Define o menor comprimento de uma senha, em caracteres. O valor mínimo é 1 caracter.
  - **A senha pode ser reutilizada?** Define se uma senha anterior do usuário pode ser reutilizada. Selecione *sim* ou *não* na lista.
6. Clique em **OK**.

**Notas:**

1. Você não pode excluir uma diretiva de senhas se ela estiver em uso (ou seja, um usuário estiver atribuído à diretiva de senhas).
2. As diretivas de senha serão reforçadas apenas se os usuários forem autenticados junto ao banco de dados do WebSphere Commerce.

Consulte também “Diretivas de Autenticação Padrão” na página 65 para obter informações adicionais.

---

## Configurando uma Diretiva de Bloqueio de Contas

A página Diretiva de Bloqueio de Contas do WebSphere Commerce Administration Console permite configurar uma diretiva de bloqueio de contas para diferentes funções de usuário no WebSphere Commerce. Essa página lista todas as diretivas de bloqueio de contas existentes, incluindo qualquer das predefinidas fornecidas com o WebSphere Commerce por padrão. Uma diretiva de bloqueio de contas desativará uma conta de usuário, se ações maldosas forem executadas nessa conta, para reduzir as chances dessa ações que comprometem a conta.

Uma diretiva de bloqueio de contas reforçam os seguintes itens:

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

Para definir uma diretiva de bloqueio de contas:

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

Para uma nova diretiva de bloqueio de contas, na página Diretiva de Bloqueio de Contas:

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

**Notas:**

1. Você não pode excluir uma diretiva de bloqueio de conta, se ela estiver em uso (ou seja, um usuário será atribuído à diretiva de bloqueio de conta).
2. As diretivas de bloqueio de contas serão aplicadas apenas se os usuários estiverem autenticados junto ao banco de dados do WebSphere Commerce.

---

## Lançando uma Verificação de Segurança

 400 Esse recurso não é aplicável no WebSphere Commerce for iSeries.

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

Para invocar o programa de verificação de segurança:

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

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

▶ **AIX** ▶ **Linux** ▶ **Solaris** `WC_installdir/instances/instance_name/logs`

▶ **Windows** `WC_installdir\instances\instance_name\logs`

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

1. No Windows Explorer, clique no botão direito na pasta *unidade*:\WebSphere.
2. Clique em **Propriedades** e **Segurança**. Por padrão, o grupo "Todos" tem a permissão **todos** para essa pasta.
3. Clique em **Adicionar**.
4. Uma janela é exibida (Selecione usuários, computadores...). Nessa janela, selecione o grupo **Administradores**.

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

Clique em **Adicionar** e, em seguida, em **OK**.

5. Na guia Segurança, o Grupo Administradores foi adicionado. Você precisa remover "Todos". Selecione **Todos** e limpe a caixa que indica "Aceitar Permissão Herdada...."
6. Clique em **Remover** na janela Segurança que é exibida.

---

## Campo de Encrypt PDI do Configuration Manager

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

---

## Diretivas de Autenticação Padrão

O WebSphere Commerce fornece duas diretivas de autenticação padrão:

- "Compradores"
- "Administradores" na página 66

### Compradores

A diretiva de conta padrão para compradores contém a diretiva de bloqueio de contas padrão e a diretiva de senha padrão para compradores.

A diretiva de bloqueio de contas padrão para compradores contém os seguintes atributos padrão:

Atributo	Valor padrão
Limite de bloqueio de contas	6 tentativas
Atrasos consecutivos de login sem êxito	10 segundos

A diretiva de senha padrão para compradores contém os seguintes atributos padrão:

Atributo	Valor padrão
Se o ID do usuário e a senha podem corresponder	N (eles não podem corresponder)
Número máximo de ocorrências de caracteres consecutivos	3 caracteres
Número máximo de instâncias de qualquer caractere	4 instâncias
Duração máxima das senhas	180 dias
Número mínimo de caracteres alfabéticos	1 caractere alfabético
Número mínimo de caracteres numéricos	1 caractere numérico
Comprimento mínimo da senha	6 caracteres
Se a senha anterior do usuário pode ser reutilizada	N (ela não pode ser reutilizada)

Os compradores que executam um auto-registro são atribuídos com a diretiva de autenticação de comprador padrão - Compradores.

## Administradores

A diretiva de conta padrão para administradores contém a diretiva de bloqueio de contas padrão e a diretiva de senha padrão para administradores.

A diretiva de bloqueio de contas padrão para administradores contém os seguintes atributos padrão:

Atributo	Valor padrão
Limite de bloqueio de contas	3 tentativas
Atrasos consecutivos de login sem êxito	20 segundos

A diretiva de senha padrão para compradores contém os seguintes atributos padrão:

Atributo	Valor padrão
Se o ID do usuário e a senha podem corresponder	N (eles não podem corresponder)
Número máximo de ocorrências de caracteres consecutivos	3 caracteres
Número máximo de instâncias de qualquer caractere	4 instâncias
Duração máxima das senhas	90 dias
Número mínimo de caracteres alfabéticos	1 caractere alfabético

<b>Atributo</b>	<b>Valor padrão</b>
Número mínimo de caracteres numéricos	1 caractere numérico
Comprimento mínimo da senha	8 caracteres
Se a senha anterior do usuário pode ser reutilizada	N (ela não pode ser reutilizada)

O usuário administrador wcsadmin padrão que é fornecido com o WebSphere Commerce é atribuído à diretiva de autenticação padrão - Administradores.





---

## Capítulo 5. Gerenciamento de Sessões

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

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

---

### Gerenciamento de Sessão Baseado em Cookies

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

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

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

- Um cookie de sessão não seguro

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

- Um cookie de sessão do WebSphere Application Server baseia-se no padrão de sessão HTTP do servlet. Os cookies do WebSphere Application Server persistem na memória ou no banco de dados em uma implantação de nós múltiplos. Para obter informações adicionais, pesquise "gerenciamento de

sessão" no Centro de Informações do WebSphere Application Server (<http://www.ibm.com/software/webservers/appserv/infocenter.html>).

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

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

- Um cookie de autenticação seguro

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

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

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

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

## Utilizando Cookies para Gerenciamento de Sessão

Para utilizar cookies no WebSphere Commerce, faça o seguinte:

1. Abra o Configuration Manager.
2. Selecione a **Instância**, em seguida abra a pasta **Gerenciamento de Sessão**.
3. Selecione os valores de sessão adequados.
  - Teste de aceitação de cookies  
Selecione esta caixa de opção para verificar se o navegador do cliente aceita cookies para um site que suporta apenas cookies.
  - Gerenciador de sessão de cookies  
Selecione se deseja que o WebSphere Commerce ou o WebSphere Application Server gerencie seus cookies. O padrão é WebSphere Commerce.
    - Um cookie de sessão do WebSphere Application Server baseia-se no padrão de sessão HTTP do servlet. Os cookies do WebSphere Application Server persistem na memória ou no banco de dados em uma implantação de nós múltiplos. Para obter informações adicionais, pesquise "gerenciamento de sessão" no Centro de Informações do WebSphere Application Server (<http://www.ibm.com/software/webservers/appserv/infocenter.html>).
    - Um cookie de sessão do WebSphere Commerce é interno ao WebSphere Commerce e não persiste no banco de dados.
4. Clique na guia **Avançado**. Selecione os valores de sessão adequados.
  - Caminho do cookie

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

Para obter detalhes sobre caminhos do cookie, consulte a Especificação de Cookie do Netscape e o RFC 2109.

- **Domínio do cookie**

Especifica um padrão de restrição de domínio. Normalmente, este campo não deve ser alterado.

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

5. Clique em **Aplicar**.

6. Feche o Configuration Manager.

7. No WebSphere Application Server Administration Console, pare e inicie novamente a instância de servidor do WebSphere Commerce.

---

## Regravação de URL

Com a regravação de URL, todos os links retornados ao navegador ou redirecionados têm o ID de sessão anexados a ele. Quando o usuário clica nesses links, o formulário de regravação do URL é enviado ao servidor como parte do pedido do cliente. O mecanismo de servlet reconhece o ID de sessão no URL e o salva para obter o objeto adequado para esse usuário. Para utilizar a regravação de URL, os arquivos HTML (arquivos com extensão .html ou .htm) não podem ser utilizados para links. Para utilizar a regravação de URL, os arquivos JSP devem ser utilizados para fins de exibição. Uma sessão com regravação de URL expira quando o comprador efetua logoff.

**Nota:** O armazenamento em cache dinâmico do WebSphere Commerce e a regravação de URL não podem interoperar. Com a regravação de URL ativada, é necessário desativar o armazenamento em cache dinâmico do WebSphere Commerce. Para obter informações adicionais, consulte o capítulo sobre armazenamento em cache dinâmico no *WebSphere Commerce - Guia de Administração*.

## Utilizando Gerenciamento de Sessões de Regravação de URL

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

1. Abra o Configuration Manager.

2. Selecione a **Instância**, em seguida abra a pasta **Gerenciamento de Sessão**.

3. Selecione os valores de sessão adequados.

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

Gerenciador de sessão de cookies. Selecione o WebSphere Application Server.

4. Clique em **Aplicar**.

5. Feche o Configuration Manager.

6. No WebSphere Application Server Administration Console, pare e inicie novamente a instância de servidor do WebSphere Commerce.

## Gravando Gabaritos JSP para Regravação de URL

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

### Gravando Links

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

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

é regravado como

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

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

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

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

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

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

substitua-o por:

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

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

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

Os métodos `encodeURL()` e `encodeRedirectURL()` fazem parte do objeto `HttpServletResponse`. Em ambos os casos, essas chamadas verificam se a

regravação de URL foi configurada antes da codificação do URL. Se não tiver sido configurada, ela retornará o URL original.

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

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

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

---

## Gerenciamento de Sessão em Nível de Loja

O diagrama a seguir ilustra a infra-estrutura do registro em nível de loja do WebSphere Commerce. O registro em nível de loja utiliza funções de controle de acesso para associar um comprador a uma loja.

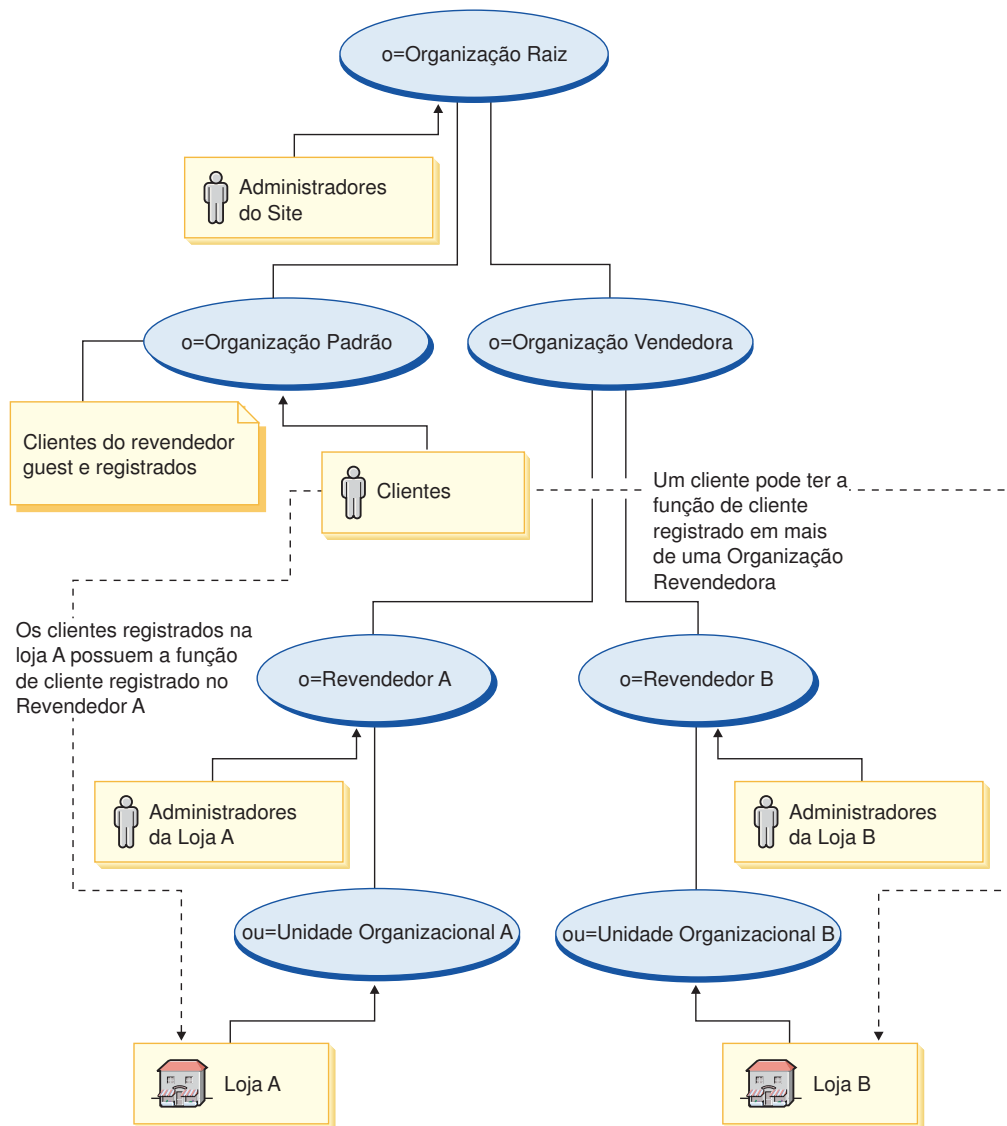


Figura 3. Registro em Nível de Loja

Usuários que compram em uma loja não precisam necessariamente ser membros da organização da loja, mas precisam exercer uma função de compra (isto é, Cliente Registrado) na organização. Usuários que exercem uma função administrativa em uma organização são geralmente associados a ela por meio de um relacionamento hereditário.

Por exemplo, suponha que você tenha uma loja, Loja A como no diagrama acima. Suponha também que Sue faça compras na Loja A e Joe seja um funcionário da Loja A responsável pelas tarefas administrativas de colocar a Loja A em funcionamento. Para modelar este cenário a partir de uma perspectiva organizacional, Joe deve ser colocado sob a organização da Loja A, mas Sue não. Como Sue não é uma funcionária da Loja A, ela está associada à Loja A desempenhando sua função de compra na organização da Loja A.

Uma loja determina todos seus compradores registrados localizando todos os usuários que exercem uma função de compra na organização da loja. Um administrador de usuário da loja pode então continuar a executar todas as

atividades na loja, como configurar uma campanha para todos os usuários registrados de uma loja ou ações específicas, como redefinir a senha de um usuário registrado em sua loja.

Consultando o diagrama na Figura 3 na página 74, considere o seguinte cenário:

- Sue, que é membro da Organização Padrão, possui uma função de compra na organização A do Revendedor. A organização pai A do Revendedor é a Organização Revendedora.
- O Revendedor A possui a loja A
- Sue não possui uma função organizacional na organização B do Revendedor
- O Revendedor B possui a loja B

Sue efetua login na Loja A e faz compras normalmente. Quando Sue acessa a Loja B, a ela é atribuída uma nova identidade de sessão para a Loja B como um usuário guest. Se ela acessar a Loja A mais uma vez, as informações em sua identidade de sessão anterior para a Loja A será utilizada pelo WebSphere Commerce para gerenciar sua sessão.

A identidade de sessão para a Loja A seria reutilizada para a Loja B se:

- A Loja A e a loja B pertencerem à mesma organização.
- Sue tiver uma função definida nas organizações do Revendedor A e do Revendedor B.





---

## Capítulo 6. Definindo e Alterando Senhas

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

---

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

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

#### ▶ 400 Perfis de usuário do iSeries

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

- Um perfil de usuário que você cria e utiliza para instalar o WebSphere Commerce e iniciar o Configuration Manager. Para instalar e configurar o WebSphere Commerce, você deve utilizar um perfil do usuário do iSeries de USRCLS(\*SECOFR) ou utilizar o perfil do usuário QSECOFR. Se você precisar criar um perfil do usuário, consulte o *WebSphere Commerce - Guia de Instalação* para iSeries.
- Um perfil do usuário que é criado pelo Configuration Manager quando você cria uma instância WebSphere Commerce. Esse perfil do usuário também é referido como o *perfil do usuário da instância*. Um perfil do usuário de USRCLS(\*USER) é criado pelo Configuration Manager sempre você cria uma instância do WebSphere Commerce. Se você precisar criar um perfil do usuário, consulte o *WebSphere Commerce - Guia de Instalação* para iSeries.

#### ID do usuário do Configuration Manager

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

▶ AIX ▶ Linux ▶ Solaris ▶ Windows Você pode acessar o Configuration Manager na máquina do WebSphere Commerce ou em qualquer máquina que esteja na mesma rede que o WebSphere Commerce.

▶ 400 Para o iSeries, você pode acessar o Configuration Manager em qualquer máquina do Windows que esteja na mesma rede que o servidor iSeries.

#### ID do Usuário do IBM HTTP Server

▶ AIX ▶ Linux ▶ Solaris ▶ Windows Se estiver utilizando o IBM HTTP Server, poderá acessar a home page do servidor Web abrindo o navegador da Web e digitando o seguinte endereço da Web:

`http://host_name`

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

## Instance Administrator do WebSphere Commerce

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

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

`https://host_name:8000/accelerator`

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

`https://host_name:8002/adminconsole`

- WebSphere Commerce Organization Administration Console. Para acessar o WebSphere Commerce Organization Administration Console a partir de uma máquina remota executando um sistema operacional Windows, abra o navegador da Web Internet Explorer e digite o seguinte endereço da Web:

`https://host_name:8004/orgadminconsole`

Para obter as ferramentas acima, insira o ID do usuário e a senha do administrador inseridos quando você criou sua instância do WebSphere Commerce.

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

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

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

## Administrador do WebSphere Commerce Payments

Ao instalar o WebSphere Commerce Payments, o ID do Administrador do Site do WebSphere Commerce é atribuído automaticamente à função de Payments Administrator. Siga as instruções no *WebSphere Commerce - Guia de Instalação* para alternar o Payments Realm Class para WCSRealm se isso ainda não tiver sido feito.

A função de Payments Administrator ativa um ID do usuário para que controle e administre o WebSphere Commerce Payments.

### 400 Nota:

- Não exclua ou renomeie o ID do usuário do Administrador do Site criado para sua instância e não altere qualquer das funções pré-atribuídas do WebSphere Commerce Payments, pois as funções do WebSphere Commerce relacionadas à integração do WebSphere Commerce Payments não funcionarão.

### Windows ID do usuário do Windows

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

- Não podem ter mais de 8 caracteres de comprimento.

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



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

#### Importante

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

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



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

## Alterando a Senha do Configuration Manager

Você poderá alterar a senha do Configuration Manager quando ativar o Configuration Manager clicando em **Modificar** na janela em que digita seu ID do usuário e senha.

De forma alternativa, para alterar o ID do usuário ou a senha do Configuration Manager, mude para o subdiretório bin sob o caminho de instalação do WebSphere Commerce e digite o seguinte em uma janela de comando:

1. Vá para o subdiretório bin do WebSphere Commerce:  

```
cd WC55_installdir/bin
```
2. Execute o script wcs\_encrypt para obter uma versão criptografada de sua senha:



```
./wcs_encrypt.sh new_password
```

Windows

```
wcs_encrypt new_password
```

3. Abra o arquivo PwdMgr.xml no diretório `WC55_installdir/instances` e modifique LoginPassword com a senha criptografada na etapa 2.

---

## Definindo a Senha do Administrador do IBM HTTP Server

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

1. Alterne para o diretório `HTTPServer_installdir/bin` em sua máquina.
2. Digite o seguinte comando:

AIX Linux Solaris 

```
./htpasswd -b ../conf/admin.passwd user password
```

Windows 

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

 em que `user` e `password` são o ID do usuário e a senha que você quer para ter autoridade administrativa para o IBM HTTP Server.

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

**Nota:** Se a senha do administrador não existir, será necessário executar `htpasswd` com a opção `-c` para criar a senha primeiro.

---

## Alterando a Senha do Arquivo de Chaves SSL

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

1. Windows Clique em **Menu Iniciar** → **Programas** → **IBM HTTP Server** → **Iniciar Utilitário Key Management**.
2. No menu **Arquivo do Banco de Dados Chave**, selecione **Abrir**.
3. Mude para o subdiretório `ssl` sob o caminho de instalação do IBM HTTP Server em sua máquina. O arquivo de chaves (que possui a extensão de arquivo `.kdb`) deve estar nesta pasta. Se não estiver, crie um arquivo de chaves seguindo as instruções descritas em Capítulo 17, “Ativando o SSL para Produção com o IBM HTTP Server”, na página 197.
4. No menu **Arquivo de Banco de Dados Chave**, selecione **Alterar Senha**. A janela **Alterar Senha** é exibida.
5. Digite sua nova senha e ative **Armazenar a senha em um arquivo**.
6. Clique em **OK**. Sua senha foi alterada.





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

---


## Gerando Senhas Criptografadas para o WebSphere Commerce

Você pode gerar senhas criptografadas para redefinir manualmente a senha de um usuário a partir de uma linha de comandos. Existem outras ferramentas (tais como, o comando `ResetPassword`) que executa a mesma tarefa. Para redefinir manualmente a senha, o administrador pegaria a senha criptografada exibida pelos

utilitários abaixo e atualizaria o campo LOGONPASSWORD da tabela USERREG. O administrador então atualizaria o campo SALT da tabela USERREG com o conteúdo escolhido.

    O WebSphere Commerce permite gerar senhas criptografadas. Para gerar senhas criptografadas, proceda da seguinte maneira:


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

 `wcs_password.bat password SALT merchant_key`

   `./wcs_password.sh password SALT merchant_key`

em que

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

 Para iSeries, para alterar a senha criptografada para compradores, utilize o comando `chgwcpwd.sh`.

1. Inicie uma sessão QShell em seu sistema iSeries.
2. Navegue para o seguinte diretório: `WC_installdir/bin`
3. Execute o seguinte script a partir da linha de comandos: `chgwcpwd.sh` (Os parâmetros de utilização serão exibidos).
4. Execute o comando novamente, utilizando os parâmetros apropriados.

Para obter detalhes sobre a execução desse comando, consulte Ajuda On-line do WebSphere Commerce Production and Development.

---

## Gerando Senhas Criptografadas para o WebSphere Commerce Payments

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

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

 `wcs_pmpassword.bat password SALT`

    `./wcs_pmpassword.sh password SALT`

em que:

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

---

## Redefinindo uma Conta de Administrador

Se uma conta do WebSphere Commerce for travada ou desativada por algum motivo, você poderá destravá-la ou ativá-la da seguinte forma:

Se a conta *não for* uma conta do administrador do site:

1. Abra o Administration Console.
2. Clique em **Gerenciamento de Acesso > Usuários**.
3. Dê um clique duplo na conta do usuário ou selecione-a na lista e clique em **Alterar**.
4. Selecione **Ativar** no campo Status da Conta.
5. Dê um clique sobre **OK**.

Se a conta *for* uma conta de um administrador do site ou qualquer outra conta de usuário, execute as seguintes instruções SQL a partir de uma janela de comandos do DB2 ou de um prompt SQLPlus (para bancos de dados Oracle):

```
CONNECT TO db_name [USER user_id USING password]  
UPDATE USERREG SET STATUS=1, PASSWORDRETRIES=0 WHERE  
LOGONID=' logonId'
```

em que

*db\_name*

É o nome do banco de dados do WebSphere Commerce (por exemplo, MALL).

*user\_id* É o ID do usuário do administrador do banco de dados para o banco de dados.

*password*

É a senha correspondente ao ID do usuário do administrador do banco de dados.

*logonId*

É o ID do usuário da conta que você deseja redefinir (por exemplo, wcsadmin).

Por exemplo, para redefinir a conta wcsadmin, você poderá emitir as seguintes instruções SQL se tiver feito logon em seu sistema com o ID do usuário do administrador do banco de dados:

```
CONNECT TO mall  
UPDATE USERREG SET STATUS=1, PASSWORDRETRIES=0 WHERE  
LOGONID='wcsadmin'
```

▶ 400 Para inserir instruções SQL na plataforma iSeries, você pode utilizar o DB2/400 Query Manager e o SQL Development Kit ou pode utilizar o iSeries Navigator. Para utilizar o IBM iSeries Access para executar consultas do banco de dados, faça o seguinte:

1. Inicie o Navegador iSeries a partir do PC no qual está instalado.
2. Expanda o sistema iSeries. Expanda Bancos de Dados, clique com o botão direito do mouse em Banco de Dados Relacional e selecione **Executar Scripts SQL**. A janela Executar Scripts SQL é aberta.
3. No menu Conexão, selecione **Configuração do JDBC** . Clique na guia **Servidor**.
4. No campo Bibliotecas Padrão, apague quaisquer valores existentes e informe o nome do esquema do banco de dados de sua instância. Por padrão, o nome do esquema é o nome da instância. Clique em **OK** para salvar suas alterações.
5. Digite as instruções SQL acima na janela.





---

## Capítulo 7. Sign-on Único

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

---

### Pré-requisitos

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

- Deve existir um servidor LDAP instalado e configurado. Para configurar um servidor LDAP, consulte o *WebSphere Commerce - Guia de Software Adicional*.
- O WebSphere Commerce deve estar instalado e configurado para utilizar o LDAP.
- A segurança do WebSphere Application Server deve estar ativada. Para ativar a segurança do WebSphere Application Server, consulte Capítulo 16, "Ativando a Segurança do WebSphere Application Server", na página 185.

---

### Ativando Sign-on Único

#### Atenção

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

- Os cookies do LTPA podem fluir entre diferentes portas de servidor da Web.
- Talvez seja necessário modificar o arquivo `ldapentry.xml` e adicionar a classe de objeto `ePerson`. Esse é um atributo do elemento `ldapocs`.
- É necessário modificar o `instance.xml` e assegurar-se de que o sinalizador `MigrateUsersFromWCSdb` está definido como "ON".
- As máquinas participando da configuração de sign-on único devem ter os relógios de seus sistemas sincronizados.
- O sign-on único só é suportado entre aplicativos que possam ler e emitir o token LTPA (Light Weight Third Party Authentication) do WebSphere Application Server.

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

1. Ativar o sign-on único no WebSphere Application Server. Para obter informações adicionais, pesquise "conexão única" no Centro de Informações do WebSphere Application Server (<http://www.ibm.com/software/webservers/appserv/infocenter.html>). Selecione **Sign-on Único: WebSphere Application Server** e conclua as seções a seguir:
  - **Configurando SSO para WebSphere Application Server**.
    - **Modificar as definições de segurança do WebSphere Application Server.**

**Nota:** A etapa que detalha como preencher os campos do LDAP pode ser ignorada com segurança.
    - **Exportar as chaves de LTPA para um arquivo.**
2. Em sua máquina WebSphere Commerce, inicie o WebSphere Commerce Configuration Manager.

3. Para configurar o nó **Subsistema de Membros**, faça o seguinte:
  - a. Sob **WebSphere Commerce** expanda *host\_name* → **Lista de Instâncias** → *instance\_name* → **Propriedades da Instância** → **Subsistema do Membro**.
  - b. No menu drop-down **Modo de Autenticação**, selecione **LDAP**.
  - c. Ative a caixa de opções **Conexão Única**.
  - d. No campo **Host**, digite o nome completo do seu servidor LDAP.
  - e. Digite o nome distinto do administrador no campo **Nome Distinto do Administrador**. Deve ser o mesmo nome que foi utilizado no seu servidor LDAP.
  - f. No campo **Senha do Administrador**, digite a senha do administrador. Deve ser a mesma senha que foi utilizada no seu servidor LDAP. Confirme a senha no campo **Confirmar Senha**.
  - g. Preencha cada um dos campos remanescentes.
  - h. Clique em **Aplicar**, em seguida, clique em **OK**.
4. Configure as funções que serão atribuídas aos usuários entrando no sistema a partir de uma SSO (Conexão Única). Sempre que um usuário conecta-se ao sistema pelo SSO, o WebSphere Commerce tentará atribuir funções do arquivo `MemberRegistrationAttributes.xml` com o tipo de registro = "SSO". Link para a nova seção, descrevendo `MRA.xml`.
5. Inicie Novamente o WebSphere Application Server.

## Configurar Funções para Usuários SSO

No WebSphere Commerce 5.5, as funções de segurança são atribuídas como parte do processo de registro. Com conexão única, o cliente pode ignorar a etapa de registro para seu site, se autenticada com êxito em um sistema de colaboração. A habilidade de ser implicitamente autenticado a um site do WebSphere Commerce 5.5 possui pouco valor se for simplesmente negado o acesso ao usuário aos recursos que deseja utilizar, como por exemplo, comprar em uma loja.

Portanto, a mesma funcionalidade da atribuição de funções automatizadas, que acontece com o registro do usuário, também acontece no código de gerenciamento da sessão. Nesse caso, as funções serão configuradas para compradores SSO utilizando o tipo de registro 'SSO'. Desta forma, quando um cliente autentica-se no sistema, o WebSphere Commerce 5.5 fornecerá automaticamente todas as funções necessárias para o site. Tenha em mente que a atribuição de funções SSO ocorre em um nível de site e não em um nível de loja (com o registro de usuário típico). Portanto, você deve assegurar-se de que o atributo `storeAncestor` especificado é realmente predecessor do site (loja 0).

### Exemplo:

```
<User registrationType="SSO" memberAncestor="o=Default Organization,o=Root Organization" storeAncestor="o=Root Organization"><BR>
<Role name="Registered Customer" roleContext="explicit" DN="o=Reseller Organization,o=Root Organization"/><BR>
<Role name="Registered Customer" roleContext="explicit" DN="o=Seller Organization,o=Root Organization"/><BR>
<Role name="Registered Customer" roleContext="explicit" DN="o=Supplier Organization,o=Root Organization"/><BR>
<Role name="Registered Customer" roleContext="explicit" DN="ou=Supplier Hub Organization,o=Business Indirect Supplier Organization,
o=Root Organization"/><BR>
</User>
```

Esse exemplo determinará quatro funções a qualquer comprador que entrar no sistema a partir do SSO

---

## Capítulo 8. Administrando os Certificados X.509

O WebSphere Commerce suporta logon de certificado pelo cliente como mecanismo de segurança, protegendo o site e o cliente. O certificado X.509 complementa a autenticação básica de clientes que entram em um site. Um cliente que possui este certificado pode acessar um site protegido do WebSphere Commerce, que foi ativado para autenticação de certificado do cliente.

Ao criar uma instância do WebSphere Commerce, você seleciona o Modo de Autenticação. Este pode ser Básico ou X.509. O padrão é a autenticação Básica que é a autenticação por logon utilizando um ID e uma senha de login. Para ativar a autenticação por logon utilizando certificados X.509, selecione a autenticação X.509.

Antes de começar a utilizar certificados X.509, você deve preparar um relacionamento de confiança com uma autoridade de certificação externa para tratar da autenticação eletrônica dos certificados X.509. Se você estiver utilizando o Netscape Enterprise como seu servidor Web, será necessário seguir etapas adicionais para ativar os certificados X.509 no servidor Web. Consulte a documentação do Netscape Enterprise Server para obter informações adicionais e instruções completas.

Os usuários do X.509 podem ser acessados através do WebSphere Commerce Accelerator. Antes da autenticação do certificado X.509 ser ativada, o administrador deve assegurar que haja um certificado de cliente que seja reconhecido pelo certificado de servidor e instalado no navegador. Caso contrário, o administrador não conseguirá efetuar logon. Quando o administrador acessa a janela de login do WebSphere Commerce Administration Console pela primeira vez, um registro de comprador de certificado é criado e um cookie do comprador emitido, semelhante a quando um comprador normal acessa um URL seguro. Depois que o administrador efetua logon no WebSphere Commerce Administration Console utilizando o ID e senha corretos, um cookie de administrador é emitido, substituindo o cookie do comprador. Um administrador terá então, dois registros de usuário: o usuário administrador e o usuário comprador anterior.

Uma mensagem de erro é exibida quando:

- O certificado X.509 de um usuário foi revogado por um site
- Um certificado de cliente não contém as informações necessárias para garantir que o comprador seja exclusivo no WebSphere Commerce.

A tarefa de exibição de erro de X.509 é registrada como X509 ErrorView na tabela de banco de dados VIEWREG.

---

### Ativando os Certificados X.509

Ao criar uma instância do WebSphere Commerce, você seleciona autenticação Básica ou autenticação X.509 utilizando o Configuration Manager. O padrão é a autenticação Básica, que é a autenticação que utiliza um ID e uma senha de logon.

Para ativar a autenticação utilizando certificados X.509, faça o seguinte:

1. Configure o certificado SSL do Servidor Web IBM HTTP. O certificado do servidor SSL inclui uma lista de autoridades clientes para relacionamentos de confiança. Pode ser necessário adicionar autoridades de certificação clientes.

2. Inicie o WebSphere Commerce Configuration Manager.
3. Selecione **Propriedades da Instância -> Servidor Web**.
4. Verifique o Modo de Autenticação na caixa **X.509**. Clique em **Aplicar**. Os usuários do certificado cliente X.509 serão aceitos agora. O servidor IBM HTTP é automaticamente ativado para suporte a certificados, quando o Modo de Autenticação X.509 é selecionado.
5. Inicie e pare o servidor WebSphere Commerce. O WebSphere Commerce não registrará usuários X.509 na tabela CERT\_X509 até que o servidor tenha sido iniciado novamente.

**Nota:** Você pode configurar o servidor IBM HTTP para tornar os certificados X.509 opcionais ou obrigatórios.

1. Abra o arquivo de configuração httpd.conf e localize a diretiva SSLClientAuth. Defina a diretiva como 1 (opcional) ou 2 (obrigatório). O parâmetro recomendado é *obrigatório*.
2. Como o cliente WebSphere Commerce Payments não suporta a Autenticação do Cliente SSL, você deverá desativar o SSL entre o cliente WebSphere Commerce Payments e o servidor Web.
  - a. Em um editor de texto, abra o arquivo PaymentServlet.properties. O arquivo está no diretório de instalação do WebSphere Commerce Payments.
    - Localize a propriedade UseNonSSLWCClient. Defina a propriedade como um valor de '1' (um).
    - Se você não puder localizar a propriedade UseNonSSLWCClient no arquivo, adicione a linha:  
UseNonSSLWCClient=1
  - b. Salve o arquivo e saia do editor.
3. Se o WebSphere Commerce Payments estiver instalado na mesma máquina que o WebSphere Commerce:
  - a. Inicie o Configuration Manager.
  - b. Selecione a instância, em seguida selecione **Pagamentos**.
  - c. Marque **Utilizar Não-SSL WebSphere Commerce Payments Client**. Isto permite que o cliente do WebSphere Commerce Server comunique-se com o WebSphere Commerce Payments, sem utilizar SSL.
  - d. Clique em **Aplicar**.
  - e. Feche o Configuration Manager.
4. Inicie novamente o servidor de aplicativos WebSphere Commerce Payments a partir do WebSphere Administration Console.
5. Inicie novamente o servidor de aplicativos WebSphere Commerce a partir do WebSphere Administration Console.

Consulte a documentação do servidor IBM HTTP para obter informações adicionais e opções adicionais sobre como definir restrições e parâmetros de filtragem para certificados.

---

## Atualizando o Status de Usuários do Certificado X.509

Utilizando o WebSphere Commerce Accelerator, um administrador do site pode atualizar o status de um usuário de certificado X.509 para um dos três valores de status a seguir:

**Válido**

O usuário pode acessar um site protegido do WebSphere Commerce com seu certificado.

**Revogado**

O usuário não pode acessar o site do WebSphere Commerce. Quando um usuário do certificado revogado tenta efetuar logon, recebe uma página de erro do certificado X.509.

**Expirado**

O usuário não pode acessar o site do WebSphere Commerce. Quando um usuário do certificado expirado tenta efetuar logon, recebe uma página de erro do certificado X.509.

Ao administrar certificados X.509, também é possível definir restrições e filtrar parâmetros para portadores de certificados. Por exemplo, você também pode permitir que determinados tipos de portadores de certificados acessem seu site protegido, modificando o arquivo de configuração `httpd.conf`.

Para obter informações e instruções adicionais, consulte a documentação do servidor Web.

---

## Um Cenário de Autenticação Típico

As seguintes etapas ilustram um cenário de autenticação típico para certificados X.509:

1. Um comprador acessa:
  - Um URL não protegido através de `http://`  
Nenhuma autenticação é executada.
  - Um URL protegido através de `https://`  
O comprador é solicitado a selecionar um certificado de cliente.
  - Um comando do URL e é redirecionado para `https://` devido ao modo de acesso de comando do URL  
O comprador é solicitado a selecionar um certificado de cliente.
2. O servidor WebSphere Commerce utiliza as informações do certificado do cliente para ver se o comprador já existe na tabela SHOPPER do WebSphere Commerce:
  - Se o comprador existir com um status de certificado válido, ele será autenticado e o fluxo de compras continuará.
  - Se o comprador não existir:
    - Ele será registrado automaticamente no banco de dados do WebSphere Commerce e o fluxo de compras continuará.

**Nota:** Apenas as informações localizadas na tabela `CERT_X509` são obtidas no certificado. No entanto, as informações de endereço do comprador poderiam ter sido obtidas no certificado do cliente X.509, se estivessem disponíveis.



---

## **Parte 3. Administrando a Autorização de Segurança**

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





---

## Capítulo 9. 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 comercializar 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 diretivas de controle de acesso padrão que são automaticamente carregadas no sistema no momento da criação da instância. Essas diretivas 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 on-line. 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.

---

### 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 diretivas padrão que estão prontas para uso "fora da caixa", como também as ferramentas e a capacidade de personalizar as diretivas 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 após a personalização
Os clientes podem se auto-registrar.	Apenas os administradores de vendedoras podem registrar novos clientes.

<b>O que os usuários têm permissão para fazer por padrão</b>	<b>O que os usuários têm permissão para fazer após a personalização</b>
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 compradora 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 diretiva de controle de acesso em detalhes.

---

## Capítulo 10. 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 diretivas 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 diretivas 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 iniciar 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. No WebSphere Commerce 5.5, foram introduzidos os modelos de negócios. Após a criação de uma instância, existem modelos de negócios de amostra que os administradores podem publicar que configurarão a estrutura da organização. Para obter informações adicionais sobre modelos de negócios, consulte o “Modelos de Negócios” na página 17.

Em alguns casos, as organizações que se juntam ao seu site podem ser organizações compradoras, 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 estiver utilizando os modelos de negócios de amostra fornecidos, poderá avançar para a próxima seção sobre controle de acesso. Se desejar definir sua própria estrutura de organização, continue com as etapas a seguir.

Para localizar detalhes de como criar organizações, usuários e funções, consulte a ajuda on-line, que está disponível na página Technical Library:

► Business

[http://www.ibm.com/software/webservers/commerce/wc\\_be/lit-tech-general.html](http://www.ibm.com/software/webservers/commerce/wc_be/lit-tech-general.html)

[http://www.ibm.com/software/webservers/commerce/wc\\_pe/lit-tech-general.html](http://www.ibm.com/software/webservers/commerce/wc_pe/lit-tech-general.html)

Também é recomendável consultar o *WebSphere Commerce - Fundamentos*. Para obter uma visão geral dos modelos de negócios, consulte o *WebSphere Commerce Store Development Guide* e o *WebSphere Commerce - Guia de Loja de Exemplo*, respectivamente.

## Definindo uma Organização Vendedora

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

Até agora, vamos considerar que você está configurando uma organização vendedora que não tem nenhuma suborganização. Para configurar a organização vendedora, 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 vendedora exigem aprovação, como processamento de pedidos ou registro de usuários. Esta etapa só é exigida para um site business-to-business. Consulte a ajuda on-line 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. Como você está criando uma organização vendedora, as funções comuns que você pode atribuir incluem Administrador de Vendedora, Vendedor e outras. Consulte "Funções" na página 29 para obter uma lista de 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.
5. Atribua grupos de diretivas à nova organização para que os clientes possam comprar na loja que é gerenciada pela organização. Os grupos de diretivas típicas requeridos são: Grupo de diretivas de gerenciamento e de administração, grupo de diretivas de compras comuns, grupo de diretivas B2C ou grupo de diretivas B2B. Para obter informações adicionais sobre os grupos de diretivas, consulte "Diretivas e Grupos de Controle de Acesso Padrão", na página 213.

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

**Nota:** No WebSphere Commerce Professional Edition, não é possível criar organizações. Uma organização vendedora já será criada para você.

## Definindo uma Organização Compradora

Se você estiver executando um site business-to-business, pode haver uma ou mais organizações compradoras pertencentes ao seu site. (Se você estiver executando um site business-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 compradora para cada empresa. Você pode ter quantas organizações compradoras precisar.

As organizações compradoras são estruturalmente semelhantes a organizações vendedoras. Da mesma forma que as organizações vendedoras, 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 compradoras não têm nenhuma suborganização. Para configurar uma organização compradora, aqui está um esboço do que é necessário fazer:

1. Como foi feito ao criar a organização vendedora, 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 compradora. Uma vez que está criando uma organização compradora, as funções típicas que podem ser atribuídas incluem Administrador de Compradora, Comprador, Autorizador da Compradora, 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 compradora na etapa anterior.
4. Repita todo o procedimento para cada organização compradora que desejar adicionar no seu site.

**Nota:** Em situações normais, as organizações compradoras não precisam ser assinantes de nenhum dos grupos de diretivas, pois herdarão os grupos de diretivas dos quais a Organização Raiz é assinante.

Novamente, todas as etapas descritas acima são executadas a partir do menu Gerenciamento de Acesso no Organization 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 diretivas, um processo conhecido como *controle de acesso*. Nesta próxima seção, analisaremos as diretivas de controle de acesso e sua estrutura básica.

### O Que É uma Diretiva de Controle de Acesso?

Uma diretiva 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, gerenciamento de leilões, atualização de

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

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

## Como Funciona uma Diretiva de Controle de Acesso?

As diretivas 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 diretiva. 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.

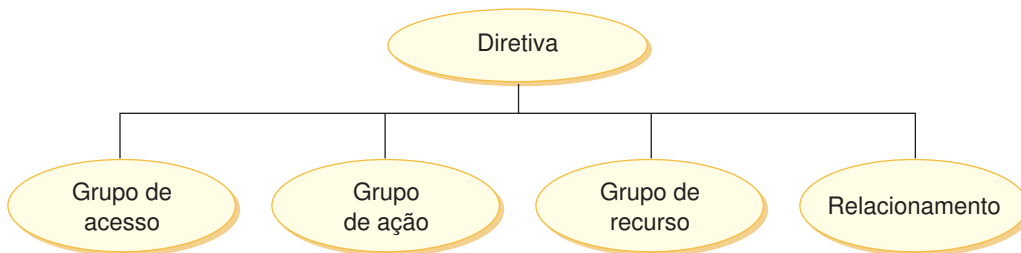


Figura 4. As Quatro Partes de uma Diretiva de Controle de Acesso

Juntas, essas quatro partes definem uma diretiva 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 sobre Autorização”, na página 17.

---

## Como Início a Utilização do Controle de Acesso?

Em alguns casos, não temos que fazer nada! A introdução de modelos de negócios também ajuda a fornecer a estrutura básica de controle de acesso em um sistema, as diretivas padrão no WebSphere Commerce foram projetados para fornecer uma estrutura básica de controle de acesso baseada em usuários comuns em seu sistema e nas atividades que eles desempenham que estão associadas às suas funções em uma organização. As diretivas 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 diretivas 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 diretivas padrão ou personalizá-las, é importante compreender com o que elas se parecem no WebSphere Commerce. Para obter uma consulta mais precisa da diretiva padrão, consulte “Analisando uma Diretiva em Detalhes” na página 42.





---

## Capítulo 11. Personalizando as Diretivas de Controle de Acesso Padrão

As diretivas 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. Frequentemente, as diretivas padrão podem ser suficientes para as necessidades do seu site. Ao mesmo tempo, as diretivas padrão são altamente personalizáveis, o que permite que você as adapte para suas próprias necessidades.

A diretiva `SiteAdministratorsCanDoEverything`, é uma diretiva padrão especial que concede acesso de super-usuário aos administradores com a função `Administrador de Site`. Nesta diretiva, 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 diretivas 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 sobre Autorização”, na página 17 para obter informações adicionais.

---

### Identificando as Diretivas Afetadas por uma Alteração

No Capítulo 3, “Conceitos sobre Autorização”, na página 17, você aprendeu que as diretivas estão frequentemente relacionadas a outras diretivas. Você também aprendeu como iniciar uma diretiva em nível do recurso e a identificar as diretivas baseadas em funções associadas a ela. Nesta seção, explicaremos com detalhes adicionais como as diretivas estão relacionadas uma com as outras e porque você precisa compreender seus relacionamentos antes de poder modificar uma diretiva existente ou criar uma nova. Em muitos casos, você precisa alterar diversas diretivas para implementar adequadamente uma alteração.

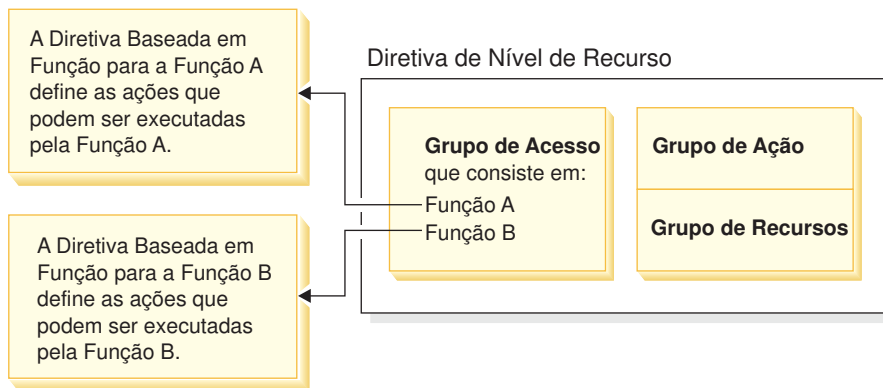
### Compreendendo o Relacionamento entre as Diretivas Baseadas em Funções e em Nível de Recurso

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

- Cada função padrão tem um grupo de acesso correspondente. Por exemplo, o grupo de acesso para a função `Vendedor` é `Sellers`.
- Cada grupo de acesso “baseado em função” geralmente tem duas diretivas com base em funções associadas:
  - Uma diretiva que define os comandos do controlador que a função está autorizada a executar.
  - Uma diretiva que define as ações de exibição que a função está autorizada a executar. Exiba mapa de ações para exibições na tabela `VIEWREG`. Por exemplo, `OperationalReportsHomeRHSView` exibe uma página da Web com a lista de relatórios operacionais, à qual o `Vendedor` possui acesso.

Alguns comandos do controlador possuem apenas uma diretiva baseada na função, mas nenhuma diretiva 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 diretiva 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 diretiva a nível do recurso. .

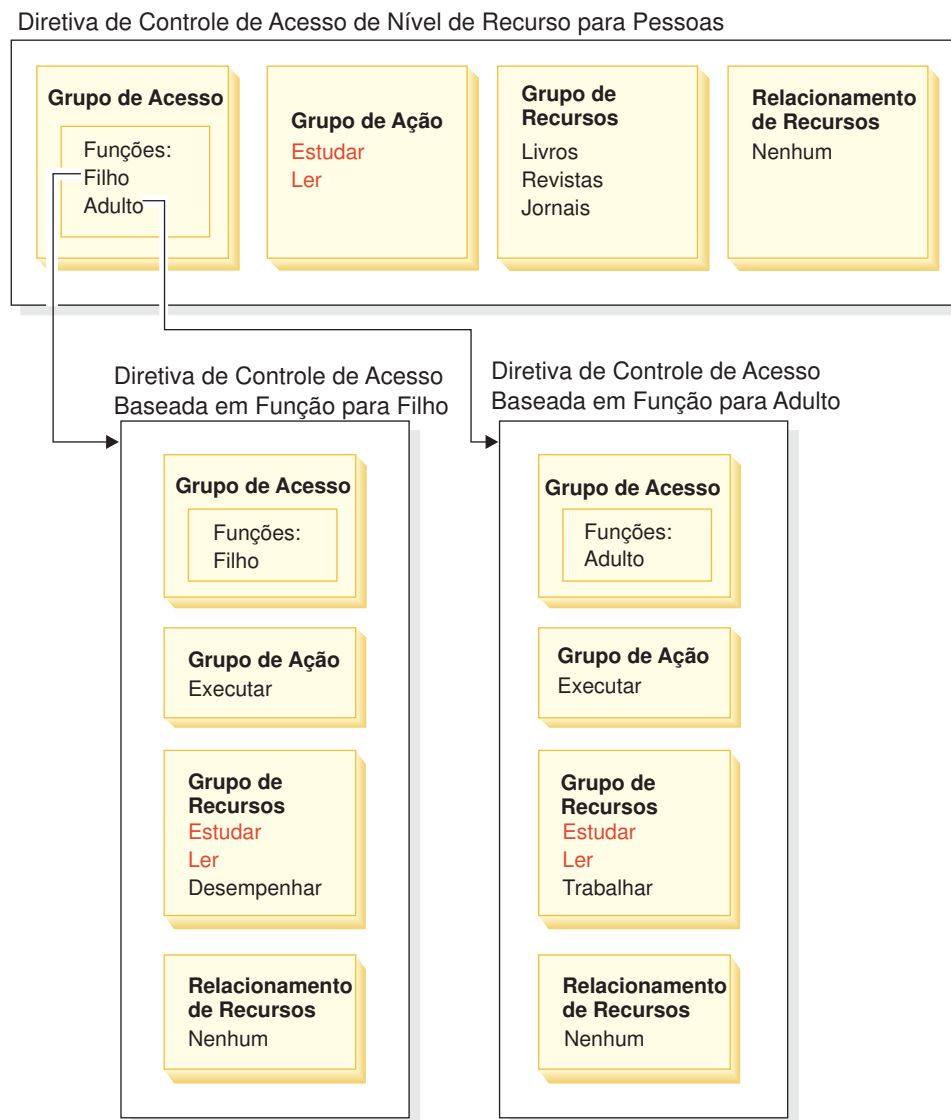
As diretivas a nível do recurso para comandos do controlador estão diretamente relacionadas a determinadas diretivas baseadas em funções para os comandos do controlador. Na diretiva a nível do recurso, o comando do controlador faz parte do grupo de ação, mas na diretiva baseada em funções, o comando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



*Figura 5. Relacionamento Entre uma Diretiva em Nível do Recurso e suas Diretivas Baseadas em Funções Associadas*

A figura a seguir mostra uma amostra de diretiva 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 diretiva é corretamente formulada porque as diretivas baseadas em funções para as funções filho e adulto também as autoriza a ler ou estudar livros, revistas e jornais.

Figura 6. Uma Diretiva em Nível do Recurso e as Diretivas Baseadas em Funções que a Afetam.



Observe que em diretivas 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 diretivas 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 diretivas 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 diretiva em nível do recurso pode apenas autorizar os usuários em uma determinada função para executar ações já autorizadas pela diretiva 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 diretiva 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 diretivas baseadas em funções para duas funções. A diretiva para adulto lista a ação trabalhar no seu grupo de recursos. A diretiva para filho não. Embora filho e adulto sejam adequadamente autorizados pela diretiva em nível do recurso, a diretiva baseada em funções para filho não autoriza a ação trabalhar.

Por causa da forma que as diretivas em nível do recurso estão ligadas às diretivas baseadas em funções, a melhor maneira de acompanhar todas as diretivas afetadas por uma determinada alteração é trabalhar de volta a partir da diretiva em nível do recurso. A primeira etapa é examinar o grupo de acesso da diretiva 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 Organization Administration Console.

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

### **Compreendendo o Modelo da Diretiva**

Uma diretiva 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** diretiva fornecer a autorização necessária. Contudo, se você definir uma diretiva nova mais limitada do que a padrão, deverá excluir ou modificar a diretiva padrão mais ampla para evitar que ela substitua a nova.

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

A tabela a seguir resume as alterações adicionais necessárias a fazer ao criar, excluir ou alterar uma diretiva de nível do recurso.

*Tabela 9. Alterações Adicionais Necessárias Quando Você Altera uma Diretiva em Nível do Recurso que Utiliza as Funções.*

<b>Alterar para uma Diretiva de Nível de Recurso</b>	<b>Alteração Requerida se o Grupo de Acesso de Nível de Recurso Utilizar Funções</b>
Adicionar uma ação no grupo de ação da diretiva.	Garantir que as diretivas baseadas em funções aplicáveis incluam a ação em seus grupos de recursos.
Remover uma ação do grupo de ação da diretiva.	Nenhuma alteração adicional obrigatória. Por coerência, é melhor remover esta ação dos grupos de recurso correspondente nas diretivas 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 diretivas baseadas em funções que ainda precisam ter esta ação em seu grupo de recursos.
Utilizar um grupo de ação diferente.	Garantir que as diretivas baseadas em funções aplicáveis incluam em seus grupos de recursos as novas ações do grupo de ação.
Adicionar uma função no grupo de acesso da diretiva.	Certifique-se de que a diretiva baseada em função correspondente à nova função, refere-se a um grupo de recursos que inclui as ações especificadas na diretiva em nível do recurso.
Remover uma função do grupo de acesso da diretiva.	Nenhuma alteração adicional obrigatória. Por coerência, é melhor modificar a diretiva 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 diretivas baseadas em funções aplicáveis incluam nos seus grupos de recursos as ações no grupo de ação da diretiva em nível do recurso.
Criar uma nova diretiva.	Verificar se há uma diretiva existente que autorize as mesmas ações. Excluir, se necessário.
Exclua a diretiva.	Para impedir que alguns usuários executem essas ações da diretiva, excluir quaisquer outras diretivas que autorizem as mesmas ações.

## **Determinando se uma Diretiva é Baseada em Funções ou em Nível do Recurso**

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

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

### **Diretivas Baseadas em Funções**

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

<AccessGroupforRoleXYZ> Execute <XYZCmdResourceGroup>

Por exemplo: ProductManagersExecuteProductManagersCmdResourceGroup.

Nas diretivas 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 diretivas que definem as exibições que uma função pode executar seguem a convenção de nomenclatura:

<AccessGroupforRoleXYZ> Execute <XYZViews>

Por exemplo: SalesManagersExecuteSalesManagersViews.

O grupo de recursos contém um único recurso, denominado:  
com.ibm.commerce.command.ViewCommand .

## Diretivas em Nível do Recurso

As diretivas 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 diretivas 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 diretivas que autorizam a criação de uma entidade como um pedido, um lance ou uma RFQ. Essas diretivas 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 diretivas têm nomes como:

<AccessGroupXYZs> Execute <XYZCommands> On <StoreEntityResource>

Por exemplo:

AuctionAdministratorsForOrgExecuteAuctionCreateCommandsOnStoreEntityResource

.

As diretivas 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 Diretivas Padrão

Fique ciente do seguinte ao alterar suas diretivas 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 29.
- Antes de alterar uma diretiva 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 Organization Administration Console.
- Dependendo do valor selecionado para Exibir, a página Diretivas lista as diretivas pertencentes à organização selecionada. Ela não distingue entre diretivas de nível do site e diretivas específicas a uma organização particular.
- Renomeie quaisquer diretivas padrão alteradas de forma que o nome da diretiva reflita o que a diretiva faz e que você possa identificar as diretivas padrão que você alterou. Considere implementar uma convenção de nomenclatura para suas diretivas personalizadas. Se adequado, você também deve modificar a descrição da diretiva e seu nome de exibição.

**Nota:** O menu da diretiva de controle de acesso é movido ao Organization Administration Console. O Organization Administration Console pode executar apenas modificações simples para as definições das diretivas de controle de acesso e definições dos grupos 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.
3. Atribuindo uma nova diretiva a um grupo de diretivas.

---

## Depois de Fazer as Alterações na Diretiva

Após a criação de uma nova diretiva, a nova diretiva deve ser atribuída a um grupo de diretivas, antes de ter efeito. É necessário atribuir uma nova diretiva a um grupo que serve à finalidade da diretiva. Para obter informações adicionais sobre os nomes de grupos de diretivas, consulte “Diretivas e Grupos de Controle de Acesso Padrão”, na página 213.

Cada vez que você criar ou modificar uma diretiva de controle de acesso, deverá executar determinados testes para verificar se a diretiva está funcionando corretamente. Após ter terminado de testar todas as suas diretivas 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 diretiva de controle de acesso inicial:

defaultAccessControlPolicies.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 diretiva armazenadas nos bancos de dados. Os arquivos XML que foram utilizados para carregar as diretivas 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 do WebSphere Commerce, a diretiva 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 diretivas e partes de componentes; portanto, manter os arquivos atualizados é essencial.

## Testando as Alterações da Diretiva

Para cada diretiva, certifique-se do seguinte:

- Um usuário que pertence ao grupo de acesso da diretiva 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 diretiva 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 diretiva estiver funcionando corretamente, suas tentativas falharão.

## Extraindo as Alterações das Diretivas em Arquivos XML

Quando tiver concluído e testado suas alterações na diretiva, você deverá atualizar os arquivos XML para mantê-los em sincronia com as informações da diretiva nos bancos de dados. Para obter uma descrição de arquivos XML diferentes, relacionados às diretivas de controle de acesso e grupos de acesso, consulte Capítulo 13, “Personalizando as Diretivas de Controle de Acesso Utilizando o XML”, na página 139. Explicações sobre como extrair alterações de diretivas dos bancos de dados em arquivos XML e como carregar as informações de diretivas dos arquivos XML em bancos de dados também estão incluídas.



---

## Capítulo 12. Personalizando as Diretivas de Controle de Acesso Utilizando a GUI

Os cenários apresentados abaixo permitem aplicar o que você aprendeu sobre as diretivas de controle de acesso para fazer uma série de alterações básicas em suas diretivas padrão utilizando a GUI. Se desejar fazer alterações sofisticadas, será necessário utilizar o XML. Consulte Capítulo 13, “Personalizando as Diretivas de Controle de Acesso Utilizando o XML”, na página 139.

Para todos esses cenários, presume-se que o Administrador do Site esteja modificando as diretivas 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 10. Tabela de Conteúdo para Cenários*

Área de Negócios	Iniciando na Página
Leilões	“Cenário 1 de Leilões: Removendo a Capacidade dos Administradores de Leilões para Fechar o Lance do Leilão” na página 110
Contratos	“Cenário 1 de Contratos: Remover a Habilidade dos Gerenciadores de Contratos em Adicionar ou Excluir Anexos a Contratos” na página 114
Pedidos	“Cenário 1 de Pedidos: Permitindo que Apenas Compradores Criem Pedidos” na página 116
Associação	“Cenário 1 de Associação: Remover a Capacidade dos Usuários de Auto-Registrem” na página 122
Cupons	“Cenário 1 de Cupons: Permitindo que Apenas Compradores Resgatem Cupons” na página 127
Aquisição	“Cenário 1 de Aquisição: Permitindo que os Gerentes de Carrinho de Compras Gerenciem o Carrinho de Compras de Aquisição para Pedidos Criados por sua Organização” na página 131
Estoque	“Cenário 1 de Estoque: Permitir que os Gerentes do Centro de Distribuição Atualizem os Centros de Distribuição, Mas Não os Exclua” na página 134
Inteligência de negócios	“Cenário 1 Inteligência de Negócios: Permitindo que Auditores Exibam os Relatórios de Inteligência de Negócios” na página 136

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 11. Cenários de Personalização Organizados por Tipo de Personalização*

<b>Personalização</b>	<b>Consulte a Página</b>
Adicionando uma função em um grupo de acesso de diretiva	129
Alterando o grupo de ação de uma diretiva	132,134
Alterando o relacionamento de recursos de uma diretiva	118,131
Alterando uma diretiva para utilizar um grupo de acesso diferente	112,116,118,123,127,129
Criando um novo grupo de acesso e utilizando-o em uma diretiva	121,124
Criando um novo grupo de ação e utilizando-o em uma diretiva	124,132
Criando uma nova diretiva em nível do recurso	115,132
Criando uma nova diretiva baseada em funções	124,136
Criando uma nova função e utilizando-a em uma diretiva em nível do recurso	124,136
Excluindo uma diretiva	111,123
Removendo uma ação de um grupo de ação da diretiva	3,114

**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 diretiva 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 diretiva.
3. Exclua a ação para fechar o lance de leilão a partir do grupo de ação da diretiva.

### **Etapas a Serem Executadas**

#### **Identificar a Diretiva Cujo Grupo de Ação Deve Ser Alterado**

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

AuctionAdministratorsForOrgExecuteAuctionManageCommandsOnAuctionResource

2. A partir do Organization Administration Console, clique em **Gerenciamento de Acesso > Diretivas**.
3. Para Exibir, selecione **Organização Raiz** para exibir as diretivas que ela possui.
4. Localize a diretiva na lista.
5. Anote o nome do grupo de ação da diretiva — 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 Diretiva**

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 Ação.
4. Na lista Ações Seleccionadas, selecione **com.ibm.commerce.negotiation.commands.CloseBiddingCmd**.
5. Clique em **Remover**.
6. Clique em **OK**.

### **Atualizar o Registro da Diretiva com suas Alterações**

1. Efetue logon no Administration Console.
2. Clique em **Configuração > Registro**.
3. Da lista de registros, selecione **Diretivas de Controle de Acesso**.
4. Clique em **Atualizar**.

---

## **Cenário 2 de Leilões: Removendo a Habilidade dos Gerenciadores de Leilão em Retirar Lances**

Por padrão, os gerenciadores de leilão para uma loja podem retirar lances submetidos em seus leilões. Em alguns casos, talvez você não queira conceder esta autoridade a ninguém. Para fazer esta alteração, você deve localizar a diretiva 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 diretiva. Conseqüentemente, você teve apenas que remover a ação do grupo de ação da diretiva. Neste cenário, no entanto, uma diretiva inteira controla a retirada do lance. No entanto, você deve excluir uma diretiva, não apenas uma ação.

Para excluir a diretiva, é necessário fazer o seguinte:

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

**Nota:** Antes de excluir a diretiva, 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 diretiva em nível do recurso a ser alterada. A diretiva é:

AuctionManagersForOrgExecuteAdminRetractBidCommandsOnAuctionResource

2. A partir do Organization Administration Console, clique em **Gerenciamento de Acesso > Diretivas**.
3. Para Exibir, selecione **Organização Raiz** para exibir as diretivas que ela possui.
4. Da lista de diretivas, selecione o seguinte:  
`AuctionManagersForOrgExecuteAdminRetractBidCommandsOnAuctionResource`
5. Clique em **Excluir**.

### **Atualizar o Registro da Diretiva com suas Alterações**

1. Efetue logon no Administration Console.
2. Clique em **Configuração > Registro**.
3. Da lista de registros, selecione **Diretivas de Controle de Acesso**.
4. Clique em **Atualizar**.
5. Repita as etapas 3 e 4 para o **Registro de Grupos de Diretivas de Controle de Acesso**.

---

## **Cenário 3 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 diretiva em nível do recurso, bem como sua diretiva 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 diretiva em nível do recurso que especifica quem pode criar um lance de leilão.
- Altere o grupo de acesso da diretiva de todos os usuários registrados para aqueles com a função comprador.
- Renomeie a diretiva, descrição e o nome de exibição.
- Identifique o comando para criar lances.
- Utilize o Apêndice para localizar a diretiva baseada em funções para compradores (buy-side). Esta diretiva define os comandos que os usuários com a função Comprador (buy-side) podem executar. Você deve atualizar este grupo de recursos da diretiva para permitir que os compradores executem o comando para criar lances.
- Atualize o grupo de recursos da diretiva baseada nesta função para incluir o comando para criar lances.

## **Etapas a Serem Executadas**

### **Identificar a Diretiva em Nível do Recurso**

1. Procure Leilões, no Apêndice, para identificar a diretiva em nível do recurso a ser alterada. A diretiva é:  
`RegisteredApprovedUsersExecuteBidCreateCommandsOnAuctionResource`.
2. A partir do Organization Administration Console, clique em **Gerenciamento de Acesso > Diretivas**.
3. Para Exibir, selecione **Organização Raiz** para exibir as diretivas que ela possui.
4. Na lista de diretivas, selecione  
`RegisteredApprovedUsersExecuteBidCreateCommandsOnAuctionResource`.

5. Anote o nome do grupo de ação da diretiva — 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 Diretiva**

1. Clique em **Alterar** para exibir a página Alterar Diretiva.
2. Para Grupos de Usuários, clique em **Localizar** e selecione **Compradores (lado de compra)**.
3. Clique em **OK**.
4. Renomeie a diretiva, o nome de exibição e a descrição da diretiva, 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 adicionar este comando ao grupo de recursos que contém a lista de comandos que um comprador pode executar.

### **Identificar a Diretiva Baseada em Funções e o Grupo de Recursos para a Função dos Compradores (Lado de Compra)**

1. Procure Diretivas Baseadas em Funções, no Apêndice, para localizar a diretiva baseada em funções para compradores (buy-side). A diretiva é:  
`Buyers(buy-side)ExecuteBuyers(buy-side)CommandsResourceGroup`.
2. Clique em **Gerenciamento de Acesso > Diretivas**.
3. Para Exibir, selecione **Organização Raiz** para exibir as diretivas 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 Diretiva 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 **Adicionar** para adicioná-lo no grupo de recursos.
7. Clique em **Concluir**.

### **Atualizar o Registro da Diretiva de Controle de Acesso com suas Alterações**

1. Efetue logon no Administration Console.
2. Clique em **Configuração > Registro**.
3. Da lista de registros, selecione **Diretivas de Controle de Acesso**.
4. Clique em **Atualizar**.

---

## Cenário 1 de Contratos: Remover a Habilidade dos Gerenciadores de Contratos em Adicionar ou Excluir Anexos a Contratos

Por padrão, os gerenciadores de contrato para uma loja podem adicionar ou excluir anexos aos contratos que gerenciam. Em alguns casos, é possível que você não queira conceder essa autoridade aos gerenciadores de contratos.

Neste cenário, você irá alterar uma diretiva de nível do recurso que define as ações que um gerenciador de contratos pode executar. Para remover a autoridade de gerenciadores de contratos para adicionar ou excluir anexos de contratos, é necessário fazer o seguinte:

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

### Etapas a Serem Executadas

#### Identificar a Diretiva em Nível do Recurso e o Grupo de Ação

1. Procure em Contratos, no Apêndice, para identificar a diretiva em nível do recurso a ser alterada. A diretiva é:  
`ContractManagersForOrgExecuteContractManageCommandsOnContractResource`
2. A partir do Organization Administration Console, clique em **Gerenciamento de Acesso > Diretivas**.
3. Para Exibir, selecione **Organização Raiz** para exibir as diretivas que ela possui.
4. Localize a diretiva na lista.
5. Anote o nome do grupo de ação da diretiva —`ContractManage`. Este é o grupo de ação que você precisa alterar para remover as ações para adicionar e excluir conexões.

#### Remover as Ações para Adicionar e Excluir Conexões do Grupo de Ação da Diretiva

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 Diretiva de Controle de Acesso com suas Alterações

1. Efetue logon no Administration Console.
2. Clique em **Configuração > Registro**.
3. Da lista de registros, selecione **Diretivas de Controle de Acesso**.
4. 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 diretivas 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 diretiva que define quem pode implementá-los.
- Você pode adicionar a ação implementar contrato na diretiva que especifica as ações que um administrador de contratos pode executar.
- Você pode criar uma nova diretiva que permite que os administradores de contratos implemente-os.

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

Para criar esta diretiva, será necessário fazer o seguinte:

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

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

#### Definir a Nova Diretiva

1. Clique em **Novo** para exibir a página Nova Diretiva.
2. Para Nome, especifique:  
`ContractAdministratorsForOrgExecuteContractDeployCommandsOnContractResource`

3. Para Nome de Exibição, especifique uma descrição resumida da diretiva em seu idioma local.
4. Para Descrição, especifique uma descrição mais longa do que a diretiva 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 Diretiva, selecione **Diretiva de Gabarito Agrupável** para designar a diretiva como uma diretiva de gabarito.
10. Clique em **OK**.

### **Atualizar o Registro da Diretiva de Controle de Acesso com suas Alterações**

1. Efetue logon no Administration Console.
2. Clique em **Configuração > Registro**.
3. Da lista de registros, selecione **Diretivas de Controle de Acesso**.
4. Clique em **Atualizar**.

**Nota:** Essa nova diretiva deve ser atribuída a um grupo de diretivas antes dessa ter efeito. A atribuição de diretivas deve ser feita através do XML. Consulte para obter informações adicionais.

---

## **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 usuários com a função Comprador, é necessário fazer o seguinte:

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



## Etapas a Serem Executadas

### Identificar a Diretiva em Nível do Recurso

1. Procure Pedidos, no Apêndice, para identificar a diretiva em nível do recurso a ser alterada. A diretiva é: `AllUsersExecuteOrderCreateCommandsOnStoreResource`.
2. A partir do Organization Administration Console, clique em **Gerenciamento de Acesso > Diretivas**.
3. Para Exibir, selecione **Organização Raiz** para exibir as diretivas que ela possui.
4. Na lista de diretivas, selecione **AllUsersExecuteOrderCreateCommandsOnStoreResource**. Anote o nome do grupo de ação da diretiva —`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 Diretiva.
2. Para Grupos de Usuários, clique em **Localizar** e selecione **Compradores (lado de compra)**.
3. Clique em **OK**.
4. Atualize o nome da diretiva, 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
com.ibm.commerce.orderitems.commands.OrderItemAddCmd
com.ibm.commerce.orderquotation.commands.OrderQuotationCreateCmd
```

Você deve adicionar 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 Diretiva Baseada em Funções para Compradores (Lado de Compra)

1. Procure Diretivas Baseadas em Funções, no Apêndice, para localizar a diretiva baseada em funções para compradores (buy-side). A diretiva é: `Buyers(buy-side)ExecuteBuyers(buy-side)CommandsResourceGroup`.
2. Clique em **Gerenciamento de Acesso > Diretivas**.
3. Para Exibir, selecione **Organização Raiz** para exibir as diretivas em nível de site.
4. Localize a diretiva na lista.

5. Anote o nome do grupo de recursos—Buyers(buy-side)CommandsResourceGroup. Este é o grupo de recursos que você precisa atualizar.

### **Atualizar o Grupo de Recursos na Diretiva 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(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 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  
com.ibm.commerce.orderitems.commands.OrderItemAddCmd  
com.ibm.commerce.orderquotation.commands.OrderQuotationCreateCmd
```

6. Clique em **Adicionar**.
7. Clique em **Concluir**.

### **Atualizar o Registro da Diretiva de Controle de Acesso com suas Alterações**

1. Efetue logon no Administration Console.
2. Clique em **Configuração > Registro**.
3. Da lista de registros, selecione **Diretivas de Controle de Acesso**.
4. 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 diretiva em nível de recurso, bem como uma diretiva baseada em funções. Para permitir apenas que os administradores de comprador modifiquem pedidos pertencentes a membros de uma organização compradora, é necessário fazer o seguinte:

- Utilize o Apêndice para localizar a diretiva em nível de recurso que especifica quem pode modificar um pedido.
- Altere o grupo de acesso da diretiva 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 diretiva, o nome da exibição e a descrição.

- Identifique os comandos para modificar pedidos.
- Utilize o Apêndice para localizar a diretiva baseada em funções para o administrador de comprador. Essa diretiva define os comandos que os usuários com a função de administrador de comprador podem executar. Você deve atualizar este grupo de recursos da diretiva para permitir que os administradores de comprador executem os comandos para modificar os pedidos.
- Atualize o grupo de recursos da diretiva baseada em funções para incluir os comandos para modificar pedidos.

## Etapas a Serem Executadas

### Identificar a Diretiva em Nível do Recurso

1. Procure Pedidos, no Apêndice, para identificar a diretiva em nível do recurso a ser alterada. A diretiva é: `AllUsersExecuteOrderWriteCommandsOnOrderResource`.
2. A partir do Organization Administration Console, clique em **Gerenciamento de Acesso > Diretivas**.
3. Para Exibir, selecione **Organização Raiz** para exibir as diretivas que ela possui.
4. Na lista de diretivas, selecione **AllUsersExecuteOrderWriteCommandsOnOrderResource**.
5. Anote o nome do grupo de ação da diretiva —`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 Diretiva.
2. Para Grupo de Usuários, clique em **Localizar** e selecione **Administradores de Comprador**.
3. Clique em **OK**.
4. Para Relacionamento, selecione **Nenhum**.
5. Atualize o nome da diretiva, o nome da exibição e a descrição para refletir a alteração do grupo de acesso.
6. 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
com.ibm.commerce.orderquotation.commands.OrderItemSelectCmd
```

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

**Nota:** 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 Diretiva Baseada em Funções para a Função de Administrador de Compradores

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

## Atualizar o Grupo de Recursos na Diretiva 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`  
`com.ibm.commerce.orderquotation.commands.OrderItemSelectCmd`
6. Clique em **Adicionar** para adicionar o comando no grupo de recursos.
7. Clique em **Concluir**.

## Atualizar o Registro da Diretiva de Controle de Acesso com suas Alterações

1. Efetue logon no Administration Console.
2. Clique em **Configuração > Registro**.
3. Da lista de registros, selecione **Diretivas de Controle de Acesso**.
4. Clique em **Atualizar**.

---

## Cenário 3 de Pedidos: Permitindo que Aprovadores RMA Aprovevem 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 diretiva em nível do recurso. Para permitir que aprovadores de RMA aprovevem RMAs em qualquer loja, será necessário fazer o seguinte:

- Utilize o Apêndice para localizar a diretiva 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 diretiva.
- Exiba o grupo de acesso da diretiva, `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 diretiva utilizando:
  - O novo grupo de acesso, `RMAApprovers`
  - O grupo de ação da diretiva existente
  - O grupo de recursos da diretiva existente

## Etapas a Serem Executadas

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

1. Procure Pedidos, no Apêndice, para localizar a diretiva em nível do recurso que autoriza `RMAApproversForOrg` para aprovar RMAs para suas lojas. A diretiva é: `RMAApproversForOrgExecuteRMAApproveCommandsOnRMAResource`
2. A partir do Organization Administration Console, clique em **Gerenciamento de Acesso > Diretivas**.
3. Para Exibir, selecione **Organização Raiz** para exibir as diretivas que ela possui.
4. Localize a diretiva na lista.
5. Anote o nome do grupo de ação da diretiva—`RMAApproveCommands`. Este é o grupo de ação que você utilizará na definição da nova diretiva.
6. Anote o nome do grupo de recursos—`RMADataResourceGroup`. Este é o grupo de recursos que você utilizará na definição da sua nova diretiva.
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 Diretiva

1. Clique em **Gerenciamento de Acesso > Diretivas**.
2. Clique em **Novo** para exibir a página Nova diretiva.
3. Para Nome, especifique:  
RMAApproversExecuteRMAApproveCommandsOnRMAResource
4. Para Nome de Exibição, especifique uma descrição resumida da diretiva em seu idioma local.
5. Para Descrição, especifique uma descrição mais longa do que a diretiva 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 Diretiva de Controle de Acesso com suas Alterações

1. Efetue login no Administration Console.
2. Clique em **Configuração > Registro**.
3. Da lista de registros, selecione **Diretivas de Controle de Acesso**.
4. Clique em **Atualizar**.

---

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

Por padrão, os usuários têm permissão para se auto-registarem 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 Vendedora.

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

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

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

## Etapas a Serem Executadas

### Excluir a Diretiva

1. Procure Associação, no Apêndice, para localizar a diretiva em nível do recurso que permite aos usuários se auto-registrem. A diretiva é: `GuestsExecuteUserSelfRegistrationCommandsOnOrganizationResource`.
2. A partir do Organization Administration Console, clique em **Gerenciamento de Acesso > Diretivas**.
3. Para Exibir, selecione **Organização Raiz** para exibir as diretivas que ela possui.
4. Na lista de diretivas, selecione `GuestsExecuteUserSelfRegistrationCommandsOnOrganizationResource`
5. Clique em **Excluir**.

### Atualizar o Registro da Diretiva de Controle de Acesso com suas Alterações

1. Efetue logon no Administration Console.
2. Clique em **Configuração > Registro**.
3. Da lista de registros, selecione **Diretivas de Controle de Acesso**.
4. Clique em **Atualizar**.
5. Repita as etapas 3 e 4 para o **Registro de Grupos de Diretivas de Controle de Acesso**.

---

## 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 diretiva em nível do recurso que autoriza os usuários a gerenciar suas informações de endereço, como segue:

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

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

## Etapas a Serem Executadas

### Alterar o Grupo de Acesso da Diretiva em Nível do Recurso

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

**Nota:** Usuários não rejeitados são usuários cujo registro não foi rejeitado. Seu registro foi aprovado ou está pendente de aprovação.

2. A partir do Organization Administration Console, clique em **Gerenciamento de Acesso > Diretivas**.
3. Para Exibir, selecione **Organização Raiz** para exibir as diretivas que ela possui.
4. Na lista de diretivas, selecione **NonRejectedUsersExecuteAddressManageCommandsOnUserResource**.
5. Clique em **Alterar** para exibir a página Alterar Diretiva.
6. Para Grupo de Usuários, clique em **Localizar** e selecione **RegisteredApprovedUsers**.
7. Clique em **OK**.
8. Atualize o nome da diretiva, o nome da exibição e a descrição para refletir a alteração do grupo de acesso.
9. Clique em **OK**.

### Atualizar o Registro da Diretiva de Controle de Acesso com suas Alterações

1. Efetue logon no Administration Console.
2. Clique em **Configuração > Registro**.
3. Da lista de registros, selecione **Diretivas de Controle de Acesso**.
4. 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 compradora e de vendedora, 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 diretiva baseada em funções.
- Modifique uma diretiva 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 diretiva 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 diretiva baseada em funções para a nova função. Tenha em mente que, nas diretivas 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 `UserAdminRegistrationCommands`, que inclui o comando para registrar membros. Você utilizará este grupo de recursos na diretiva baseada em funções para a função de registro de membros.
- Defina uma nova diretiva baseada em funções para registradores de membros, que utiliza o grupo de acesso `MemberRegistrars` e o grupo de recursos `MemberRegistrationCommands`.
- Modifique a diretiva 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. A partir do Organization 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 ser desempenhada na organização do usuário ou em seus ascendentes.
10. Clique em **Concluir**.

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

1. Procure Associação, no Apêndice, para localizar a diretiva que permite aos administradores de associação registrarem usuários. A diretiva é:  
`CSAMembershipAdministratorsForOrgExecuteUserAdminRegistrationCommandsOnOrganizationResource`
2. Clique em **Gerenciamento de Acesso > Diretivas**.
3. Para Exibir, selecione **Organização Raiz** para exibir as diretivas em nível de site.

4. Localize a diretiva na lista.
5. Anote o nome do grupo de ação da diretiva—`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 Diretiva 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 **Adicionar**.
11. Clique em **Concluir**.

### **Definir uma Diretiva Baseada em Funções para a Função de Registrador de Membros**

1. Clique em **Gerenciamento de Acesso > Diretivas**.
2. Na página Diretivas, clique em **Novo**.
3. Para Nome, especifique **MemberRegistrarsExecuteUserAdminRegistrationCommands**.
4. Para Nome de Exibição, especifique uma descrição da diretiva em seu idioma local.
5. Para Descrição, especifique uma descrição mais longa do que a diretiva 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**.

**Nota:** Após a criação dessa nova diretiva, ela deve ser atribuída a um grupo de diretivas antes de ter efeito. Isso deve ser feito através do XML. Para obter informações adicionais, consulte Capítulo 13, “Personalizando as Diretivas de Controle de Acesso Utilizando o XML”, na página 139.

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

Após modificar a diretiva de nível do recurso, apenas aos usuários que utilizam a função Registrar Membros na mesma organização que o recurso será permitido registrar o usuário. Usuários que utilizam a função em qualquer outra organização não estarão aptos a isso.

1. Da lista de diretivas, selecione o seguinte:

```
CSAMembershipAdministratorsForOrgExecuteUserAdmin  
RegistrationCommandsOnOrganizationResource
```

2. Clique em **Alterar** para exibir a página Alterar Diretiva.
3. Atualize o nome da diretiva, 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 Diretiva de Controle de Acesso com suas Alterações

1. Efetue logon no Administration Console.
2. Clique em **Configuração > Registro**.
3. Da lista de registros, selecione **Diretivas de Controle de Acesso**.
4. Clique em **Atualizar**.

---

## Cenário 1 de Cupons: Permitindo que Apenas Compradores Resgatem Cupons

Por padrão, todos os usuários têm permissão para resgatar cupons. Em alguns casos, é possível que você queira limitar o resgate de cupons para usuários com a função de Comprador no WebSphere Commerce.

Neste cenário, você irá alterar uma diretiva em nível do recurso, bem como sua diretiva 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 diretiva em nível do recurso que especifica quem pode resgatar um cupom.
- Altere o grupo de acesso da diretiva de todos os usuários para aqueles com a função Comprador.
- Identifique o comando para resgatar cupons.
- Utilize o Apêndice para localizar a diretiva baseada em funções para Compradores (lado de compra). Esta diretiva define os comandos que os usuários com a função Comprador (buy-side) podem executar. Você deve atualizar este grupo de recursos da diretiva para permitir que os compradores executem o comando para resgatar cupons.
- Atualize o grupo de recursos da diretiva baseada nesta função para incluir os comandos para resgatar cupons.

## Etapas a Serem Executadas

### Identificar a Diretiva em Nível do Recurso e seu Grupo de Ação

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

AllUsersExecuteCouponRedemptionCommandsOnCouponWalletResource

2. A partir do Organization Administration Console, clique em **Gerenciamento de Acesso > Diretivas**.
3. Para Exibir, selecione **Organização Raiz** para exibir as diretivas que ela possui.
4. Da lista de diretivas, selecione o seguinte:  
**AllUsersExecuteCouponRedemptionCommandsOnCouponWalletResource**
5. Anote o nome do grupo de ação da diretiva— 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 Diretiva.
2. Para Grupos de Usuários, clique em **Localizar** e selecione **Compradores (lado de compra)**.
3. Clique em **OK**.
4. Atualize o nome da diretiva, 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 adicionar esses comandos ao grupo de recursos que contém a lista de comandos que um comprador pode executar.

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

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

### Atualizar o Grupo de Recursos na Diretiva 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 **Adicionar** para adicionar os comandos no grupo de recursos.
7. Clique em **Concluir**.

### **Atualizar o Registro da Diretiva de Controle de Acesso com suas Alterações**

1. Efetue logon no Administration Console.
2. Clique em **Configuração > Registro**.
3. Da lista de registros, selecione **Diretivas de Controle de Acesso**.
4. Clique em **Atualizar**.

---

## **Cenário 2 de Cupons: Permitindo que Administradores de Cupons e Gerenciadores de Operações Criem Promoções com Cupons Eletrônicos**

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

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

- Você pode adicionar a função de Gerenciador de Operações ao grupo de acesso para a diretiva que especifica quem pode criar promoções com cupons eletrônicos.
- Você pode criar uma nova diretiva que permite aos Gerenciadores de Operações criarem promoções com cupons eletrônicos.

Este cenário ilustra a primeira abordagem. Ele mostra como adicionar a função de Gerenciador de Operações na diretiva de 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 diretiva em nível do recurso que especifica quem pode criar promoções com cupons eletrônicos.
- Altere o grupo de acesso da diretiva para incluir usuários na função de Gerenciador de Operações.
- Exiba o grupo de ação da diretiva em nível do recurso para identificar o comando para criar promoções com cupons eletrônicos.
- Utilize o Apêndice para localizar a diretiva baseada em funções para um Gerenciador de Operações. Essa diretiva define os comandos que os usuários com a função de Gerenciador de Operações podem executar. Você deve atualizar este grupo de recursos da diretiva para permitir que os administradores de loja executem os comandos para criar promoções com cupons eletrônicos.
- Atualize o grupo de recursos da diretiva 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 Diretiva em Nível do Recurso

1. Procure Leilões, no Apêndice, para identificar a diretiva em nível do recurso a ser alterada. A diretiva é:  
`CouponAdministratorsForOrgExecuteCouponPromotionCreateCommandsOnStoreEntityResource`
2. A partir do Organization Administration Console, clique em **Gerenciamento de Acesso > Diretivas**.
3. Para Exibir, selecione **Organização Raiz** para exibir as diretivas que ela possui.
4. Localize a diretiva na lista.
5. Anote o nome do grupo de ação da diretiva—`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 diretiva—`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 **Gerenciador de Operações**.
6. Clique em **Para Organização** para especificar que a função deve ser desempenhada com a organização do recurso ou seus ascendentes.
7. Clique em **Adicionar**.
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`. É necessário adicionar esse comando ao grupo de recursos que contém a lista de comandos que um Gerenciador de Operações pode executar.

### Identificar a Diretiva Baseada em Funções para Gerenciadores de Operações

1. Procure Diretivas Baseadas em Funções no Apêndice para localizar a diretiva baseada em funções para Gerenciadores de Operações. A diretiva é:  
`OperationsManagersExecuteOperationsManagersCmdResourceGroup`.
2. Clique em **Gerenciamento de Acesso > Diretivas**.
3. Para Exibir, selecione **Organização Raiz** para exibir as diretivas em nível de site.
4. Localize a diretiva na lista.

5. Anote o nome do seu grupo de recursos—`OperationsManagersCmdResourceGroup`. Este é o nome do grupo de recursos que você precisa atualizar.

### **Atualizar o Grupo de Recursos na Diretiva 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 **OperationsManagersCmdResourceGroup**.
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 **Adicionar**.
7. Clique em **Concluir**.

### **Atualizar o Registro da Diretiva de Controle de Acesso com suas Alterações**

1. Efetue logon no Administration Console.
2. Clique em **Configuração > Registro**.
3. Da lista de registros, selecione **Diretivas de Controle de Acesso**.
4. Clique em **Atualizar**.

---

## **Cenário 1 de Aquisição: Permitindo que os Gerentes de Carrinho de Compras Gerenciem o Carrinho de Compras de Aquisição 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 aquisição são autorizados a gerenciar o carrinho de compras de aquisição quando eles criaram o pedido. Em alguns casos, talvez você possa querer ampliar a autoridade dos gerentes de carrinhos de compras de aquisição para permitir que eles gerenciem o carrinho de aquisição para pedidos criados por qualquer membro de sua organização.

Para efetuar esta alteração, é necessário fazer o seguinte:

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

## **Etapas a Serem Executadas**

### **Alterar o Relacionamento de Recursos para Diretiva em Nível do Recurso**

1. Procure Aquisição, no Apêndice, para localizar a diretiva em nível do recurso que autoriza os gerentes de carrinhos de compras de aquisição a gerenciá-los para pedidos. A diretiva é:  
`ProcurementShoppingCartManagersExecuteProcurementShoppingCartManageOnOrderResource`

2. A partir do Organization Administration Console, clique em **Gerenciamento de Acesso > Diretivas**.
3. Para Exibir, selecione **Organização Raiz** para exibir as diretivas que ela possui.
4. Da lista de diretivas, selecione o seguinte:  
**ProcurementShoppingCartManagersExecuteProcurementShoppingCartManageOnOrderResource**
5. Clique em **Alterar** para exibir a página Alterar Diretiva.
6. Para Relacionamento, selecione **sameOrganizationalEntityAsCreator**.
7. Clique em **OK**.

### **Atualizar o Registro da Diretiva de Controle de Acesso com suas Alterações**

1. Efetue login no Administration Console.
2. Clique em **Configuração > Registro**.
3. Da lista de registros, selecione **Diretivas de Controle de Acesso**.
4. Clique em **Atualizar**.

---

## **Cenário 2 de Aquisição: Permitir Administradores de Compradores de Aquisição a Submeter o Carrinho de Compras de Aquisição 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 aquisição podem salvar ou submeter os carrinhos de compras de aquisição 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 aquisição salvem esses carrinhos contendo pedidos que eles criaram, porém dar aos administradores de compradores de aquisição na mesma organização que o criador do pedido autoridade para submeter o carrinho de compras de aquisição. Isso pode ser benéfico se você quiser que o administrador de compras de aquisição reveja as compras planejadas antes de elas serem submetidas.

Para efetuar esta alteração, é necessário fazer o seguinte:

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

1. Procure Aquisição, no Apêndice, para localizar a diretiva em nível do recurso que autoriza os gerentes de carrinhos de compras de aquisição a gerenciá-los para pedidos. A diretiva é:  
`ProcurementShoppingCartManagersExecuteProcurementShoppingCartManageOnOrderResource`
2. A partir do Organization Administration Console, clique em **Gerenciamento de Acesso > Diretivas**.
3. Localize a diretiva na lista de diretivas.
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 aquisição.
5. Anote o nome do seu grupo de recursos — `OrderDataResourceGroup`. Você utilizará este grupo de recursos para definir a nova diretiva em nível do recurso.

### Atualizar o Grupo de Ação da Diretiva 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 Seleccionadas, 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 diretiva 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 **Adicionar**.
8. Clique em **OK**.

### Definir a Nova Diretiva

1. Clique em **Gerenciamento de Acesso > Diretivas**.
2. Para Exibir, clique em **Organização Raiz** para exibir as diretivas que ela possui.
3. Clique em **Novo** para exibir a página Nova Diretiva.
4. Para Nome, especifique:  
`ProcurementBuyerAdministratorsExecuteProcurementShoppingCartSubmitCommandsOnOrderResource`

5. Para Nome da Exibição, especifique uma descrição resumida da diretiva em seu idioma local.
6. Para Descrição, especifique uma descrição mais longa do que a diretiva 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 Diretiva, selecione **Diretiva de Gabarito Agrupável** para designar a diretiva como uma diretiva de gabarito.
13. Clique em **OK**.

### **Atualizar o Registro da Diretiva de Controle de Acesso com suas Alterações**

1. Efetue logon no Administration Console.
2. Clique em **Configuração > Registro**.
3. Da lista de registros, selecione **Diretivas de Controle de Acesso**.
4. Clique em **Atualizar**.

**Nota:** Após a criação dessa nova diretiva, ela deve ser atribuída a um grupo de diretivas antes de ter efeito. Isso é feito utilizando o XML. Consulte Capítulo 13, “Personalizando as Diretivas de Controle de Acesso Utilizando o XML”, na página 139 para obter informações adicionais.

---

## **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 diretiva 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 diretiva.

### **Etapas a Serem Executadas**

#### **Remover a Ação para Excluir um Centro de Distribuição**

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

```
FulfillmentCenterManagersForOrgExecuteFulfillmentCenter
ManageCommandsOnFulfillmentResource
```
2. A partir do Organization Administration Console, clique em **Gerenciamento de Acesso > Diretivas**.
3. Localize a diretiva na lista de diretivas.

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 Seleccionadas, selecione **com.ibm.commerce.inventory.commands.FulfillmentCenterDeleteCmd**.
9. Clique em **Remover**.
10. Clique em **OK**.

### **Atualizar o Registro da Diretiva de Controle de Acesso com suas Alterações**

1. Efetue logon no Administration Console.
2. Clique em **Configuração > Registro**.
3. Da lista de registros, selecione **Diretivas de Controle de Acesso**.
4. Clique em **Atualizar**.

---

## **Cenário de Inventário 2: Permitir Apenas Gerenciadores de Logística, Gerenciadores de Operações e Representantes de Contas para Criar, Atualizar ou Excluir 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 gerenciador do centro de distribuição inclui as funções: Vendedor, Gerenciador de Logística, Gerenciador de Operações e Representante de Contas. Em alguns casos, é possível que 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 diretiva 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 Aquisição, no Apêndice, para localizar a diretiva em nível do recurso que autoriza os gerentes de carrinhos de compras de aquisição a gerenciá-los para pedidos. A diretiva é:  
FulfillmentCenterManagersForOrgExecuteFulfillmentCenterManage  
CommandsOnFulfillmentResource
2. No Organization 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 Diretiva de Controle de Acesso com suas Alterações**

1. Efetue logon no Administration Console.
2. Clique em **Configuração > Registro**.
3. Da lista de registros, selecione **Diretivas de Controle de Acesso**.
4. 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 (Auditor) e, para ela, um novo grupo de acesso Auditores, um novo grupo de recursos e uma nova diretiva baseada em funções.
- Adicione uma nova função no grupo de acesso da diretiva em nível do recurso.
- Adicione a função Auditor ao grupo de acesso da diretiva de 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 diretiva 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 diretiva baseada em funções para a nova função. Tenha em mente que, nas diretivas 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 diretiva baseada em funções para a função de auditor.
- Defina uma nova diretiva baseada em funções para auditores, que utiliza o grupo de acesso Auditores e o grupo de recursos AuditorCommands.
- Adicione a função de auditor no grupo de acesso para a diretiva 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. A partir do Organization 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—Audidores.
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 **Adicionar**.
10. Clique em **Concluir**.

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

1. Procure Inteligência de Negócios, no Apêndice, para localizar a diretiva que autoriza os visualizadores de relatório de inteligência a exibir os relatórios de inteligência de negócios. A diretiva é:  
`IntelligenceReportViewersForOrgExecuteViewBusinessIntelligenceReport  
CommandsOnStoreEntityResource`
2. A partir do Organization Administration Console, clique em **Gerenciamento de Acesso > Diretivas**.
3. Para Exibir, selecione **Organização Raiz** para exibir as diretivas que ela possui.
4. Localize a diretiva na lista.
5. Anote o nome do grupo de ações da diretiva—`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 Diretiva 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 **Adicionar**.
11. Clique em **Concluir**.

### **Definir a Diretiva Baseada em Funções para a Função do Auditor**

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

### **Adicionar a Função de Auditor no Grupo de Acesso da Diretiva 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 ser desempenhada na organização do recurso ou em seus ascendentes.
7. Clique em **Adicionar**.
8. Clique em **OK**.

### **Atualizar o Registro da Diretiva com suas Alterações**

1. Efetue logon no Administration Console.
2. Clique em **Configuração > Registro**.
3. Da lista de registros, selecione **Diretivas de Controle de Acesso**.
4. Clique em **Atualizar**.

---

## Capítulo 13. Personalizando as Diretivas de Controle de Acesso Utilizando o XML

O WebSphere Commerce Administration Console permite fazer alterações simples nas diretivas de controle de acesso e suas partes. Para fazer alterações mais sofisticadas, você precisa editar arquivos XML diretamente e, em seguida, carregá-los no banco de dados.



Antes de começar a fazer alterações nos arquivos XML para controle de acesso, você deve ler o capítulo sobre controle de acesso no *WebSphere Commerce Programming Guide and Tutorials*. Este capítulo fornece uma visão geral técnica do controle de acesso e explica como criar comandos personalizados, beans de entidade e de gabaritos JSP (JavaServer Pages) que podem ser protegidos pelas diretivas de controle de acesso.

Assim que terminar as personalizações de código seguindo as orientações fornecidas no *WebSphere Commerce Programming Guide and Tutorials*, você poderá editar os arquivos XML para controle de acesso para estabelecer as proteções exigidas.

---

### 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:

- Criando ou modificando uma ação
- Criando ou modificando um relacionamento
- Criando ou modificando um grupo de relacionamentos
- Criando ou modificando um recurso
- Criando ou modificando atributos
- Criando ou modificando grupos de acesso utilizando critérios complexos
- Criando ou modificando grupos de recursos utilizando critérios complexos
- Criando uma diretiva baseada em funções para exibições
- Alterando o grupo de ações em uma diretiva baseada em funções para exibições
- Criando ou modificando um grupo de diretivas
- Associando diretivas aos grupos de diretivas

---

### 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 12. Arquivos XML do WebSphere Commerce para Controle de Acesso

Nome do Arquivo	Descrição
ACUserGroups_de_DE.xml 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 diretivas 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 diretivas 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 todas as informações de controle de acesso do banco de dados.
OrganizationPoliciesFilter.xml	Arquivo de filtro utilizado na extração de todas as informações de controle de acesso relacionadas às diretivas de propriedade de uma organização específica.
ACUserGroupsFilter.xml	Arquivo de filtro utilizado na extração de todas as informações de grupo de acesso.



Tabela 12. Arquivos XML do WebSphere Commerce para Controle de Acesso (continuação)

Nome do Arquivo	Descrição
accesscontrolpolicies.dtd	O arquivo XML das diretivas de controle de acesso deve se ajustar a este DTD.
accesscontrolpoliciesnls.dtd	O arquivo XML NLS (national language specific) das diretivas 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.
accesscontrol.xsl	O arquivo de regra de transformação XSL para o arquivo XML das diretivas de controle de acesso.
accesscontrolnls.xsl	O arquivo de regra de transformação XSL para o arquivo XML NLS das diretivas 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 diretivas 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 diretivas 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.

## Alterando os Arquivos XML

É possível manipular os arquivos XML para executar as seguintes tarefas de autorização:

- Protegendo as exibições
- Protegendo comandos do controlador
- Implementando o controle de acesso em nível de recurso
- Protegendo os beans de dados
- Agrupando recursos por atributos
- Definindo relacionamentos

- Definindo grupos de relacionamentos

## Protegendo as Exibições

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

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

O nome do ResourceGroup, ViewCommandResourceGroup, indica que isso é uma diretiva baseada em função para exibições. A diretiva indica que usuários no grupo de usuários ProductManagers, podem mostrar as exibições no grupo de ação ProductMangersViews. Semelhantemente, para a maioria das funções, há um grupo de ação correspondente que agrupa as exibições, às quais a função possui acesso, como função Seller -> grupo de acesso Sellers -> grupo de ações SellersViews.

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, que deve corresponder a CommandName na definição da ação. O valor de CommandName está armazenado na coluna ACTION da tabela ACACTION. Os atributos Name e CommandName não devem ser iguais.

## Adicionando uma nova Exibição Utilizando as Diretivas já Existentes

Para adicionar uma nova exibição acessível por funções nas diretivas de Exibição baseada em funções existentes, crie um arquivo XML semelhante ao mostrado e, em seguida, faça o seguinte:

```
<?xml version="1.0" encoding="ISO-8859-1" standalone="no" ?>
<!DOCTYPE Policies SYSTEM "../dtd/accesscontrolpolicies.dtd">

<Policies>
```

```

<Action Name="MyNewView"
      CommandName="MyNewView">
</Action>
<ActionGroup Name="ProductManagersViews" OwnerID="RootOrganization">
      <ActionGroupAction Name="MyNewView"/>
</ActionGroup>
</Policies>

```

1. Crie uma nova definição de ação no arquivo XML que tem o nome de exibição *MyNewView*. Pode ser qualquer nome que escolher.

```

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

```

2. Determine quais funções devem ter acesso a essa exibição e associe a nova ação aos grupos de ação correspondentes no arquivo XML, como no seguinte exemplo:

```

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

      <ActionGroupAction Name="MyNewView"/>

</ActionGroup>

```

Como já existe uma diretiva baseada na função, *ProductManagersExecuteProductManagersViews*, que inclui esse grupo de ações, uma nova diretiva não precisa ser criada. Além disso, como as diretivas baseadas em função padrão pertencem ao grupo de diretivas *ManagementAndAdministrationPolicyGroup* que aplica-se à maioria, se não a todas, as organizações no site, nenhuma assinatura adicional do grupo de diretivas é necessária.

3. Carregue suas alterações de XML no banco de dados. Para obter informações adicionais sobre como carregar as alterações de XML, consulte “Carregando suas Alterações no Banco de Dados” na página 172.
4. Atualize o Registro de Diretivas de Controle de Acesso no Administration Console fazendo o seguinte:
  - a. Efetue logon no Administration Console como um Administrador do Site.
  - b. Clique em **Configuração > Registro**.
  - c. Da lista de registros, selecione **Diretivas de Controle de Acesso**.
  - d. Clique em **Atualizar**.

### Adicionando uma Nova Exibição Utilizando uma Nova Diretiva

Para adicionar uma nova exibição, acessível por uma nova função que não possui uma diretiva baseada em funções existente, crie um arquivo XML semelhante ao mostrado e, em seguida, faça o seguinte:

```

<?xml version="1.0" encoding="ISO-8859-1" standalone="no" ?>
<!DOCTYPE Policies SYSTEM "../dtd/accesscontrolpolicies.dtd">

<Policies>

  <Action Name="MyNewView"
        CommandName="MyNewView">
  </Action>
  <ActionGroup Name="XYZViews" OwnerID="RootOrganization">
        <ActionGroupAction Name="MyNewView"/>
  </ActionGroup>
  <Policy Name="XYZExecuteXYZViews"
        OwnerID="RootOrganization"
        UserGroup="XYZ"
        ActionGroupName="XYZViews"
        ResourceGroupName="ViewCommandResourceGroup"

```

```

    PolicyType="groupableStandard">
  </Policy>

  <PolicyGroup Name="ManagementAndAdministrationPolicyGroup" OwnerID="RootOrganization">
    <PolicyGroupPolicy Name="XYZExecuteXYZViews" PolicyOwnerId="RootOrganization" />
  </PolicyGroup>

</Policies>

```

1. Crie uma nova definição de ação no arquivo XML que tem o nome de exibição *MyNewView*. Pode ser qualquer nome que escolher.

```

<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>

```

Em que *XYZViews* é o nome de seu grupo de ações. O *OwnerID* para os grupos de ações deve sempre ser *RootOrganization*.

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

```

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

  <ActionGroupAction Name="MyNewView" />

</ActionGroup>

```

Em que *XYZViews* é seu grupo de ações e *MyNewView* é a ação criada.

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

```

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

```

Em que *XYZExecuteXYZViews* é o nome de sua diretiva e *XYZViews* é seu grupo de ações. No WebSphere Commerce 5.5, devido ao modelo de assinatura de diretiva, o *OwnerID* para as diretivas padrão agrupáveis e de gabarito agrupáveis não é utilizado para determinar a quais recursos uma diretiva será aplicada. O valor *OwnerID* atualmente é utilizado apenas pelo Administration Console ao exibir diretivas por organização (proprietário). Se uma diretiva tiver que ser aplicada a várias organizações, será recomendável que o *OwnerID* seja definido como a organização ascendente comum, tal como, Organização Raiz. Se uma diretiva tiver que ser aplicada a uma organização específica, será recomendável que o *OwnerID* seja definido como o *orgentity\_id* dessa organização.

5. Inclua a nova diretiva no grupo de diretivas apropriado. Por padrão, a maioria das diretivas baseadas em função são colocadas no *ManagementAndAdministrationPolicyGroup*, que deve ser aplicada a todas as organizações.

```

<PolicyGroupName="ManagementAndAdministrationPolicyGroup"
OwnerID="RootOrganization">
<PolicyGroupPolicy Name="XYZExecuteXYZViews" PolicyOwnerId="RootOrganization" />
</PolicyGroup>

```

Em que o valor `PolicyOwnerId` deve ser igual ao valor `OwnerId` utilizado na definição da diretiva.

6. Carregue suas alterações de XML no banco de dados. Para obter informações adicionais sobre como carregar as alterações de XML, consulte “Carregando suas Alterações no Banco de Dados” na página 172.
7. Atualize o Registro de Diretivas de Controle de Acesso no Administration Console fazendo o seguinte:
  - a. Efetue logon no Administration Console como um Administrador do Site.
  - b. Clique em **Configuração > Registro**.
  - c. Da lista de registros, selecione **Diretivas de Controle de Acesso**.
  - d. Clique em **Atualizar**.

Agora você pode utilizar sua exibição.

## Protegendo os Comandos do Controlador

Todos os comandos do controlador exigem uma diretiva de controle de acesso baseada em função para serem executados. Um comando do controlador ou da tarefa também requer uma diretiva em nível do recurso se o comando estiver fazendo uma verificação em nível de recurso. Para obter informações adicionais, consulte “Protegendo os Recursos” na página 152. O exemplo a seguir exibe uma diretiva baseada em função para comandos do controlador:

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

O `ActionGroupName`, `ExecuteCommandActionGroup`, indica que esta é uma diretiva baseada em função para comandos do controlador. A diretiva 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 amostra 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 diretivas 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="ExecuteCommand
CommandName="Execute">
</Action>
```

**Nota:** O nome da interface do comando do controlador deve corresponder ao ResourceBeanClass na definição de recursos. O valor de ResourceBeanClass está armazenado na coluna RESCLASSNAME da tabela ACRESCGRY. Estes comandos podem ser utilizados como recursos, porque estendem a interface ControllerCommand, que estende a interface AccCommand que, por sua vez, estende a interface Protectable. Para obter informações adicionais sobre estas interfaces, consulte o *WebSphere Commerce Programming Guide and Tutorials*.

## Adicionando um Novo Comando do Controlador Utilizando as Diretivas Existentes

Para adicionar um novo comando do controlador a ser acessado por uma nova função que possui uma diretiva baseada em função existente, crie um arquivo XML, semelhante ao mostrado. As etapas específicas são listadas posteriormente.

```
<?xml version="1.0" encoding="ISO-8859-1" standalone="no" ?>
<!DOCTYPE Policies SYSTEM "../dtd/accesscontrolpolicies.dtd">
```

```
<Policies>
```

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

```
    <ResourceAction Name="ExecuteCommand"/>
  </ResourceCategory>
```

```
    <ResourceGroup Name="SellersCmdResourceGroup" OwnerID="RootOrganization">
ResourceGroupResource Name="com.xyz.commands.MyNewControllerCmdResource
Category"/>
  </ResourceGroup>
```

```
</Policies>
```

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 recursos correspondentes no arquivo XML, como no seguinte exemplo:

```

    <ResourceGroup Name="SellersCmdResourceGroup" OwnerID="RootOrganization">
      <ResourceGroupResource Name="com.xyz.commands.
MyNewControllerCmdResourceCategory"/>
    </ResourceGroup>

```

Você pode alterar o grupo de recursos dependendo da função que deseja utilizar. Para obter informações adicionais sobre diretivas baseadas em função, consulte “Diretivas Baseadas em Funções” na página 214.

3. Carregue suas alterações de XML no banco de dados. Para obter informações adicionais sobre como carregar as alterações de XML, consulte “Carregando suas Alterações no Banco de Dados” na página 172.
4. Atualize o Registro de Diretivas de Controle de Acesso no Administration Console fazendo o seguinte:
  - a. Efetue login no Administration Console como um Administrador do Site.
  - b. Clique em **Configuração > Registro** .
  - c. Da lista de registros, selecione **Diretivas de Controle de Acesso**.
  - d. Clique em **Atualizar**.

Uma vez que já existe uma diretiva baseada em função que inclui este grupo de recursos, agora você pode utilizar seu novo comando do controlador, se não estiver fazendo nenhuma verificação em nível de recurso. Para obter informações sobre verificação em nível de recurso e comandos, consulte “Modificando o Controle de Acesso em Nível de Recurso de uma Diretiva Existente” na página 150.

## Adicionando um Novo Comando do Controlador Utilizando uma Nova Diretiva

Para adicionar um novo comando do controlador a ser acessado por uma nova função que não possui uma diretiva baseada em função existente, crie um arquivo XML, semelhante ao mostrado. As etapas específicas são listadas posteriormente.

```

<?xml version="1.0" encoding="ISO-8859-1" standalone="no" ?>
<!DOCTYPE Policies SYSTEM "../dtd/accesscontrolpolicies.dtd">
<Policies>

  < ResourceCategory Name="com.xyz.commands.MyNewControllerCmdResourceCategory"
    <ResourceBeanClass="com.xyz.commands.MyNewControllerCmd">

      <ResourceAction Name="ExecuteCommand"/>
    </ResourceCategory>

    <ResourceGroup Name="XYZCmdResourceGroup" OwnerID="RootOrganization"
    <ResourceGroupResource Name="com.xyz.commands.MyNewController
CmdResourceCategory"/>
    </ResourceGroup>

    <Policy Name="XYZExecuteXYZsCmdResourceGroup"
    OwnerID="RootOrganization"
    UserGroup="XYZ"
    ActionGroupName="ExecuteCommandActionGroup"
    ResourceGroupName="XYZCmdResourceGroup"
    PolicyType="groupableStandard">
  </Policy>

  <PolicyGroup Name="ManagementAndAdministrationPolicyGroup"
    OwnerID="RootOrganization">
  <PolicyGroupPolicy Name="XYZExecuteXYZsCmdResourceGroup"

```

```
PolicyOwnerId="RootOrganization" />
</PolicyGroup>
```

```
</Policies>
```

1. Crie uma nova definição de recurso no arquivo XML que corresponde ao nome da interface do comando do controlador. Consulte “Adicionando um Novo Comando do Controlador Utilizando as Diretivas Existentes” na página 146 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 diretiva que menciona seu novo grupo de recursos:  

```
<Policy Name="XYZExecuteXYZsCmdResourceGroup"
OwnerID="RootOrganization"
UserGroup="XYZ"
ActionGroupName="ExecuteCommandActionGroup"
ResourceGroupName="XYZCmdResourceGroup">
PolicyType="groupableStandard">
</Policy>
```
5. Carregue suas alterações de XML no banco de dados. Para obter informações adicionais sobre como carregar as alterações de XML, consulte “Carregando suas Alterações no Banco de Dados” na página 172.
6. Atualize o Registro de Diretivas de Controle de Acesso no Administration Console fazendo o seguinte:
  - a. Efetue logon no Administration Console como um Administrador do Site.
  - b. Clique em **Configuração > Registro**.
  - c. Da lista de registros, selecione **Diretivas de Controle de Acesso**.
  - d. Clique em **Atualizar**.

Agora você pode utilizar seu comando do controlador se não estiver fazendo nenhuma verificação em nível de recurso. Para obter informações sobre verificação em nível de recurso e comandos, consulte “Modificando o Controle de Acesso em Nível de Recurso de uma Diretiva Existente” na página 150.

## Modificando o Controle de Acesso de Nível do Comando para o Comando do Controlador

Com base nas diretivas de controle de acesso padrão, o comando `UserRegistrationAdminAddCmd` não pode ser executado por usuários que possuem apenas a função de Gerente de Marketing. O cenário a seguir descreve as etapas necessárias para modificar as diretivas existentes, para que estes usuários possam executar este comando. Você pode utilizar as etapas deste cenário e personalizá-las com seus próprios requisitos.

Todos os comandos do controlador requerem uma diretiva de controle de acesso em nível de comando que tenha `ActionGroupName = ExecuteCommandActionGroup`. Também deve ter um grupo de recursos que inclua o nome da interface do comando do controlador. Estas diretivas geralmente se referem a uma função específica, por exemplo, `MarketingManagersExecuteMarketingManagerCmdResourceGroup`.



```
<Policy Name="MarketingManagersExecuteMarketingManagerCmdResourceGroup"
  OwnerID="RootOrganization"
  UserGroup="MarketingManagers"
  ActionGroupName="ExecuteCommandActionGroup"
  ResourceGroupName="MarketingManagerCmdResourceGroup"
  PolicyType="groupableStandard">

</Policy>
```

**Nota:** A diretiva acima é uma das diretivas padrão que é carregada no banco de dados durante a criação da instância. Para obter informações adicionais sobre as diretivas padrão, consulte “Diretivas e Grupos de Controle de Acesso Padrão”, na página 213.

Neste caso, se desejar que os usuários com a função de Gerente de Marketing possam executar `UserRegistrationAdminAddCmd`, será necessário adicionar este comando ao Grupo de Recursos existente utilizado na diretiva, criando seu próprio arquivo XML e fazer o seguinte:

1. Redefina a ação `ExecuteCommand`
2. Redefina com `com.ibm.commerce.usermanagement.commands.UserRegistrationAddCmd` como uma categoria de recurso.
3. Associe a categoria de recursos ao grupo de recursos requerido, neste caso, `MarketingManagerCmdResourceGroup`.
4. Copie o arquivo XML para `WC_installdir/xml/policies/xml`. A seguir, um exemplo de como poderia ser seu XML:

```
<?xml version="1.0" encoding="ISO-8859-1" standalone="no" ?>
<!DOCTYPE Policies SYSTEM "../dtd/accesscontrolpolicies.dtd">
<Policies> <Action Name="ExecuteCommand"
  CommandName="Execute">
</Action> <ResourceCategory
  Name="com.ibm.commerce.usermanagement.commands.UserRegistrationAdmin
AddCmdResourceCategory"
  ResourceBeanClass="com.ibm.commerce.usermanagement.commands.
UserRegistrationAdminAddCmd">
  <ResourceAction Name="ExecuteCommand"/>
</ResourceCategory>

  <ResourceGroup Name="MarketingManagerCmdResourceGroup"
  OwnerID="RootOrganization"
  ResourceGroupResource
  Name="com.ibm.commerce.usermanagement.commands.
UserRegistrationAdminAddCmdResourceCategory"/>
</ResourceGroup>

</Policies>
```

5. Carregue o arquivo XML no banco de dados utilizando o script `WC_installdir/bin/acpload`. Para obter informações adicionais sobre como carregar os arquivos XML, consulte “Carregando suas Alterações no Banco de Dados” na página 172.
6. Atualize o Registro de Diretiva de Controle de Acesso no WebSphere Commerce Administration Console fazendo o seguinte:
  - a. Efetue logon no Administration Console como um Administrador do Site.
  - b. Clique em **Configuração > Registro**.
  - c. Da lista de registros, selecione **Diretivas de Controle de Acesso**.
  - d. Clique em **Atualizar**.

Agora você pode utilizar seu comando do controlador se não estiver fazendo nenhuma verificação em nível de recurso. Se ele estiver fazendo verificação em nível de recurso, consulte “Modificando o Controle de Acesso em Nível de Recurso de uma Diretiva Existente” na página 150.

## Modificando o Controle de Acesso em Nível de Recurso de uma Diretiva

**Existente:** Para comandos que requeiram controle de acesso em nível de recurso, eles retornam o(s) recurso(s) protegidos(s) que irão acessar no método `getResources()` do comando. Isso aciona uma verificação de controle de acesso de nível de recurso pela estrutura de controle de acesso do WebSphere Commerce. O WebSphere Commerce pesquisará uma diretiva de controle de acesso no sistema com um Grupo de Ação que inclui a ação que é igual ao comando atual; neste exemplo, `com.ibm.commerce.usermanagement.commands.UserRegistrationAdminAddCmd`. O Grupo de Recursos da diretiva também deve incluir o recurso que foi retornado no método `getResources()`. Nesse caso, o comando `UserRegistrationAdminAddCmd` implementa o método `getResources()` e ele retorna a organização à qual o novo usuário vai ser registrado.

Pronto para utilização, no `defaultAccessControlPolicies.xml`, `com.ibm.commerce.usermanagement.commands.UserRegistrationAdminAddCmd` já está definido como uma ação:

```
<Action
Name="com.ibm.commerce.usermanagement.commands.UserRegistrationAdminAddCmd"
  CommandName="com.ibm.commerce.usermanagement.commands.UserRegistrationAdminAddCmd">
</Action>
```

Também está incluído em um grupo de ação, definido no arquivo XML `defaultAccessControlPolicies.xml`:

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

  <ActionGroupAction

Name="com.ibm.commerce.usermanagement.commands.UserRegistrationAdminAddCmd"/>
</ActionGroup>
```

Esse grupo de ações já foi utilizado em uma diretiva bootstrap existente:

```
<Policy
  Name="MembershipAdministratorsForOrgExecuteUserAdminRegistrationCommandsOnOrganizationResource"
  OwnerID="RootOrganization"
  UserGroup="MembershipAdministratorsForOrg"
  ActionGroupName="UserAdminRegistration"
  ResourceGroupName="OrganizationDataResourceGroup"
  PolicyType="groupableTemplate">

</Policy>
```

**Nota:** Várias diretivas são padrão e carregadas no banco de dados durante a criação da instância. Para obter informações adicionais sobre as diretivas padrão, consulte “Diretivas e Grupos de Controle de Acesso Padrão”, na página 213.

Para adicionar a função requerida a `UserRegistrationAdminAddCmd`, faça o seguinte:

1. Adicione a função requerida ao grupo de acesso utilizado pela diretiva. Nesse exemplo, `MembershipAdministratorsForOrg`.

Esse grupo de acesso é definido em `WC_installdir/xml/policies/xml/ACUserGroup_en_US.xml`, da seguinte forma:

```
<UserGroup
Name=" MembershipAdministratorsForOrg"
OwnerID="RootOrganization"
  Description="Administrators of membership for the organization"
MemberGroupID="-97"

<UserCondition><![CDATA[
<profile>
  <orListCondition>
    <simpleCondition>
      <variable name="role"/>
      <operator name="="/>
```

```

<value data="Buyer Administrator"/>
  <qualifier name="org" data="?"/>
</simpleCondition>
<simpleCondition>
  <variable name="role"/>
  <operator name="="/>
<value data="Seller Administrator"/>
  <qualifier name="org" data="?"/>
</simpleCondition>
</orListCondition>
</profile>
]]</UserCondition>
</UserGroup>

```

No XML acima, são incluídos os usuários que possuem pelo menos uma das funções especificadas, Administrador da Compradora ou Administrador da Vendedora de uma organização que é uma ascendente do proprietário do recurso (organização) retornado por `getResources()`. Se você quisesse adicionar a função de Gerenciador de Marketing, seria necessário melhorá-la para também incluir a nova função.

2. Copie o arquivo XML para `WC_installdir/xml/policies/xml`. A seguir, um exemplo de como poderia ser seu XML:

```

?xml version="1.0" encoding="UTF-8"?
<!DOCTYPE UserGroups SYSTEM "../dtd/ACUserGroups_en_US.dtd">

<UserGroups>

<UserGroup Name="MembershipAdministratorsForOrg" OwnerID="RootOrganization"
  Description="Administrators of membership for the organization" MemberGroupID="-97">

  <UserCondition><![CDATA[
    <profile>
      <orListCondition>
        <simpleCondition>
          <variable name="role"/>
          <operator name="="/>
          <value data="Buyer Administrator"/>
          <qualifier name="org" data="?"/>
        </simpleCondition>
        <simpleCondition>
          <variable name="role"/>
          <operator name="="/>
          <value data="Seller Administrator"/>
          <qualifier name="org" data="?"/>
        </simpleCondition>
        <simpleCondition>
          <variable name="role"/>
          <operator name="="/>
          <value data="Marketing Manager"/>
          <qualifier name="org" data="?"/>
        </simpleCondition>
      </orListCondition>
    </profile>
  ]]></UserCondition>
</UserGroup>

</UserGroups>

```

3. Carregue o arquivo XML no banco de dados utilizando o script `WC_installdir/bin/acpload`. Para obter informações adicionais sobre como carregar os arquivos XML, consulte "Carregando suas Alterações no Banco de Dados" na página 172.
4. Atualize o Registro de Diretiva de Controle de Acesso no WebSphere Commerce Administration Console fazendo o seguinte:
  - a. Efetue logon no Administration Console como um Administrador do Site.
  - b. Clique em **Configuração > Registro**.
  - c. Da lista de registros, selecione **Diretivas de Controle de Acesso**.
  - d. Clique em **Atualizar**.

## Protegendo os Recursos

É possível adicionar controle de acesso em nível de recurso aos comandos do controlador ou da tarefa. 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 em nível de recurso também pode ser feita durante a parte do comando `performExecute()`, fazendo chamadas diretas ao gerenciador de diretiva de controle de acesso utilizando o método `void checkIsAllowed(Object resource, String action) throws ECEException`. Este método enviará o `ECAApplicationException` 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 diretiva em nível do recurso para novos comandos nas seguintes instâncias:

- O novo comando se estende de um comando base do WebSphere Commerce que está fazendo uma verificação de nível de recurso e possui uma diretiva de nível de recurso e o novo comando que está implementando uma interface diferente do comando base.
- O próprio comando faz a verificação do controle de acesso em nível do recurso.

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

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

Em que:

**Name:** O nome da diretiva.

**PolicyType:** O tipo da diretiva. Esta é uma diretiva de gabarito agrupável e será aplicada dinamicamente à entidade organizacional que possui o recurso e seus ascendentes.

**OwnerID:** O membro que possui a diretiva.

**UserGroup:** A diretiva se aplica aos usuários deste grupo. A convenção de nomenclatura para grupos de acesso nos quais as funções são dinamicamente colocadas em escopo na organização que possui o recurso deve 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 diretiva em nível do recurso acima:

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

Os comandos que foram definidos anteriormente como recursos para as diretivas 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 diretivas em nível do recurso estão protegendo. A seguir, uma definição de amostra do grupo de recursos que é utilizado na diretiva 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 informações adicionais sobre a interface Protectable, consulte o *WebSphere Commerce Programming Guide and Tutorials*.

## 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 diretivas 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 informações adicionais sobre a interface `Protectable`, consulte o *WebSphere Commerce Programming Guide and Tutorials*.

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

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

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

Em que:

**Name:** O nome desta diretiva.

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

**ActionGroupName:** O valor `DisplayDataBeanActionGroup` indica que é uma diretiva 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, uma amostra 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 diretiva 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 totalmente definidos 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 diretiva 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 informações adicionais sobre a interface Groupable, consulte o *WebSphere Commerce Programming Guide and Tutorials*.

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>
    </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 recursos.

<![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.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 as finalidades de gerenciamento do Grupo de Recursos Implícitos no WebSphere Commerce Administration Console, o atributo também deve ser definido na tabela ACATTR e associado ao recurso na tabela ACRESATREL. Quando é momento de localizar as diretivas 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

<andListCondition>, 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).

Uma definição de atributo de amostra para ocupar a tabela ACATTR é mostrada 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 primária.

## Definindo Relacionamentos

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

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

A entrada Name é o nome do relacionamento utilizado em qualquer diretiva, e é adicionado à tabela ACRELATION. Name corresponde ao parâmetro de relacionamento do método fulfill() 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="Root Organization">
  <RelationCondition><![CDATA[
    <profile>
```

```

    Relationship Chain Open Condition XML
  </profile>
]]></RelationCondition>
</RelationGroup>

```

## Cadeias de Relacionamentos

Cada grupo de relacionamentos consiste em uma ou mais condições abertas RELATIONSHIP\_CHAIN, agrupadas por 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 <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>

```

Em que:

aValue: Uma cadeia que representa o relacionamento entre o usuário e o recurso. Esta cadeia deve ser um dos relacionamentos verificados no método de preenchimento do recurso.

Quando uma cadeia de relacionamento tem um comprimento de dois ou mais, ela é uma série de dois relacionamentos. A primeira entrada, <parameter name= "X" value="Y">, está entre um usuário e uma entidade organizacional. A última entrada <parameter name= "X" value="Y"> está entre uma entidade organizacional e o recurso. As entradas intermediárias <parameter 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 for HIERARCHY, os possíveis valores de aValue2 incluirão child, que retorna a entidade organizacional para a qual o usuário é um filho direto na hierarquia de membros. Se o valor de aValue1 for ROLE, os possíveis valores de aValue2 incluirão quaisquer entradas válidas na coluna NAME da tabela ROLE que retornam todas as entidades organizacionais nas quais o usuário atual desempenha 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 mais de uma entidade organizacional tiver sido retornada pela avaliação do parâmetro aValue1, esta parte de RELATIONSHIP\_CHAIN será atendida se pelo menos uma destas entidades organizacionais atender o relacionamento especificado pelo parâmetro aValue2.

**Nota:** Para obter informações adicionais sobre a definição de grupos de relacionamentos, consulte “Definindo Grupos de Relacionamentos” na página 157

### Definindo Grupos de Relacionamentos em Cadeia Única

Se como parte de sua diretiva 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 diretiva 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 informações adicionais 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 diretiva 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 `<andListCondition>` deve ser alterada para a tag `<orListCondition>`.

## Grupos de Acesso

Os grupos de acesso padrão que fazem parte do WebSphere Commerce estão localizados em arquivos XML específicos de idioma, tais como, `WC_installdir/xml/policies/xml/ACUserGroups_locale.xml`. Este arquivo segue o DTD especificado por `WC_installdir/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. Estes critérios estão armazenados 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 13. Nomes Suportados da Condição Simples

Nome da Variável	Descrição	Operadores Suportados	Valores Suportados	Qualificadores	Valores do Qualificador
role	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.	<ul style="list-style-type: none"> <li>OrgEntityID : Onde o usuário deve ter a função.</li> <li>OrgAndAncestorOrgs: Quando é utilizado em uma diretiva de gabarito agrupável. Verificará se o usuário possui a função especificada na organização que possui o recurso ou qualquer uma de suas organizações ascendentes.</li> </ul>
registration status	Especifica que o usuário deve ter este status de registro.	= !=	Qualquer valor da coluna REGISTER-TYPE na tabela USERS, como G para guest 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

Tabela 13. Nomes Suportados da Condição Simples (continuação)

Nome da Variável	Descrição	Operadores Suportados	Valores Suportados	Qualificadores	Valores do Qualificador
org	Especifica que o usuário é um filho da organização especificada. Estas informações são baseadas nos dados armazenados na tabela MBRREL	= !=	<ul style="list-style-type: none"> <li>Qualquer valor de ORGENTITY_ID na tabela ORGENTITY.</li> <li>?: se for uma diretiva de gabarito agrupável. Verificará se o usuário é um filho da organização que possui o recurso. Também verificará se o usuário é um filho de qualquer um dos ascendentes do proprietário do recurso, até e incluindo o ascendente mais próximo que é assinante de um grupo de diretivas</li> </ul>	none	n/a

## 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 diretivas baseadas em funções. Neste exemplo o usuário deve ter uma função de Administração de Vendedora para qualquer entidade organizacional.

```
<UserCondition>
  <![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 diretivas em nível de organização. Neste exemplo, o usuário deve ter uma função de Vendedor para a entidade organizacional com ORGENTITY\_ID = 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 o valor de dados especial `OrgAndAncestorOrgs`. Este valor de dados qualificado, `OrgAndAncestorOrgs`, funciona apenas em diretivas de gabarito agrupáveis. Neste exemplo, o usuário deve ter uma função de Gerente de Vendas, Gerente de Contas ou Vendedor na organização que possui o recurso ou qualquer um dos ascendentes da organização.

```

<UserCondition><![CDATA[
  <profile>
    <orListCondition>
      <simpleCondition>
        <variable name="role"/>
        <operator name="="/>
        <value data="Sales Manager"/>
        <qualifier name="org" data="OrgAndAncestorOrgs"/>
      </simpleCondition>
      <simpleCondition>
        <variable name="role"/>
        <operator name="="/>
        <value data="Account Representative"/>
        <qualifier name="org" data="OrgAndAncestorOrgs"/>
      </simpleCondition>
      <simpleCondition>
        <variable name="role"/>
        <operator name="="/>
        <value data="Seller"/>
        <qualifier name="org" data="OrgAndAncestorOrgs"/>
      </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`, deve haver um registro no qual o usuário é descendente de uma organização que possui `ANCESTOR_ID = 100` e `SEQUENCE = 1`.

```

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

```

## Diretivas

O arquivo `WC_installdir/xml/policies/xml/defaultAccessControlPolicies.xml` define as diretivas de controle de acesso padrão, enviadas prontas. Ele segue o DTD especificado por:  
`WC_installdir/xml/policies/dtd/accesscontrolpolicies.dtd`.

A seguir, o gabarito de um elemento de diretiva:

```

<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 diretiva. Ele 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 diretiva. Ele 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`. Ele é carregado na coluna `mbrgrp_id` da tabela `ACPOLICY`. Os grupos de acesso padrão são definidos no arquivo `WC_installdir/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



diretiva. 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 diretivas baseadas em funções para comandos do controlador têm o `ActionGroupName` definido como `ExecuteCommandActionGroup`. As diretivas 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 está armazenado na tabela `ACPOLICY`. As diretivas baseadas em funções para exibições têm o `ResourceGroupName` definido como `ViewCommandResourceGroup`.

**PolicyType:** O tipo da diretiva. Os valores válidos são `groupableStandard` e `groupableTemplate`. Para compatibilidade reversa, os valores padrão e de gabarito também são suportados. Se este atributo não estiver especificado durante o carregamento de uma nova diretiva, será utilizado o valor nulo. Se este atributo não estiver especificado durante a atualização de uma diretiva existente, o valor permanecerá inalterado. A tabela a seguir exibe o mapeamento de valores de cadeia para valores do banco de dados armazenados na coluna `POLICYTYPE` da tabela `ACPOLICY`.

*Tabela 14. Mapeamento de Valores de Cadeia para Valores do Banco de Dados*

Cadeia	ACPOLICY.POLICYTYPE
<code>groupableTemplate</code>	3
<code>groupableStandard</code>	2
<code>template</code>	1
<code>standard</code>	0 ou nulo

Para obter informações adicionais sobre os tipos de diretivas, consulte Capítulo 3, “Conceitos sobre Autorização”, na página 17.

**RelationName (optional):** O nome do Relacionamento, conforme especificado na coluna `RELATIONNAME` da tabela `ACRELATION`. Se estiver especificado, será utilizado para obter o ID de relacionamento correspondente (`ACRELATION_ID`) que está 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 Diretiva

### Diretivas 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="AllUsersExecuteAllUserCmdResourceGroup"
  OwnerID="RootOrganization"
  UserGroup="AllUsers"
  ActionGroupName="ExecuteCommandActionGroup"
  ResourceGroupName="AllUserCmdResourceGroup"
  PolicyType="groupableStandard">
</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"
  PolicyType="groupableStandard">
</Policy>
```

### **Diretivas em Nível do Recurso:**

*Para Comandos:* Neste exemplo, os usuários que pertencem ao grupo de acesso AllUsers podem executar as ações especificadas pelo grupo de ação CouponRedemption em recursos especificados por CouponWalletResourceGroup, desde que os usuários preencham o relacionamento creator referente ao recurso.

```
<Policy Name="AllUsersExecuteCouponRedemptionCommandsOnCouponWalletResource"
  OwnerID="RootOrganization"
  UserGroup="AllUsers"
  ActionGroupName="CouponRedemption"
  ResourceGroupName="CouponWalletResourceGroup"
  RelationName="creator"
  PolicyType="groupableStandard">
</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"
  PolicyType="groupableStandard">
</Policy>
```

**Diretivas de Gabaritos Agrupáveis:** Neste exemplo, os usuários que pertencem ao grupo de acesso

OrgAdminConsoleMembershipAdministratorsForOrg

podem executar as ações especificadas pelo grupo de ação ApproveGroupUpdate em recursos especificados por OrganizationDataResourceGroup.

```
<Policy Name="OrgAdminConsoleMembershipAdministratorsForOrgExecuteApprove
GroupUpdateCommandsOnOrganizationResource"
  OwnerID="RootOrganization"
  UserGroup="OrgAdminConsoleMembershipAdministratorsForOrg"
```

```

    ActionGroupName="ApproveGroupUpdate"
    ResourceGroupName="OrganizationDataResourceGroup"
    PolicyType="groupableTemplate">
</Policy>

```

Examinar a definição do grupo de acesso OrgAdminConsoleMembershipAdministratorsForOrg revelará a seguinte condição para filiação:

```

<UserCondition>
  <profile>
    <orListCondition>
      <simpleCondition>
        <variable name="role"/>
        <operator name="="/>
        <value data="Buyer Administrator"/>
        <qualifier name="org" data="OrgAndAncestorOrgs"/>
      </simpleCondition>
      <simpleCondition>
        <variable name="role"/>
        <operator name="="/>
        <value data="Seller Administrator"/>
        <qualifier name="org" data="OrgAndAncestorOrgs"/>
      </simpleCondition>
      <simpleCondition>
        <variable name="role"/>
        <operator name="="/>
        <value data="Channel Manager"/>
        <qualifier name="org" data="OrgAndAncestorOrgs"/>
      </simpleCondition>
    </orListCondition>
  </profile>
</UserCondition>

```

**Nota:** O simpleCondition de role é qualificado por org = **OrgAndAncestorOrgs**. OrgAndAncestorOrgs é uma palavra-chave que está disponível apenas em diretivas de gabarito agrupáveis. Ele coloca dinamicamente a função em escopo para o contexto do proprietário do recurso atual. Neste exemplo, o usuário deve ter uma das funções especificadas na organização que possui o recurso ou qualquer um dos ascendentes da organização.

## Definindo Grupos de Diretivas

São criados grupos de diretivas para diretivas do grupo, com base em requisitos de negócios e de controle de acesso. Alguns grupos de diretivas padrão são criados prontos para utilização; para obter informações adicionais, consulte “Diretivas e Grupos de Controle de Acesso Padrão”, na página 213. São criados outros grupos de diretivas, conforme necessário, durante a publicação de uma loja ou de um modelo de negócios. Na maioria dos casos, você pode apenas adicionar novas diretivas criadas a grupos de diretivas existentes. Se precisar criar um novo grupo de diretivas, é necessário defini-lo em um arquivo XML, semelhante a defaultAccessControlPolicies.xml e, em seguida, carregá-lo no banco de dados. A seguir está uma definição de amostra:

```

<PolicyGroup Name="aValue" OwnerID="aValue">
  </PolicyGroup>

```

em que:

Name: O nome do grupo de diretivas.

OwnerID: O ID do membro da entidade organizacional que possui o grupo de diretivas. Ele será carregado na coluna member\_id da tabela ACPOLGRP. O OwnerID e

o Name juntos devem ser exclusivos. Existem dois valores especiais que são reconhecidos pela ferramenta do transformador, são eles RootOrganization: -2001 e DefaultOrganization: -2000.

### **Associando Diretivas a Grupos de Diretivas**

As diretivas podem pertencer a vários grupos de diretivas. No entanto, para encerrar a administração de diretivas, é recomendável que uma diretiva pertença apenas a um grupo de diretivas. Esta associação deve ser definida em um arquivo XML, semelhante a defaultAccessControlPolicies.xml e, em seguida, carregada no banco de dados. A seguir está uma definição de amostra:

```
<PolicyGroup Name="aValue" OwnerID="aValue">  
  <PolicyGroupPolicy Name="aValue" PolicyOwnerID="aValue" />  
</PolicyGroup>
```

em que:

PolicyGroupPolicy Name: O nome da diretiva, definido anteriormente, a ser associado ao grupo de diretivas especificado. Esta diretiva deve ter um dos seguintes tipos de diretivas: groupableStandard ou groupableTemplate.

PolicyGroupPolicy PolicyOwnerID (opcional): O ID do membro da entidade organizacional que possui a diretiva especificada. Se este parâmetro não for especificado, o valor padrão será OwnerID do grupo de diretivas. Existem dois valores especiais que são reconhecidos pela ferramenta do transformador, são eles RootOrganization: -2001 e DefaultOrganization: -2000.

### **Assinando Grupos de Diretivas**

Os recursos de uma organização são protegidos pelas diretivas nos grupos de diretivas dos quais essa organização é assinante. Se essa organização não for assinante de nenhum dos grupos de diretivas, serão aplicados os grupos de diretivas dos quais o ascendente mais próximo dessa organização é assinante. Para obter informações adicionais sobre quais grupos de diretivas uma organização deve ser assinante, consulte "Diretivas e Grupos de Controle de Acesso Padrão", na página 213.

A assinatura do grupo de diretivas pode ser feita no Organization Administration Console, mas também pode ser definida em um arquivo XML, semelhante a defaultAccessControlPolicies.xml e, em seguida, carregada no banco de dados. A seguir está uma definição de amostra:

```
<PolicyGroup Name="aValue" OwnerID="aValue">  
  <PolicyGroupSubcription OrganizationID="aValue"/>  
</PolicyGroup>
```

em que:

OrganizationID: O ID do membro da entidade organizacional que é assinante deste grupo de diretivas. Existem dois valores especiais que são reconhecidos pela ferramenta do transformador, são eles RootOrganization: -2001 e DefaultOrganization: -2000.

### **Dados da Diretiva Traduzíveis**

A seguir está um gabarito de um arquivo de diretivas personalizado que pode ser utilizado para definir dados de diretivas traduzíveis:

```
<?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>
<PolicyGroup_nls>-->
<!DOCTYPE PoliciesNLS SYSTEM "../dtd/accesscontrolpoliciesnls.dtd">

<PoliciesNLS LanguageID="value">

```

```

<!--Insert access control element definitions here -->
</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 Diretiva não Traduzíveis

A seguir, um gabarito de um arquivo de diretiva personalizada contendo dados não traduzíveis:

```

<?xml version="1.0" encoding="ISO-8859-1" standalone="no" ?>
<!DOCTYPE Policies SYSTEM "../dtd/accesscontrolpolicies.dtd">

<!--The following NON-TRANSLATABLE access control elements
devem ser definidos neste arquivo:

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

<!--Insert access control element definitions here-->
</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_installdir\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:

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

Em que:

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

**DisplayName\_nls:** O nome de exibição do atributo. Este valor está armazenado na coluna DISPLAYNAME da tabela ACATTRDESC.

**Description\_nls:** Uma descrição opcional do atributo. Este valor está 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 Accelerator"  
>
```

Em que:

**ActionName:** O nome da ação. Este valor está armazenado na coluna ACTION da tabela ACACTION.

**DisplayName\_nls:** O nome de exibição da ação. Este valor está armazenado na coluna DISPLAYNAME da tabela ACACTDESC.

**Description\_nls:** Uma descrição opcional da ação. Este valor está 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 está armazenado na coluna RELATIONNAME da tabela ACRELATION.

**DisplayName\_nls:** O nome de exibição do relacionamento. Este valor está armazenado na coluna DISPLAYNAME da tabela ACRELDESC.

**Description\_nls:** Uma descrição opcional do relacionamento. Este valor está 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 está armazenado na coluna RESCLASSNAME da tabela ACRESCGRY.

**DisplayName\_nls:** O nome de exibição da categoria de recursos. Este valor está armazenado na coluna DISPLAYNAME da tabela ACRSCGDES.

**Description\_nls:** Uma descrição opcional da categoria de recursos. Este valor está 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 está armazenado na coluna GROUPNAME da tabela AACTGRP.

**DisplayName\_nls:** O nome de exibição do grupo de ação. Este valor está armazenado na coluna DISPLAYNAME da tabela ACACGPDESC.

**Description\_nls:** Uma descrição opcional do grupo de ação. Este valor está 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 está armazenado na coluna GRPNAME da tabela ACRESGRP.

**DisplayName\_nls:** O nome de exibição do grupo de recursos. Este valor está armazenado na coluna DISPLAYNAME da tabela ACRESGPDES.

**Description\_nls:** Uma descrição opcional do grupo de recursos. Este valor está armazenado na coluna DESCRIPTION da tabela ACRESGPDES.

**Diretiva:** O exemplo a seguir define as informações da diretiva:

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

Em que:

**PolicyName:** O nome da diretiva de controle de acesso. Este valor está armazenado na coluna POLICYNAME da tabela ACPOLICY.

**OwnerID:** O ID do membro da entidade organizacional que possui esta diretiva.

**DisplayName\_nls:** O nome de exibição da diretiva. Este valor está armazenado na coluna DISPLAYNAME da tabela ACPOLDESC.

**Description\_nls:** Uma descrição opcional da diretiva. Este valor está armazenado na coluna DESCRIPTION da tabela ACPOLDESC.

**Grupo de Diretivas:** O exemplo a seguir define informações adicionais do grupo de diretivas:

```
<PolicyGroup_nls PolicyGroupName="B2CPolicyGroup" OwnerID="RootOrganization"
  DisplayName_nls="B2C Policy Group"
  Description_nls="This policy group contains all the B2C specific policies."
/>
```

em que:

**PolicyGroupName:** O nome do grupo de diretivas de controle de acesso ao qual as informações adicionais estão sendo adicionadas. Este valor está localizado na coluna NAME da tabela ACPOLGRP.

**OwnerID:** O ID do membro da entidade organizacional que possui este grupo de diretivas.

**DisplayName\_nls:** O nome de exibição do grupo de diretivas. Este valor está armazenado na coluna DISPLAYNAME da tabela ACPLGPDESC.

**Description\_nls:** Uma descrição opcional do grupo de diretivas. Este valor está armazenado na coluna DESCRIPTION da tabela ACPLGPDESC.

---

## Depois de Alterar os Arquivos XML

### Testando suas Alterações

Para obter informações sobre como testar suas alterações, consulte “Depois de Fazer as Alterações na Diretiva” na página 107.

### Carregando suas Alterações no Banco de Dados

Se você fizer alterações na diretiva 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 diretiva e as definições do grupo de acesso são carregadas a partir dos arquivos XML.




- Se quiser implementar as mesmas diretivas 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 diretivas 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 diretiva de controle de acesso e as definições do grupo de acesso e carrega-os nos bancos de dados apropriados. A diretiva 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.

### Notas:

1. Se você criar arquivos XML personalizados, precisará copiá-los no diretório `<diretório_de_instalação_do_WC>/xml/policies/xml` para carregá-los nos bancos de dados.
2. Existe uma definição nos scripts de carregamento que especifica a seguinte definição de parâmetro ao resolver IDs e carregar os dados no banco de dados: `"-maxerror 100000"`. Isto significa que, se houver até 100.000 violações de chaves externas durante o carregamento de dados, elas serão ignoradas, em vez de interrompidas. Este valor pode ser aumentado ou reduzido, conforme necessário. Por exemplo, se desejar parar após um erro desse tipo, será necessário alterar o valor para 1.

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

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

Para :

1. A partir do diretório `<diretório_de_instalação_do_WC>\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 <nome do banco de dados> <usuário do banco de dados> <senha do usuário do banco de dados> <arquivo xml do UserGroups>[schema name]` **Exemplo:** `acugload mall dbuser dbusrpwd ACUserGroups_en_US.xml`
  - Para carregar o arquivo de diretivas de controle de acesso principal, execute o arquivo de comando **acpload**. **Sintaxe:** `acpload.cmd <nome do banco de dados> <usuário do banco de dados> <senha do usuário do banco de dados> <arquivo xml de Diretivas>[schema name]` **Exemplo:** `acpload mall dbuser dbusrpwd defaultAccessControlPolicies.xml`
  - Para carregar os nomes de exibição e o arquivo de descrições, execute o arquivo de comando **acpnload**. **Sintaxe:** `acpnload.cmd <nome do banco de dados> <usuário do banco de dados> <senha do usuário do banco de dados> <arquivo xml de Diretivas NLS>[schema name]` **Exemplo:** `acpnload mall dbuser dbusrpwd defaultaccesscontrolpolicies_en_US.xml`
2. Verifique os arquivos de log **acugload.log**, **acpload.log**, e **acpnload.log** em `<diretório_de_instalação_do_WC>\logs` para consultar qualquer erro.

Para    

O ID do usuário do banco de dados deve ter a seguinte permissão para prosseguir com as seguintes etapas:

- Autoridade de leitura/gravação/execução para os diretórios, subdiretórios e arquivos de *WC\_installdir/xml/policies* e *WC\_installdir/logs*.
- Autoridade de leitura/execução para o diretório *WC\_installdir/bin* e seus arquivos.


Se o ID do usuário do banco de dados não tiver a autoridade requerida acima, será necessário conceder esta autoridade utilizando o comando `chmod`.

1. Efetuar login como o ID do usuário do banco de dados.
2. A partir do diretório *<diretório\_de\_instalação\_do\_WC>/bin*, execute os seguintes scripts de shell, conforme necessário, na ordem listada aqui:
  1. Para carregar as definições do grupo (acesso) de usuário, execute o script de shell **acugload**. **Sintaxe:** `acugload.sh <nome do banco de dados> <usuário do banco de dados> <senha do usuário do banco de dados> <nome do arquivo xml do UserGroups>[schema name]` **Exemplo:** `acugload mall dbuser dbusrpwd ACUserGroups_en_US.xml`
  2. Para carregar o arquivo de diretivas de controle de acesso principal, execute o seguinte script de shell **acpload**. **Sintaxe:** `acpload.sh <nome do banco de dados> <usuário do banco de dados> <senha do usuário do banco de dados> <nome do arquivo xml de Diretivas>[schema name]` **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 <nome do banco de dados> <usuário do banco de dados> <senha do usuário do banco de dados> <nome do arquivo xml de Diretivas NLS>[schema name]` **Exemplo:** `acpnlsload mall dbuser dbusrpwd defaultaccesscontrolpolicies_en_US.xml`

Verifique os arquivos de log `acugload.log`, `acpload.log`, e `acpnlsload.log` no *<diretório\_de\_instalação\_do\_WC>/logs* para consultar qualquer erro.

**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 

**Nota:** Para , os arquivos de log estão localizados em *WC\_userdir/instances*.

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

O processo de extração lê as informações da diretiva e do grupo de acessos nos bancos de dados do controle de acesso e gera arquivos que capturam as informações no formato XML. O utilitário de extração utiliza um arquivo XML de filtro de entrada para especificar quais dados serão extraídos do banco de dados. São fornecidos os seguintes arquivos de filtro:

- `ACPoliciesFilter.xml`: utilizado para extrair todos os dados do grupo de acesso e de diretivas.
- `ACUserGroupsFilter.xml`: utilizado para extrair todos os dados do grupo de acesso.

- OrganizationPoliciesFilter.xml: utilizado para extrair todos os dados do grupo de acesso e de diretivas para uma determinada organização. Antes de utilizar este arquivo, ele deve ser editado para especificar o ID da organização requerido. Os dados de diretivas pertencentes a este ID da organização serão extraídos.

Para  

1. A partir do diretório <diretório\_de\_instalação\_do\_WC\bin, execute o seguinte comando acpextract:

```
acpextract.cmd
<nome do banco de dados>
<usuário do banco de dados>
<senha do usuário do banco de dados>
<arquivo de filtro xml de entrada> [schema name]
```

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 diretiva de controle de acesso independente da linguagem.
  - AccessControlPolicies\_LOCALE.xml: O arquivo das diretivas de controle de acesso dependente de linguagem que contém os nomes de exibição e descrições.
2. Verifique o arquivo de log <diretório\_de\_instalação\_do\_WC>\logs\acpextract.log para consultar qualquer erro de processamento que possa ter ocorrido.

Para    

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

```
acpextract.sh <nome do banco de dados>
<usuário do banco de dados>
<senha do usuário do banco de dados>
<arquivo de filtro xml de entrada> [schema name]
```

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 diretiva de controle de acesso independente da linguagem.

- AccessControlPolicies\_LOCALE.xml: O arquivo das diretivas de controle de acesso dependente de linguagem que contém os nomes de exibição e descrições.
3. Verifique o arquivo de log  
<diretório\_de\_instalação\_do\_WC>\logs\acpextract.log para consultar qualquer erro de processamento que possa ter ocorrido.

Para ▶ 400

1. Os arquivos a seguir são criados no diretório *WC\_installdir/xml/policies/xml* 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 diretiva de controle de acesso independente da linguagem.
  - AccessControlPolicies\_LOCALE.xml: O arquivo das diretivas de controle de acesso dependente de linguagem que contém os nomes de exibição e descrições.

---

## **Parte 4. Segurança de Pagamentos**

Esta parte descreve as tarefas de administração de segurança de Pagamentos.



---

## Capítulo 14. Acesso ao WebSphere Commerce Payments

O WebSphere Commerce Payments autentica os usuários por intermédio da utilização de regiões. Uma região é um registro de usuários com um único método de autenticação desses usuários, por exemplo, o nome e senha de um usuário. Cada instalação do WebSphere Commerce Payments pode utilizar apenas uma região de cada vez. Exemplos de tipos de região incluem regiões LDAP e regiões de sistema operacional. Um usuário tem que ser definido em uma região antes de ter acesso concedido aos recursos naquela região. Portanto, um usuário será válido para o WebSphere Commerce Payments se, e apenas se:

- Estiver no domínio
- Receber atribuição de uma função no WebSphere Commerce Payments

O WebSphere Commerce Payments emprega um esquema de controle de acesso com base em funções, que definem quatro funções do WebSphere Commerce Payments:

1. Payments Administrator
2. Administrador do Comerciante
3. Supervisor
4. Vendedor

O Payments Administrator pode utilizar a janela Usuário da interface do usuário do WebSphere Commerce Payments para atribuir acesso (com base na função) a um usuário definido em uma região. O WCSRealm é fornecido com o WebSphere Commerce Payments. A classe WCSRealm é configurada automaticamente para seu sistema. Esta região permite que o WebSphere Commerce Payments Servlet utilize informações do administrador que já estão registradas nas tabelas de usuário do WebSphere Commerce. Essas informações do administrador são utilizadas por Payments Administrators para que não seja necessário definir outro conjunto de IDs de administrador para utilizar a interface com o usuário do WebSphere Commerce Payments.





---

## Capítulo 15. Mantendo a Segurança do WebSphere Commerce Payments

A segurança do WebSphere Commerce Payments é construída com base em vários elementos-chave de segurança. Esses elementos combinam-se para criar um ambiente em que os serviços possam ser implantados com segurança na Web.

**Nota:** IBM WebSphere Commerce Payments (de agora em diante chamado de WebSphere Commerce Payments) era conhecido anteriormente como Payment Manager. Começando com a versão 3.1.3, o aplicativo de pagamentos foi renomeado para WebSphere Commerce Payments e as referências ao produto foram alteradas ao longo deste documento.

---

### Protegendo o WebSphere Commerce Payments

No núcleo do WebSphere Commerce Payments está o Payment Servlet. Vários produtos suplementares e o servidor Web configurado com o WebSphere Application Server, o banco de dados e a interface com o usuário completam a figura do WebSphere Commerce Payments. Este capítulo discute os métodos para proteger os vários componentes do WebSphere Commerce Payments.

#### Protegendo Dados Sensitivos

Para cada comando de consulta, a estrutura verificará a função do usuário junto a essa função mínima e definirá um indicador no objeto QueryRequest para indicar se os dados sensitivos, como números de cartão de crédito ou endereços de cobrança deverão ser retornados em exibição completa ou se deverão ser mascaradas separadamente. A estrutura do WebSphere Commerce Payments não mantém dados sensitivos que possam ser retornados por um comando de consulta. No entanto, são fornecidos novos métodos para gravadores de cassetes para verificar o valor desse indicador e também para mascarar dados sensitivos de maneira padronizada. Cada cassete deve distinguir os dados sensitivos dos dados armazenados. Normalmente, os dados sensitivos representam o mesmo conjunto de dados que um cassete criptografa antes de armazená-lo no banco de dados do WebSphere Commerce Payments.

O parâmetro do sistema JVM `wpm.MinSensitiveAccessRole={clerk|supervisor|madmin|psadmin|none}` especifica a função mínima que um usuário deve ter para ter permissão de acesso aos dados sensitivos. O valor faz distinção entre maiúsculas e minúsculas. Se essa propriedade não estiver especificada, um valor de vendedor será assumido, permitindo que todos os usuários vejam os dados sensitivos. Se for especificado um valor inválido, o Payment Servlet não será inicializado.

Observe que este parâmetro pode ser definido durante a criação da instância do Payments e atualizado a qualquer momento, utilizando o Configuration Manager do WebSphere Commerce. O nome do parâmetro no Configuration Manager é Função de Acesso Mínimo no painel da instância do Payments. Para obter informações adicionais sobre os painéis do Configuration Manager, consulte o *WebSphere Commerce - Guia de Instalação* para sua plataforma ou consulte a ajuda on-line para o painel da instância do Payments enquanto estiver no Configuration Manager.

A tabela a seguir descreve os valores suportados, listados em ordem crescente de autoridade:

*Tabela 15. Autoridade da Função de Usuário do Payments*

Usuário	Descrição
clerk	Usuários com a função de vendedor ou superior podem ver os dados sensíveis.
supervisor	Usuários com a função de supervisor ou superior podem ver os dados sensíveis.
madmin	Usuários com a função de Administrador do Comerciante ou superior podem ver os dados sensíveis.
psadmin	Apenas Payments Administrators podem ver os dados sensíveis.
none	Ninguém tem permissão para ver os dados sensíveis.

Você pode especificar o parâmetro `wpm.MinSensitiveAccessRole` através do Configuration Manager do WebSphere Commerce.

## Protegendo o Banco de Dados

O banco de dados do WebSphere Commerce Payments armazena dados sensíveis e requer proteção contra leitura e gravação pelas origens não autorizadas. O WebSphere Commerce Payments fornece suporte para a criptografia de dados sensíveis – por exemplo, senhas e informações sobre proprietários de cartões – armazenadas no banco de dados.

## Dados da Transação

Abaixo estão algumas diretrizes para tratamento de dados da transação.

- As informações transacionais sensíveis são armazenadas em uma tabela do banco de dados na biblioteca da instância. Essa biblioteca é especificada como o Instance Schema Name no Payments Instance Creation Wizard.
- Todos os backups devem ser mantidos em segurança.
- As tabelas do banco de dados na biblioteca da instância contêm informações críticas sobre configuração e transação e devem ser incluídas como parte de sua estratégia de backup do sistema. Também é necessário fazer backup do seguinte:
  - Arquivos no diretório `/QIBM/UserData/CommercePayments/V55/instance` em que `instance` é o nome da instância do WebSphere Commerce Payments
  - Instância do servidor HTTP configurada para o WebSphere Commerce Payments. Esse servidor HTTP é especificado como o Servidor Web no Payments Instance Creation Wizard.
  - Objetos na biblioteca da instância na máquina local, como a coleta de banco de dados na máquina remota quando o armazenamento de banco de dados remoto é utilizado.

---

## Parte 5. Tópicos Variados sobre Segurança

Esta parte descreve as várias tarefas de segurança que podem ser executadas pelo administrador do sistema do WebSphere Commerce.




---

## Capítulo 16. Ativando a Segurança do WebSphere Application Server

Este capítulo descreve como ativar segurança para o WebSphere Application Server. Ativar a segurança do WebSphere Application Server impede que todos os componentes Enterprise JavaBeans sejam expostos para chamada remota por qualquer pessoa.

### Notas:

1.  Se a segurança global do WebSphere Application Server estiver ativada conforme descrito nas etapas deste capítulo, não será possível parar o servidor WebSphere Application Server (por exemplo, `server1`) adequadamente a partir do painel Serviços do Windows 2000. Para parar o serviço quando a segurança está ativada, utilize o comando `stopserver` a partir do diretório `WAS_installdir\bin`, em um prompt de comandos, como segue:

```
stopserver server -username user_id -password password
```

em que `server` é o nome do diretório de configuração do WebSphere Application Server do servidor que deseja parar (por exemplo, `server1`), `user_id` é o nome do usuário para autenticação, se a segurança estiver ativada no servidor e `password` é a senha para autenticação, se a segurança estiver ativada no servidor.

Ao tentar parar o servidor a partir do painel Serviços, as propriedades são tais que o ID do usuário e a senha não estão incluídos. Com a segurança global ativada, o ID do usuário e a senha são requeridos para autenticação ao parar o servidor. O serviço continua em execução (apesar do painel Serviços mostrar que está parado). Observe que o ID do usuário e a senha não são requeridos para iniciar o serviço a partir do painel Serviços.

2. Se precisar parar o servidor de aplicativos quando a segurança do WebSphere Application Server estiver ativada, utilize o comando `stopserver` a partir do diretório `WAS_installdir/bin` em um prompt de comandos, da seguinte forma:




```
stopserver server -username user_id -password password
```

em que `server` é o nome do servidor de aplicativos WebSphere Application Server que você deseja parar (por exemplo, `server1`), `user_id` é o nome do usuário para autenticação e `password` é a senha para autenticação.



```
stopserver -instance WAS_instancename server -username user_id  
-password password
```

em que `WAS_instancename` é o nome da instância do WebSphere Application Server, `server` é o nome do servidor de aplicativos WebSphere Application Server que você deseja parar (por exemplo, `server1`), `user_id` é o nome do usuário para autenticação e `password` é a senha para autenticação.

3.     Ao ativar a segurança do WebSphere Application Server, é altamente recomendável que sua máquina atenda os seguintes requisitos:

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

---

## Antes de Iniciar

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

---

## Ativando a Segurança com um Registro de Usuário LDAP

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

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

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

1. Inicie o WebSphere Application Server e abra o WebSphere Application Server Administration Console.
2. No Administration Console, modifique as definições da segurança global como a seguir:
  - a. Em **Segurança**, expanda **Registros de Usuário** e clique em **LDAP**. Preencha os campos na guia **Configuração** como a seguir, dependendo do tipo de servidor de diretório que você está utilizando:

Tabela 16. Usuários do

IBM Directory Server.

▶ AIX
▶ 400
▶ Linux
▶ Solaris
▶ Windows

Nome do Campo	Definição	Valores de Amostra	Notas
ID do Usuário do Servidor	ID do Usuário	<i>user_ID</i>	<ul style="list-style-type: none"> <li>• Este não deve ser o administrador LDAP.</li> <li>• Não utilize um usuário especificado como cn=xxx.</li> <li>• Assegure que a classe de objeto deste usuário seja compatível com a classe de objeto especificada no campo Filtro do Usuário da janela Propriedades Avançadas de LDAP.</li> </ul>
Senha do Usuário do Servidor	Senha do Usuário	<i>password</i>	
Tipo	Tipo de servidor LDAP	SecureWay	
Host	Nome do host do servidor LDAP	<i>hostname.domain.com</i>	
Porta	Porta que o servidor LDAP está utilizando		Este campo não é necessário
Nome Distinto Base	Nome distinto sob o qual a pesquisa ocorre	<i>o=ibm,c=us</i>	
Nome Distinto de Vinculação	Nome distinto para vincular ao diretório durante a pesquisa		Este campo não é necessário
Senha de Vinculação	Senha para o Nome Distinto de Vinculação		Este campo não é necessário

Tabela 17. Usuários do Netscape. 

Nome do Campo	Definição	Valores de Amostra	Notas
ID do Usuário do Servidor	ID do Usuário	<i>user_ID</i>	<ul style="list-style-type: none"> <li>• Este não deve ser o administrador LDAP.</li> <li>• Não utilize um usuário especificado como cn=xxx.</li> <li>• Assegure que a classe de objeto deste usuário seja compatível com a classe de objeto especificada no campo Filtro do Usuário da janela Propriedades Avançadas de LDAP.</li> </ul>
Senha do Usuário do Servidor	Senha do Usuário	<i>password</i>	
Tipo	Tipo de servidor LDAP	Netscape	
Host	Nome do host do servidor LDAP	<i>hostname.domain.com</i>	
Porta	Porta que o servidor LDAP está utilizando		Este campo não é necessário
Nome Distinto Base	Nome distinto sob o qual a pesquisa ocorre	<i>o=ibm</i>	
Nome Distinto de Vinculação	Nome distinto para vincular ao diretório durante a pesquisa		Este campo não é necessário
Senha de Vinculação	Senha para o Nome Distinto de Vinculação		Este campo não é necessário

Tabela 18. Usuários do Domino. 

Nome do Campo	Definição	Valores de Amostra	Notas
ID do Usuário do Servidor	Nome Abreviado/ID do Usuário	<i>user_ID</i>	Assegure que a classe de objeto deste usuário seja compatível com a classe de objeto especificada no campo Filtro do Usuário da janela Propriedades Avançadas de LDAP.
Senha do Usuário do Servidor	Senha do Usuário	<i>password</i>	



Tabela 18. Usuários do Domino (continuação). Windows

Nome do Campo	Definição	Valores de Amostra	Notas
Tipo	Tipo de servidor LDAP	Domino 5.0	
Host	Nome do host do servidor LDAP	<i>hostname.domain.com</i>	
Porta	Porta que o servidor LDAP está utilizando		Este campo não é necessário
Nome Distinto Base	Nome distinto sob o qual a pesquisa ocorre		Este campo não é necessário
Nome Distinto de Vinculação	Nome distinto para vincular ao diretório durante a pesquisa		Este campo não é necessário
Senha de Vinculação	Senha para o Nome Distinto de Vinculação		Este campo não é necessário

Tabela 19. Usuários do Active Directory. Windows

Nome do Campo	Definição	Valores de Amostra	Notas
ID do Usuário do Servidor	sAMAccountName	<i>user_ID</i>	<ul style="list-style-type: none"> <li>Nome de Logon do Usuário de qualquer usuário comum.</li> <li>Não utilize um usuário especificado como cn=xxx.</li> <li>Assegure que a classe de objeto deste usuário seja compatível com a classe de objeto especificada no campo Filtro do Usuário da janela Propriedades Avançadas de LDAP.</li> </ul>
Senha do Usuário do Servidor	Senha do Usuário	<i>password</i>	
Tipo	Tipo de servidor LDAP	Active Directory	
Host	Nome do host do servidor LDAP	<i>hostname.domain.com</i>	
Porta	Porta que o servidor LDAP está utilizando		Este campo não é necessário
Nome Distinto Base	Nome distinto sob o qual a pesquisa ocorre	CN=users, DC=domain1, DC=domain2, DC=com	

Tabela 19. Usuários do Active Directory (continuação). Windows

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

Clique em **Aplicar** e, em seguida **Salvar**.

b. No Administration Console, expanda **Segurança** e clique em **Segurança Global**.

1) Na guia Configuração de Segurança Global, selecione **Ativado** e limpe **Reforçar Segurança de Java 2**.

**Nota:** O WebSphere Commerce 5.5 não suporta a segurança de Java 2.

2) No campo Mecanismo de Autenticação Ativo, selecione **LTPA (Lightweight Third Party Authentication)**.

3) No campo Registro do Usuário Ativo, selecione **LDAP**.

4) Clique em **Aplicar** e, em seguida **Salvar**.

c. No Administration Console, expanda **Segurança** e, em seguida, expanda **Mecanismos de Autenticação** e clique em **LTPA**.

1) Na guia Configuração de LPTA, preencha as definições de LTPA conforme requerido.

2) Em Propriedades Adicionais, clique em **SSO (Conexão Única)** e limpe a caixa de opções **Ativado** se não desejar utilizar esta funcionalidade.

3) Clique em **Aplicar** e, em seguida **Salvar**.

d. No Administration Console, expanda **Aplicativos** e, em seguida, clique em **Aplicativos Corporativos**.

1) Na janela Aplicativos Corporativos, clique no aplicativo Commerce, **WC\_instance\_name** (por exemplo, **WC\_demo**).

2) Em Propriedades Adicionais, clique em **Mapear funções de segurança para usuários/grupos**.

3) Clique em **Procurar usuários** e localize o usuário cuja função você deseja mapear.

4) Para esse usuário, selecione **WCSecurityRole** e clique em **OK**.

3. Feche o Administration Console, pare e inicie novamente o WebSphere Application Server Administration Console. A partir de agora, quando você abrir o WebSphere Application Server Administration Console, serão solicitados o ID e a senha do Servidor de Segurança.

4. Abra o WebSphere Commerce Configuration Manager e selecione **Instâncias > instance\_name > Propriedades da Instância > Segurança** e clique na caixa de opções **Ativar**. Será solicitado que você digite o nome e a senha do usuário informados na etapa 2b. Clique em **Aplicar** e saia do Configuration Manager.

5. Encerre e inicie novamente o WebSphere Application Server Administration Console.

## Ativando a Segurança com um Registro de Usuário do Sistema Operacional

**AIX** **Linux** **Solaris** Para utilizar o sistema operacional como um registro do usuário, o WebSphere Application Server precisa ser executado como ID root. Execute o WebSphere Application Server como root e execute as etapas a seguir.

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

- AIX** **Linux** **Solaris** Efetue login como root.
- AIX** **Linux** **Solaris** Inicie o WebSphere Application Server e ative o WebSphere Application Server Administration Console enquanto estiver com login efetuado como root. Para inicializar o servidor:

```
cd WAS_installdir/bin
./startServer server
```

em que *server* é o nome do servidor de aplicativos WebSphere Application Server, por exemplo, *server1*.

- No WebSphere Application Server Administration Console modifique as definições da segurança global conforme segue:
  - No Administration Console, expanda **Segurança**, expanda **Registros de Usuários** e clique em **SO Local**. Preencha os campos na guia **Configuração**, para seu servidor de registro de segurança:

Nome do Campo	Valores de Amostra	Notas
ID do Usuário do Servidor	<i>wcsuser</i>	<p><b>400</b> O ID do usuário no iSeries deve ter a autoridade *SEC0FR.</p> <p><b>AIX</b> <b>Solaris</b> <b>Linux</b> Um ID do usuário que é root ou tem autoridade root.</p> <p><b>Windows</b> O ID do usuário com privilégios administrativos do sistema operacional com o qual você efetuou login. Se a máquina pertencer a um domínio, utilize o ID do usuário completo. Por exemplo: <i>DomainXYZ\user_id</i>. Certifique-se de que esta conta exista no servidor do domínio e que seja um membro do grupo do Administrador.</p>

Nome do Campo	Valores de Amostra	Notas
Senha do Servidor de Segurança	<i>password</i>	Esta é a senha pertencente ao usuário com privilégios administrativos do sistema operacional com a qual foi efetuado login.

Clique em **Aplicar** e, em seguida **Salvar**.

- b. No Administration Console, expanda **Segurança** e clique em **Segurança Global**.
  - 1) Na guia Configuração de Segurança Global, selecione **Ativado** e limpe **Reforçar Segurança de Java 2**.
  - 2) No campo Mecanismo de Autenticação Ativo, selecione **SWAM (Simple WebSphere Authentication Mechanism)**.
  - 3) No campo Registro do Usuário Ativo, selecione **SO Local**.
  - 4) Clique em **Aplicar** e, em seguida **Salvar**.
4. No Administration Console, expanda **Aplicativos** e, em seguida, clique em **Aplicativos Corporativos**.
  - a. Na janela Aplicativos Corporativos, clique no aplicativo Commerce, **WC\_instance\_name** (por exemplo, **WC\_demo**).
  - b. Em Propriedades Adicionais, clique em **Mapear funções de segurança para usuários/grupos**.
  - c. Clique em **Procurar usuários** e localize o usuário cuja função você deseja mapear.
  - d. Para esse usuário, selecione **WCSecurityRole** e clique em **OK**.
5. Abra o WebSphere Commerce Configuration Manager e selecione **Lista de Instâncias** → *instance\_name* → **Propriedades da Instância** → **Segurança** e selecione a caixa de opção **Ativar Segurança**. Selecione **Registro de Usuário do Sistema Operacional** para o modo de autenticação e digite o nome do usuário e a senha digitados na etapa 3a na página 191. Clique em **Aplicar** e saia do Configuration Manager.
6. Pare e inicie novamente o servidor de administração do WebSphere Application Server. A partir de agora, quando você abrir o WebSphere Application Server Administration Console, serão solicitados o ID e a senha do Servidor de Segurança.

---

## Desativando a Segurança EJB do WebSphere Commerce

O WebSphere Commerce Business Edition permite desativar a segurança EJB. Para desativar a segurança EJB do WebSphere Commerce, faça o seguinte:

1. Inicie o WebSphere Application Server Administration Console.
2. No Administration Console, expanda **Segurança** e clique em **Segurança Global**. Na guia Configuração de Segurança Global, limpe a caixa de opções **Ativado**.
3. Abra o Configuration Manager do WebSphere Commerce e selecione **Lista de Instâncias** → *instance\_name* → **Propriedades da Instância** → **Segurança** e limpe a caixa de opções **Ativar Segurança**.
4. Saia do WebSphere Application Server Administration Console.
5. Pare e inicie novamente o servidor de administração do WebSphere Application Server.

## Opções de Implementação de Segurança do WebSphere Commerce

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

*Tabela 20. Cenários de Segurança de uma Única Máquina*

A segurança do WebSphere Application Server está ativada.	<ul style="list-style-type: none"> <li>• Utilize o sistema operacional como o registro do WebSphere Application Server.</li> <li>• Utilize o banco de dados como o registro do WebSphere Commerce.</li> </ul>
	<ul style="list-style-type: none"> <li>• Utilize o LDAP como o registro do WebSphere Application Server.</li> <li>• Utilize o LDAP como o registro do WebSphere Commerce.</li> </ul>
	<ul style="list-style-type: none"> <li>• Utilize o LDAP como o registro do WebSphere Application Server.</li> </ul>
A segurança do WebSphere Application Server está desativada e o site de seu WebSphere Commerce está localizado atrás de um firewall.	<ul style="list-style-type: none"> <li>• Um registro do WebSphere Application Server não é requerido.</li> <li>• Utilize o banco de dados como o registro do WebSphere Commerce.</li> </ul>
	<ul style="list-style-type: none"> <li>• Um registro do WebSphere Application Server não é requerido.</li> <li>• Utilize o LDAP como o registro do WebSphere Commerce.</li> </ul>

*Tabela 21. Cenários de Segurança de Várias Máquinas*

A segurança do WebSphere Application Server está ativada. O LDAP está sempre implementado.	<ul style="list-style-type: none"> <li>• Utilize o LDAP como o registro do WebSphere Application Server.</li> <li>• Utilize o LDAP como o registro do WebSphere Commerce.</li> </ul>
	<ul style="list-style-type: none"> <li>• Utilize o LDAP como o registro do WebSphere Application Server.</li> <li>• Utilize um banco de dados como o registro do WebSphere Commerce.</li> <li>• Será necessário configurar o LDAP e colocar uma entrada administrativa no registro do LDAP.</li> </ul>
A segurança do WebSphere Application Server está desativada e o site de seu WebSphere Commerce está localizado atrás de um firewall.	<ul style="list-style-type: none"> <li>• Utilize um banco de dados como o registro do WebSphere Commerce.</li> <li>• Um registro do WebSphere Application Server não é requerido.</li> <li>• Sign-on único não é suportado.</li> </ul>
	<ul style="list-style-type: none"> <li>• Utilize o LDAP como o registro do WebSphere Application Server.</li> <li>• Um registro do WebSphere Application Server não é requerido.</li> </ul>

**Nota:** Se você operar o site do WebSphere Commerce de trás de um firewall, será possível desativar a segurança do WebSphere Application Server. Você deve

desativar a segurança do WebSphere Application Server apenas se tiver certeza de que nenhum aplicativo mal intencionado esteja em execução atrás do firewall.

---

## Configuração de Segurança para o Monitor de Cache Dinâmico

Se estiver utilizando o Monitor de Cache Dinâmico do WebSphere Application Server para monitorar e se o aplicativo que está sendo monitorado tiver funções de segurança definidas em seu descritor de implementação, será necessário fazer o seguinte:

Para navegar para o painel "Etapa: Mapear Funções de Segurança para Usuários/Grupos" no WebSphere Application Server Administration Console, clique em **Aplicativos** —> **Instalar Novo Aplicativo** e conclua as etapas (não relacionadas à segurança) requeridas. (Para obter informações adicionais, consulte os tópicos "Implementando Aplicativos Protegidos" e "Atribuindo Funções a Usuários e Grupos" no WebSphere Application Server Information Center (<http://www.ibm.com/software/webservers/appserv/infocenter.html>.) No painel "Etapa: Mapear Funções de Segurança para Usuários/Grupos":

1. Especifique os usuários e grupos que são mapeados para cada uma das funções de segurança.
2. Selecione a caixa de opções ao lado de **Função**, conforme requerido, para selecionar todas as funções ou para selecionar funções individuais. Para cada função, você pode especificar se usuários predefinidos, tais como, Todos ou Todos os Usuários Autenticados são mapeados para a função. Para selecionar usuários ou grupos específicos do registro de usuários:
  - a. Selecione uma função e clique em **Consultar Usuários** ou **Consultar Grupos**.
  - b. No painel **Consultar Usuários** ou **Consultar Grupos** exibido, insira os critérios de pesquisa para extrair uma lista de usuários ou grupos do registro de usuários.
  - c. Selecione usuários ou grupos individuais dos resultados exibidos.
  - d. Clique em **OK** para mapear os usuários ou grupos selecionados para a função selecionada no painel "Etapa: Mapear Funções de Segurança para Usuários/Grupos".

No momento, existe uma função definida que fornece acesso a toda a funcionalidade do monitor de cache. Isto significa que esta página pode ser utilizada para especificar quais usuários podem ter acesso ao Monitor de Cache Dinâmico.

---

## Administrando Instâncias do WebSphere Commerce Através do Configuration Manager

Se você tiver a segurança global do WebSphere Application Server ativada, deverá executar as seguintes etapas para parar, iniciar, criar ou excluir corretamente instâncias do WebSphere Commerce ou do WebSphere Commerce Payments utilizando o Configuration Manager:

1. No diretório `WAS_installdir/properties`, atualize os seguintes arquivos e propriedades para os seguintes valores:
  - `sas.client.props`
    - `com.ibm.CORBA.securityEnabled=true`
    - `com.ibm.CORBA.loginSource=properties`

```
com.ibm.CORBA.LoginUserid=validUser
com.ibm.CORBA.LoginPassword=validPassword
```

- soap.client.props

```
com.ibm.SOAP.loginUserid=validUser
com.ibm.SOAP.loginPassword=validPassword
com.ibm.SOAP.secrityEnabled=true
```

2. No diretório *WAS\_installdir/bin*, execute o comando *PropFilePasswordEncoder* (em uma linha) para codificar a senha nos arquivos *sas.client.props* e *soap.client.props*.

▶ AIX ▶ Linux ▶ Solaris

```
PropFilePasswordEncoder.sh WAS_installdir/properties/
sas.client.props com.ibm.CORBA.LoginPassword
```

```
PropFilePasswordEncoder.sh WAS_installdir/properties/
soap.client.props com.ibm.SOAP.loginPassword
```

▶ 400

```
PropFilePasswordEncoder.sh WAS_userdir/WAS_instance/properties/
sas.client.props com.ibm.CORBA.LoginPassword
```

```
PropFilePasswordEncoder.sh WAS_userdir/WAS_instance/properties/
soap.client.props com.ibm.SOAP.loginPassword
```

▶ Windows

```
PropFilePasswordEncoder.bat WAS_installdir\properties\
sas.client.props com.ibm.CORBA.LoginPassword
```

```
PropFilePasswordEncoder.bat WAS_installdir\properties\
soap.client.props com.ibm.SOAP.loginPassword
```

3. Atualize o script *config\_client*:

▶ AIX ▶ 400 ▶ Linux ▶ Solaris

Adicione *\$CLIENTSOAP \$CLIENTSAS* à lista de argumentos Java. Por exemplo:

```
${JAVA_EXE?} -classpath $CLASSPATH -DIDIR="$WPMDIR"
-Djava.security.policy="config.policy" -Djava.version="1.3"
-Dwas.install.root="$WAS_HOME " -Dwas.repository.root="$CONFIG_ROOT"
-Dcom.ibm.CORBA.BootstrapHost="$COMPUTERNAME" $CLIENTSOAP $CLIENTSAS
$PM_ARGS -Xmx128m com.ibm.commerce.config.client.CMClient "$@"
```

▶ Windows

Adicione *%CLIENTSOAP% %CLIENTSAS%* à lista de argumentos Java. Por exemplo:

```
"%JAVA_HOME%\bin\java" %CLIENTSOAP% %CLIENTSAS% %PM_ARGS% "
-Dwas.install.root=%WAS_HOME% " -Dwas.repository.root=%CONFIG_ROOT%"
-Dcom.ibm.CORBA.BootstrapHost=%COMPUTERNAME%
-Djava.security.policy="config.policy"
com.ibm.commerce.config.client.CMClient %*
```

4. Atualize o script *config\_server*:

▶ AIX ▶ 400 ▶ Linux ▶ Solaris

Adicione *\$CLIENTSOAP \$CLIENTSAS* à lista de argumentos Java. Por exemplo:

```
${JAVA_EXE?} -classpath $CLASSPATH -DIDIR="$WPMDIR"
-Djava.security.policy="config.policy"
-Dwas.install.root="$WAS_HOME " -Dwas.repository.root="$CONFIG_ROOT"
-Dws.ext.dirs="$WAS_EXT_DIRS" -Dcom.ibm.CORBA.BootstrapHost="$COMPUTERNAME"
$CLIENTSOAP $CLIENTSAS $PM_ARGS $MAX_HEAP
com.ibm.commerce.config.server.CMServerImpl "$@"
```

▶ Windows

Adicione *%CLIENTSOAP% %CLIENTSAS%* à lista de argumentos Java. Por exemplo:

```
"%JAVA_HOME%\bin\java.exe" %CLIENTSOAP% %CLIENTSAS% %PM_ARGS%  
"-Dwas.install.root=%WAS_HOME%" "-Dwas.repository.root=%CONFIG_ROOT%"  
"-Dws.ext.dirs=%WAS_EXT_DIRS%" -Dcom.ibm.CORBA.BootstrapHost=%COMPUTERNAME%  
-Djava.security.policy="config.policy"  
com.ibm.commerce.config.server.CMServerImpl %*
```



---

## Capítulo 17. Ativando o SSL para Produção com o IBM HTTP Server

**400** Esta seção não se aplica à plataforma iSeries. Para obter informações do iSeries, consulte “Ativando o SSL no IBM HTTP Server (iSeries)” na página 204.

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

---

### Sobre Segurança

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

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

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

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

Estas etapas são descritas detalhadamente a seguir.

#### Notas:

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

---

### Configurando um Arquivo de Chaves de Segurança para Produção

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

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

3. Crie uma cópia de backup de `httpd.conf` e renomeie a cópia de backup do arquivo para `httpd.conf.backup`.
4. Abra `httpd.conf` em um editor de texto.
5. Assegure-se de que as seguintes linhas estejam sem a marca de comentário (removendo o sinal “#” da frente da linha) para a porta 443:

- **Windows**

- a. `LoadModule ibm_ssl_module modules/IBMModuleSSL128.dll`
- b. `Listen 443`
- c. `<VirtualHost host.some_domain.com:443>` (Também será necessário substituir o nome do host completo nessa linha.)
- d. `SSLEnable`
- e. `</VirtualHost>`
- f. `Keyfile "HTTPServer_installdir/ssl/keyfile.kdb"`

- **AIX** **Linux** **Solaris**

- a. `LoadModule ibm_ssl_module libexec/mod_ibm_ssl_128.so`
- b. `AddModule mod_ibm_ssl.c`
- c. `Listen 443`
- d. `<VirtualHost host.some_domain.com:443>` (Também será necessário substituir o nome do host completo nessa linha.)
- e. `SSLEnable`
- f. `</VirtualHost>`
- g. `SSLDisable`
- h. `Keyfile "HTTPServer_installdir/ssl/keyfile.kdb"`
- i. `SSLV2Timeout 100`
- j. `SSLV3Timeout 1000`

6. Assegure-se de que as seguintes linhas estejam sem a marca de comentário (removendo o sinal “#” da frente da linha).

- a. Para as ferramentas administrativas do WebSphere Commerce, são necessárias as portas 8000, 8002 e 8004:

```
Listen 8000
Listen 8002
Listen 8004
```

Se estiver utilizando o WebSphere Commerce Payments, também serão necessárias as portas 5432 e 5433:

```
Listen 5432
Listen 5433
```

- b. Assegure-se de que as seções virtuais do host das portas acima também não tenham a marca de comentário (removendo o sinal “#” da frente das linhas, se estiverem presentes). Você deve substituir o nome completo do host conforme apropriado nessas seções. Para obter uma lista das variáveis de nome de caminho padrão nos exemplos a seguir, consulte “Variáveis de Caminho” na página ix.



Os exemplos a seguir foram derivados das seções do host virtual não comentadas em um arquivo `httpd.conf` do sistema Windows; estas seções são semelhantes em outros sistemas operacionais.

---

---

```
##### IBM WebSphere Payments (Do not edit this section) #####
Listen 5432
Listen 5433##### End of IBM WebSphere Payments (Do not edit this section) #####

...

##### IBM WebSphere Commerce (Do not edit this section) #####
Listen 8000
Listen 8002
Listen 8004##### End of IBM WebSphere Commerce (Do not edit this section) #####
```

---

Figura 7. Exemplo de Seções "Listen" do Arquivo httpd.conf

---

```
##### End of IBM WebSphere Commerce (Do not edit this section) #####
## VirtualHost: Allows the daemon to respond to requests for more than one
## server address, if your server machine is configured to accept IP packets
## for multiple addresses. This can be accomplished with the ifconfig
## alias flag, or through kernel patches like VIF.
#
## Any httpd.conf or srm.conf directive may go into a VirtualHost command.
## See also the BindAddress entry.
#
#<VirtualHost host.some_domain.com:443>
```

---

Figura 8. Exemplo de Cabeçalho de Seção Virtual do Host de um Arquivo httpd.conf

---

```
##### IBM WebSphere Payments (Do not edit this section) #####
<VirtualHost host.some_domain.com:5433>
SSLEnable
SSLClientAuth 0
ServerName wordsworth.torolab.ibm.com
DocumentRoot
"HTTPServer_installdir\htdocs\en_US"
</VirtualHost>
##### End of IBM WebSphere Payments (Do not edit this section) #####
```

---

Figura 9. Exemplo de Seção Virtual do Host do Arquivo httpd.conf do Payments

---

```
##### IBM WebSphere Commerce (Do not edit this section) #####
#Instance name : instance_name
<VirtualHost host.some_domain.com:80>
ServerName host.some_domain.com
DocumentRoot
"HTTPServer_installdir\htdocs/en_US"
Alias /wcsdoc "WC_installdir/web/doc"
Alias /wcsstore "WAS_installdir\installedApps\host\WC_instance_name.ear/Stores.war"
Alias /wcs "WAS_installdir\installedApps\host\WC_instance_name.ear/CommerceAccelerator.war"
</VirtualHost>
```

---

Figura 10. Exemplo de Seção Virtual do Host do Arquivo httpd.conf da Porta 80 do WebSphere Commerce. (Porta Não Protegida)

---

```

<VirtualHost
host.some_domain.com:443>
SSLEnable
SSLClientAuth 0
ServerName host.some_domain.com
DocumentRoot "HTTPServer_installdir/htdocs/en_US"
Alias /wcsdoc "WC_installdir/web/doc"
Alias /wcsstore "WAS_installdir\installedApps\host\WC_instance_name.ear/Stores.war"
Alias /wcs "WAS_installdir\installedApps\host\WC_instance_name.ear/CommerceAccelerator.war"
</VirtualHost>

```

---

*Figura 11. Exemplo de Seção Virtual do Host do Arquivo httpd.conf da Porta 443 do WebSphere Commerce. (Porta Protegida)*

---

```

<VirtualHost host.some_domain.com:8000>
SSLEnable
SSLClientAuth 0
ServerName host.some_domain.com
DocumentRoot
"HTTPServer_installdir/htdocs/en_US"
Alias /wcsdoc "WC_installdir/web/doc"
Alias /wchelp "WC_installdir/web/doc/en_US"
Alias /adminconsole "WAS_installdir\installedApps\host\WC_instance_name.ear/SiteAdministration.war/tools/adminconsole/wcsadmincon.html"
Alias /wcsstore "WAS_installdir\installedApps\host\WC_instance_name.ear/Stores.war"
Alias /accelerator "WAS_installdir\installedApps\host\WC_instance_name.ear/CommerceAccelerator.war/tools/common/accelerator.html"
Alias /wcs "WAS_installdir\installedApps\host\WC_instance_name.ear/CommerceAccelerator.war"
Alias /wcadmin "WAS_installdir\installedApps\host\WC_instance_name.ear/SiteAdministration.war"
Alias /wcorgadmin "WAS_installdir\installedApps\host\WC_instance_name.ear/OrganizationAdministration.war"
Alias /orgadminconsole "WAS_installdir\installedApps\host\WC_instance_name.ear/OrganizationAdministration.war/tools/buyerconsole/wcsbuyercon.html"
</VirtualHost>

```

---

*Figura 12. Exemplo de Seção Virtual do Host do Arquivo httpd.conf da Porta 8000 do WebSphere Commerce. (WebSphere Commerce Accelerator)*

---

```

<VirtualHost
host.some_domain.com:8002>
SSLEnable
SSLClientAuth 0
ServerName host.some_domain.com
DocumentRoot "HTTPServer_installdir/htdocs/en_US"
Alias /wcsdoc "WC_installdir/web/doc"
Alias /wchelp "WC_installdir/web/doc/en_US"
Alias /adminconsole "WAS_installdir\installedApps\host\WC_instance_name.ear/SiteAdministration.war/tools/adminconsole/wcsadmincon.html"
Alias /wcsstore "WAS_installdir\installedApps\host\WC_instance_name.ear/Stores.war"
Alias /accelerator "WAS_installdir\installedApps\host\WC_instance_name.ear/CommerceAccelerator.war/tools/common/accelerator.html"
Alias /wcs "WAS_installdir\installedApps\host\WC_instance_name.ear/CommerceAccelerator.war"
Alias /wcadmin "WAS_installdir\installedApps\host\WC_instance_name.ear/SiteAdministration.war"
Alias /wcorgadmin "WAS_installdir\installedApps\host\WC_instance_name.ear/OrganizationAdministration.war"
Alias /orgadminconsole "WAS_installdir\installedApps\host\WC_instance_name.ear/OrganizationAdministration.war/tools/buyerconsole/wcsbuyercon.html"
</VirtualHost>

```

---

*Figura 13. Exemplo de Seção Virtual do Host do Arquivo httpd.conf da Porta 8002 do WebSphere Commerce. WebSphere Commerce Administration Console*

---

```

<VirtualHost host.some_domain.com:8004>
SSLEnable
SSLClientAuth 0
ServerName host.some_domain.com
DocumentRoot "HTTPServer_installdir/htdocs/en_US"
Alias /wcsdoc "WC_installdir/web/doc"
Alias /wchelp "WC_installdir/web/doc/en_US"
Alias /adminconsole "WAS_installdir\installedApps\host\WC_instance_name.ear\SiteAdministration.war\tools\adminconsole\wcsadmincon.html"
Alias /wcsstore "WAS_installdir\installedApps\host\WC_instance_name.ear\Stores.war"
Alias /accelerator "WAS_installdir\installedApps\host\WC_instance_name.ear\CommerceAccelerator.war\tools\common\accelerator.html"
Alias /wcs "WAS_installdir\installedApps\host\WC_instance_name.ear\CommerceAccelerator.war"
Alias /wadmin "WAS_installdir\installedApps\host\WC_instance_name.ear\SiteAdministration.war"
Alias /wcorgadmin "WAS_installdir\installedApps\host\WC_instance_name.ear\OrganizationAdministration.war"
Alias /orgadminconsole "WAS_installdir\installedApps\host\WC_instance_name.ear\OrganizationAdministration.war\tools\buyerconsole\wcsbuyercon.html"
</VirtualHost>
##### End of IBM WebSphere Commerce (Do not edit this section) #####




```


---

Figura 14. Exemplo de Seção Virtual do Host do Arquivo `httpd.conf` da Porta 8004 do WebSphere Commerce. WebSphere Commerce Organization Administration Console

**Nota:** Recomenda-se que seu software de firewall bloqueie o acesso externo às portas que você configurou para o WebSphere Commerce Tools (portas 8000, 8002 e 8004, por padrão). Consulte a documentação do software de firewall que você está utilizando em seu site para obter informações sobre como fazer isso.

7. Salve as alterações.
8. Para assegurar-se de que seu arquivo `httpd.conf` não contenha erros de sintaxe:

   Altere para o subdiretório `bin` sob o diretório de instalação do IBM HTTP Server em sua máquina e execute o seguinte comando:  
`./httpd -t`

 Altere para o diretório de instalação do IBM HTTP Server em sua máquina e execute o seguinte comando:  
`apache -t`

9. Inicie o IBM HTTP Server.

---

## Solicitando um Certificado Seguro de uma Autoridade de Certificação

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

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

### Usuários da Equifax

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

<http://www.equifax.com>

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

### Usuários da VeriSign

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

<http://www.verisign.com>

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

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

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

---

## Recebendo e Definindo seu Arquivo de Chaves de Produção como o Arquivo de Chaves Atual

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

1. Copie os arquivos *certificatename.kdb*, *certificatename.rdb* e *certificatename.sth* que você recebeu da autoridade de certificação para o subdiretório `ssl` sob o caminho de instalação do IBM HTTP Server em sua máquina, em que *certificatename* é o nome do certificado que você forneceu com seu pedido de certificado.
2. Pare o IBM HTTP Server.
3. ► **AIX** ► **Solaris** Exporte `JAVA_HOME` executando os seguintes comandos:

```
DISPLAY=host_name:0.0
export DISPLAY
JAVA_HOME=java_home
export JAVA_HOME
```

em que *host\_name* é o nome completo do host da máquina que você está utilizando atualmente e *java\_home* é:

- ► **AIX** `/usr/java130`
- ► **Solaris** `/opt/WebSphere/AppServer/java131`

4. Abra o Utilitário Key Management (ikeyman).
5. Abra o arquivo *certificatename.kdb* e digite sua senha quando solicitado.
6. Selecione **Certificados Pessoais** e clique em **Receber**.
7. Clique em **Navegar**.
8. Selecione a pasta onde você armazenou os arquivos recebidos da autoridade de certificação. Selecione o arquivo *certificatename.txt* e clique em **OK**.
9. O quadro de listagem **Certificados Pessoais**, agora, deve listar o certificado *certificatename* da VeriSign ou o certificado *certificatename* da Equifax.
10. Saia do Utilitário de Gerenciamento de Chaves.
11. Mude o diretório para o subdiretório `conf` sob o caminho de instalação do IBM HTTP Server em sua máquina.
12. Crie uma cópia de backup do `httpd.conf`.
13. Abra `httpd.conf` em um editor de texto.
14. Certifique-se de que as linhas listadas na etapa 5 na página 198 não estejam comentadas.

15. Pesquise a diretriz Keyfile "*keyfile\_path\_name/keyfile.kdb*" e altere o nome do caminho para que este aponte para o arquivo criado nas etapas anteriores.
16. Inicie Novamente o IBM HTTP Server.

---

## Testando o Arquivo de Chaves de Produção

Para testar a chave de produção, faça o seguinte:

1. Vá para a seguinte URL com seu navegador:

`https://host_name`

**Notas:**

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

Se a sua chave estiver definida corretamente, você verá várias mensagens sobre o seu novo certificado.

2. No painel **Novo Certificado do Site**, se desejar aceitar esse certificado, selecione o botão de opção **Aceitar esse certificado para sempre (até que ele expire)**.
3. No navegador Web, restaure as definições do servidor de armazenamento em cache e proxy (ou soquetes) para seus estados originais.

Agora, você ativou o SSL no servidor.

---

## Consideração sobre SSL para o WebSphere Commerce Payments

Por padrão, a comunicação entre o WebSphere Commerce e o WebSphere Commerce Payments é através do SSL. No entanto, se você ativar diretamente a interface com o usuário do WebSphere Commerce Payments como a seguir, estará chamando o WebSphere Commerce Payments utilizando a comunicação não-SSL:

`http://host_name:port_number/webapp/PaymentManager`

em que *host\_name* é o nome da máquina do servidor Payments e *port\_number* é 5432 (por padrão).

Para assegurar-se de que a comunicação seja através do SSL, utilize o seguinte URL:

`https://host_name:port_number/webapp/PaymentManager`

em que *host\_name* é o nome da máquina do servidor Payments e *port\_number* é 5433 (por padrão).

---

## Melhorando a Confidencialidade

Quando o WebSphere Commerce recebe um pedido de URL, o controlador da Web recupera o nome da interface para o comando do controlador solicitado e utiliza-o para consultar o nome da classe de implementação a partir da tabela CMDREG. Também determina se o protocolo HTTPS (protegido) é requerido para o pedido de URL, verificando a coluna HTTPS na tabela URLREG.

Qualquer comando que exiba informações sigilosas deve ter o valor HTTPS definido como um valor de "1" (um) na tabela URLREG. Por exemplo, um comando de exibição `OrderProcessView` que contém detalhes de um pedido do cliente deve ser

transmitido apenas através do protocolo HTTPS e, portanto, a entrada OrderProcessView na tabela URLREG possui um valor de "1" (um) na coluna HTTPS.

---

## Ativando o SSL no IBM HTTP Server (iSeries)

▶ 400 A seção se aplica à plataforma iSeries.

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

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

Para obter informações detalhadas sobre como ativar o SSL no IBM HTTP Server para iSeries, consulte o Centro de Informações do iSeries (<http://publib.boulder.ibm.com/html/as400/infocenter.html>). Uma vez no site, selecione a versão de seu sistema operacional e o seu idioma e clique em **Ir**. Pesquise o tópico "Protegendo aplicativos com o SSL" para obter orientação sobre como ativar o SSL.

## Utilizando o SSL com o WebSphere Commerce Payments

Se você criar a loja de certificados do sistema depois de criar sua instância do WebSphere Commerce, deverá conceder à ambas instâncias do WebSphere Commerce Payments e do WebSphere Commerce acesso à loja de certificados do sistema. Por exemplo, os seguintes comandos concederão à instância do WebSphere Commerce Payments o acesso requerido em um sistema V5R1:

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

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

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

Se você escolher utilizar uma instância remota do WebSphere Commerce Payments, deverá configurar a instância do WebSphere Commerce e a instância do WebSphere Commerce Payments para tornar confiável a autoridade de certificação remota que emite o certificado digital. Para estabelecer um relacionamento de confiança entre os dois aplicativos remotos, consulte o seguinte procedimento de alto nível:

1. Na máquina do WebSphere Commerce, utilize o Digital Certificate Manager para exportar a autoridade de certificação do servidor.
2. Transfira o arquivo de certificado para a máquina do WebSphere Commerce Payments.



3. Na máquina do WebSphere Commerce Payments, utilize o Digital Certificate Manager para importar a autoridade de certificação do servidor WebSphere Commerce.
4. Configure o servidor de aplicativos do WebSphere Commerce Payments para tornar confiável a autoridade de certificação importada do servidor WebSphere Commerce.
5. Na máquina do WebSphere Commerce Payments, utilize o Digital Certificate Manager para exportar a autoridade de certificação do servidor.
6. Transfira o arquivo de certificado para a máquina do WebSphere Commerce.
7. Na máquina do WebSphere Commerce, utilize o Digital Certificate Manager para importar a autoridade de certificação do servidor WebSphere Commerce Payments.
8. Configure o servidor de aplicativos do WebSphere Commerce para tornar confiável a autoridade de certificação importada do servidor WebSphere Commerce Payments.

Para obter informações detalhadas, consulte o seguinte endereço da Web e pesquise **Dicas e Sugestões**: página da Web WebSphere Commerce Technical Library (<http://www.software.ibm.com/software/commerce/wscom/library/lit-tech.html>)



---

## Capítulo 18. Ativando o SSL para o IBM Directory Server (LDAP)

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

---

### Configurando o IBM Directory Server

**400** Esta seção não se aplica à plataforma iSeries. Para obter informações do iSeries, consulte “Configurando o IBM OS/400 Directory Services na Plataforma iSeries”.

Para configurar o IBM Directory Server:

1. Instale o IBM Directory Server de acordo com as instruções de instalação do produto IBM Directory Server. Certifique-se de instalar o componente GSKit:
2. Após a conclusão da instalação, chame o IBM Key Manager executando o executável gsk5ikm.
3. Crie um novo arquivo de banco de dados de chave CMS. Certifique-se de que **senha de armazenamento para arquivo** esteja selecionada (por exemplo, ldap\_key.kdb)
4. Crie um certificado auto assinado utilizando a versão X509 V3 e o tamanho de chave 1024. (Você pode atribuir um rótulo significativo ao certificado, por exemplo, seu nome.)
5. Extraia o certificado como um arquivo de certificado (por exemplo, cert.arm), utilizando o tipo de dados Dados ASCII codificados em Base64.
6. Abra um navegador para o seguinte endereço: `http://host_name/ldap` em que *host\_name* é o nome da máquina do servidor LDAP.
7. Clique em **Segurança** —> **SSL** —> **Definições** e faça as seguintes alterações:
  - Status SSL: SSL ativo ou somente SSL
  - Método de autenticação: Autenticação do Servidor
  - Porta de segurança: 636
  - Caminho e nome do arquivo do banco de dados de chave:
    - AIX** **Linux** **Solaris** /Keys/ldap\_key.kdb
    - Windows** *unidade*:\Keys\ldap\_key.kdb
  - Rótulo de chave: *your\_label* (O rótulo do certificado).
  - Senha de chave: *xxxxx* (A senha do arquivo de banco de dados de Chave CMS. Se você escolher **Esconder a Senha em um Arquivo**, não é necessário inserir a senha.)
8. Clique em **Update** e inicie novamente o SecureWay.

---

### Configurando o IBM OS/400 Directory Services na Plataforma iSeries

**400** Para configurar o IBM OS/400 Directory Services no iSeries:

1. Instale o IBM iSeries Access para Windows.
2. Inicie o iSeries Navigator em uma máquina do Windows selecionando **Iniciar** —> **Programas** —> **IBM iSeries Access para Windows** —> **iSeries Navigator**.

3. Crie uma conexão com a máquina de destino do iSeries se não existir nenhuma conexão para a máquina.
4. Expanda a máquina de destino no painel à esquerda, em seguida expanda **Rede** —>**Servidores** no painel à esquerda.
5. Clique em **TCP/IP** no painel à esquerda.
6. Clique com o botão direito em **Diretório** no painel direito e selecione **Propriedades** no menu pop-up.
7. Na janela Propriedades do Diretório, clique na guia **Rede**.
8. Clique em **Digital Certificate Manager** para ativar o Digital Certificate Manager e atribuir um certificado ao Aplicativo "Servidor de Serviços do Diretório".
9. Após atribuir o certificado a um servidor de Serviços do Diretório, clique em **OK** para fechar a janela Propriedades do Diretório.
10. Abra novamente a janela Propriedades do Diretório e você verá que o SSL (Secure Socket Layer) está ativado. Você pode aceitar as definições padrão:
  - Status do SSL:
  - Método de Autenticação: Autenticação do Servidor
  - Porta de segurança: 636
11. Inicie novamente o servidor de Serviços do Diretório.

## Atribuindo e Importando um Certificado Auto Assinado ao WebSphere Application Server

**400** Se seu Certificado SSL não tiver sido emitido por uma CA (Autoridade de Certificação), tal como, VeriSign ou Thwate, será necessário exportar a CA local de uma máquina do iSeries e importá-la para o armazenamento de chaves confiável padrão na máquina do WebSphere Commerce. Para ativar o SSL com o certificado local do iSeries e exportar a CA local de uma máquina do iSeries, faça o seguinte:

1. Certifique-se de que o servidor HTTP \*Admin está ativo. Caso não esteja, execute:
 

```
STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)
```
2. Abra a página Tarefa do iSeries ativando um navegador para o seguinte endereço: `http://host name:2001/`.
3. Selecione **Digital Certificate Manager**.
4. Clique em **Selecionar uma Loja de Certificados**.
5. A partir da Loja de Certificados, selecione **\*Sistema**.
6. Se você não visualizar o link **Instalar o Certificado de CA Local em seu PC**, então é necessário criar uma CA local:
  - a. Clique em Criar uma CA (Autoridade de Certificação).
  - b. Inicie novamente o \*Admin HTTP Server no iSeries.
  - c. Crie um novo certificado como um tipo de Cliente ou Servidor.
  - d. Selecione a Autoridade de Certificação Local recém criada.
  - e. Atribua esse certificado ao servidor de Serviços de Diretório.
7. Clique em **Instalar Certificado de CA Local em seu PC**.
8. Clique em **Instalar Certificado**. Em seguida, salve o certificado (arquivo .cer) em uma pasta temporária.

9. Importe a autoridade de certificação (arquivo .cer) para o Microsoft Internet Explorer e, em seguida, exporte novamente a autoridade de certificação para um arquivo .cer (Codificação Binária 64) em um diretório temporário.
10. Importe o certificado (Codificação Binária 64) na loja chave de confiança do WebSphere Application Server. Por exemplo:

```
keytool -import -alias nck -file /temp_dir/nck.cer  
-keystore /qibm/proddata/java400/jdk13/lib/security/cacerts
```

---

## WebSphere Application Server

No WebSphere Application Server:

1. Ative o IKeyMan (IBM Key Manager) fornecido com o WebSphere Application Server. (Você pode localizá-lo a partir do menu do WebSphere Application Server ou digitando diretamente `keyman` em uma janela de comandos).

**Nota:** Este IBM Key Manager é diferente do fornecido pelo SecureWay. A senha padrão é 'changeit'.

2. Abra o armazenamento de chaves `carcerts` do WebSphere Application Server (por exemplo, `WAS_installdir\AppServer\java\jre\lib\security\cacerts` no Windows)
3. Passe para os **Certificados do Assinante**, em seguida, clique em **Adicionar**. Utilize o tipo de dados **'Dados ASCII Codificados em Base64'** e escolha o arquivo de certificado criado na etapa 5 na página 207.
4. Insira um nome para o certificado.
5. Feche o IKeyMan.

---

## WebSphere Commerce

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

1. Adicione uma nova variável de ambiente JNDI:

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

2. Altere LdapPort para '636':

```
LdapPort = 636
```

3. Inicie Novamente o WebSphere Commerce.

O seguinte é um exemplo:

```
<MemberSubSystem name="Member SubSystem"
  AuthenticationMode="LDAP"
  ProfileDataStorage="LDAP" >

  <Directory LdapAdminDN="cn=root"
    LdapAuthenticationMode="SIMPLE"
    LdapTimeOut="0"
    LdapVersion="3"
    EntryFileName="E:/WebSphere/WPS/xml/ldap/attributeMap.xml"
    LdapPort="636"
    LdapAdminPW="<adminpassword>"
    LdapHost="<hostname>"
    MigrateUsersFromWCSdb="OFF"
    JNDIEnvPropName1="java.naming.security.protocol"
    JNDIEnvPropValue1="ssl"
    display="false"
    LdapType="SECUREWAY"

    . . . .
  />

</MemberSubSystem>
```

---

## Parte 6. Apêndices





---

## Apêndice. Diretivas e Grupos de Controle de Acesso Padrão

O Apêndice lista as diretivas e grupos padrão fornecidos com o WebSphere Commerce.

---

### Diretivas de Controle de Acesso Padrão

As diretivas de controle de acesso padrão são organizados nas seguintes categorias:

- **Diretivas baseadas em funções:** As diretivas baseadas em funções para cada função padrão. Essas diretivas também são mencionadas como diretivas em nível de comandos porque elas definem quem pode executar cada comando.
- **Diretivas em nível do recurso:** As diretivas em nível do recurso, agrupadas por área de negócios. Essas diretivas definem as ações que um grupo de usuários pode executar em recursos específicos. Em cada área de negócios, as diretivas 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 22. Onde Encontrar Informações sobre Diretivas

Diretivas	Iniciando na Página
Diretivas baseadas em funções	“Diretivas Baseadas em Funções” na página 214
Diretivas de nível de recurso por área de negócios	“Diretivas em Nível do Recurso por Área de Negócios” na página 217
Pedidos	“Pedidos” na página 217
Comércio (contratos)	“Comércio (Contratos)” na página 218
Aprovações	“Aprovações” na página 219
Leilões	“Leilões” na página 219
Inteligência de negócios	“Inteligência de Negócios” na página 219
Associação	“Associação” na página 219
Marketing	“Marketing” na página 220
Catálogo	“Catálogo” na página 221
Conectividade e notificação	“Conectividade e Notificação” na página 221
Aquisição	“Aquisição” na página 222
Cupons	“Cupons” na página 222
Perfil de cliente	“Perfil de Cliente” na página 222
Descontos	“Descontos” na página 222
Estoque Programado	
Gerenciamento de Estoque	
Gerenciamento de pedidos	“Gerenciamento de Pedidos” na página 223
Pagamentos	“Pagamentos” na página 223
Editor de Diretivas	“Editor de Diretivas” na página 224
Consultor de Produto	“Consultor de Produto” na página 224
RFQ	“RFQ” na página 224
Regras	“Regras” na página 224

Tabela 22. Onde Encontrar Informações sobre Diretivas (continuação)

Diretivas	Iniciando na Página
Planejador	“Planejador” na página 225
Commerce Accelerator	“Commerce Accelerator” na página 225
Entrega	“Envio” na página 225
Taxação	“Taxação” na página 225
Ajuda Ativa/Espaços de Trabalho Colaborativos/Atendimento ao Cliente	“Ajuda Ativa/Espaços de Trabalho Colaborativos/Atendimento ao Cliente” na página 225
Estado da Loja	“Estado da Loja” na página 226
Gerenciamento da Loja	

## Diretivas Baseadas em Funções

- SiteAdministratorsCanDoEverything
- BuyerAdministratorsExecuteBuyersAdministratorsCommands
- BuyerApproversExecuteBuyerApproversCmdResourceGroup
- GuestsExecuteGuestUsersCmdResourceGroup
- BecomeUserCustomerServiceGroupExecutesBecomeUserCmdsResourceGroup
- CustomerServiceRepresentativesExecuteCustomerServiceRepCmdResourceGroup
- MarketingManagersExecuteMarketingManagerCmdResourceGroup
- CustomerServiceSupervisorsExecuteCustomerServiceSupervisorCmdResourceGroup
- AccountRepresentativesExecuteAccountRepresentativesCmdResourceGroup
- SalesManagersExecuteSalesManagersCmdResourceGroup
- ProductManagersExecuteProductManagersCmdResourceGroup
- SellerAdministratorsExecuteSellerAdministratorsCommands
- SellersExecuteSellersCmdResourceGroup
- CategoryManagersExecuteCategoryManagersCmdResourceGroup
- Buyers(buy-side)ExecuteBuyers(buy-side)CommandsResourceGroup
- Buyers(sell-side)ExecuteBuyers(sell-side)CommandsResourceGroup
- PickPackersExecutePickPackersCmdResourceGroup
- ReceiversExecuteReceiversCmdResourceGroup
- ReturnsAdministratorsExecuteReturnsAdministratorsCmdResourceGroup
- OperationsManagersExecuteOperationsManagersCmdResourceGroup
- LogisticsManagersExecuteLogisticsManagersCmdResourceGroup
- ProcurementBuyersExecuteProcurementBuyersCmdResourceGroup
- CustomerServiceRepresentativesExecuteCustomerServiceRepresentativeViews
- BuyerAdministratorsExecuteBuyerAdministratorsViews
- BuyerApproversExecuteBuyerApproversViews
- MarketingManagersExecuteMarketingManagersViews
- CustomerServiceSupervisorsExecuteCustomerServiceSupervisorViews
- SalesManagersExecuteSalesManagersViews
- AccountRepresentativesExecuteAccountRepresentativesViews
- Buyers(buy-side)ExecuteBuyers(buy-side)Views
- Buyers(sell-side)ExecuteBuyers(sell-side)Views
- CategoryManagersExecuteCategoryManagersViews

- CustomersExecuteCustomersViews
- ProductManagersExecuteProductManagersViews
- PickPackersExecutePickPackersViews
- ReceiversExecuteReceiversViews
- ReturnsAdministratorsExecuteReturnsAdministratorsViews
- OperationsManagersExecuteOperationsManagersViews
- LogisticsManagersExecuteLogisticsManagersViews
- SellerAdministratorsExecuteSellerAdministratorsViews
- SellersExecuteSellersViews
- RegisteredApprovedUsersExecuteRegisteredApprovedUsersViews
- NonRejectedUsersExecuteNonRejectedUsersViews
- GuestUsersExecuteGuestUsersViews
- RegisteredApprovedUsersExecuteRegisteredApprovedUsersCommandsResourceGroup
- ChannelManagersExecuteChannelManagersCommands
- AllUsersExecuteAllSiteUserCmdResourceGroup
- AllUsersExecuteAllSiteUsersViews
- RegisteredCustomersForOrgExecuteRegisteredUserCmdResourceGroup
- RegisteredCustomersForOrgExecuteRegisteredUserViews
- ChannelManagersExecuteChannelManagersViews
- AllUsersExecuteResellerUserCmdResourceGroup
- AllUsersExecuteResellerUserViews
- RegisteredCustomersForOrgExecuteRegisteredResellerUserCmdResourceGroup
- RegisteredCustomersForOrgExecuteRegisteredResellerUserViews

A tabela a seguir exibe as diretivas baseadas em função por função, grupo de acesso, grupo de recursos e exibição.

**Notas:**

1. A maioria dos itens na tabela, exceto a coluna **Função**, foram divididos em cada célula para fins de exibição, pois são muito grandes.
2. Nem todas as funções abaixo são funções definidas no WebSphere Commerce. Para obter informações adicionais sobre funções definidas do WebSphere Commerce, consulte “Funções” na página 29.

*Tabela 23. Diretivas Baseadas em Função por Função, Grupo de Acesso, Grupo de Recursos e Exibição*

<b>Função</b>	<b>Grupo de Acesso Utilizado em Diretivas Baseadas em Função</b>	<b>Grupo de Recursos Utilizado em Diretivas Baseadas em Função para Comandos do Controlador</b>	<b>Grupo de Ação Utilizado em Diretivas Baseadas em Função para Exibições</b>
Administrador de Site	SiteAdministrators	n/a	n/a
Administrador da Compradora	BuyerAdministrators	BuyerAdministrators CommandsResource Grupo	BuyerAdministrators Views
Aprovador do Comprador	BuyerApprovers	BuyerApproversCmd ResourceGroup	BuyerApproversViews
Guest <sup>1</sup>	Guests	GuestUsersCmd ResourceGroup	GuestUsersViews

Tabela 23. Diretivas Baseadas em Função por Função, Grupo de Acesso, Grupo de Recursos e Exibição (continuação)

Função	Grupo de Acesso Utilizado em Diretivas Baseadas em Função	Grupo de Recursos Utilizado em Diretivas Baseadas em Função para Comandos do Controlador	Grupo de Ação Utilizado em Diretivas Baseadas em Função para Exibições
Representante de Atendimento ao Cliente	CustomerServiceRepresentatives	CustomerServiceRepCmdResourceGroup	CustomerServiceRepresentativeViews
Gerente de Marketing	MarketingManagers	MarketingManagerCmdResourceGroup	MarketingManagersViews
Supervisor de Atendimento ao Cliente	CustomerServiceSupervisors	CustomerServiceSupervisorCmdResourceGroup	CustomerServiceSupervisorViews
Representante de Conta	AccountRepresentatives	AccountRepresentativesCmdResourceGroup	AccountRepresentativesViews
Gerente de Vendas	SalesManagers	SalesManagersCmdResourceGroup	SalesManagersViews
Gerente de Produtos	ProductManagers	ProductManagersCmdResourceGroup	ProductManagersViews
Administrador da Vendedora	SellerAdministrators	SellerAdministratorsCommandsResourceGroup	SellerAdministratorsViews
Vendedor	Vendedores	SellersCmdResourceGroup	SellersViews
Gerente de Categorias	CategoryManagers	CategoryManagersCmdResourceGroup	CategoryManagersViews
Comprador (Lado da Compra)	Buyers(buy-side)	Buyers(buy-side)CommandsResourceGroup	Buyers(buy-side)Views
Comprador (lado da venda)	Buyers(sell-side)	Buyers(sell-side)CommandsResourceGroup	Buyers(sell-side)Views
Coletor	PickPackers	PickPackersCmdResourceGroup	PickPackersViews
Receptor	Receptores	ReceiversCmdResourceGroup	ReceiversViews
Administrador de Devoluções	ReturnsAdministrators	ReturnsAdministratorsCmdResourceGroup	ReturnsAdministratorsExibições
Gerente de Operações	OperationsManagers	OperationsManagersCmdResourceGroup	OperationsManagersViews
Gerente de Logística	LogisticsManagers	LogisticsManagersCmdResourceGroup	LogisticsManagersViews
Comprador de Aquisições	ProcurementBuyers	ProcurementBuyersCmdResourceGroup	n/a
Usuário Aprovado Registrado <sup>2</sup>	RegisteredApprovedusuários	RegisteredApprovedUsersCommandsResourceGroup	RegisteredApprovedUsersViews
Usuário Não Rejeitado <sup>3</sup>	NonRejectedUsers	NonRejectedUserCommandsResourceGroup	NonRejectedUsersViews
Gerenciador de Canais	ChannelManagers	ChannelManagersCmdResourceGroup	ChannelManagersViews

Tabela 23. Diretivas Baseadas em Função por Função, Grupo de Acesso, Grupo de Recursos e Exibição (continuação)

Função	Grupo de Acesso Utilizado em Diretivas Baseadas em Função	Grupo de Recursos Utilizado em Diretivas Baseadas em Função para Comandos do Controlador	Grupo de Ação Utilizado em Diretivas Baseadas em Função para Exibições
Todos os Usuários <sup>4</sup>	AllUsers	ResellerUserCmd ResourceGroup <sup>5</sup>	ResellerUserViews <sup>5</sup>
		AllSiteUserCmd ResourceGroup <sup>6</sup>	AllSiteUsersViews <sup>6</sup>
Cliente Registrado (com o qualificador de função OrgandAncestorOrgs)	Registered CustomersForOrg	RegisteredUserCmd ResourceGroup	RegisteredUserViews
		RegisteredResellerUser CmdResourceGroup	RegisteredReseller UserViews

**Notas:**

1. “Guest” não é uma função real. Os usuários que possuem um status de registro definido como “G” (a coluna USER.REGISTERTYPE está definida como “G”) pertencem implicitamente ao grupo de acesso Guests.
2. “Usuário Aprovado Registrado” não é uma função real. Os usuários que possuem um status de registro definido como “R” (a coluna USER.REGISTERTYPE está definida como “R”) e cujo status é aprovado (a coluna MEMBER.STATE está definida como 1) pertencem implicitamente ao grupo de acesso RegisteredApprovedUsers.
3. “Usuário Não Rejeitado” não é uma função real. Os usuários cujo status de registro é não rejeitado (a coluna MEMBER.STATE não está definida como 2) pertencem implicitamente ao grupo de acesso NonRejectedUsers.
4. “Todos os Usuários” não é uma função real. Todos os usuários no sistema pertencem implicitamente ao grupo de acesso AllUsers.
5. Estes grupos de ação e de recursos pertencem as diretivas que fazem parte do B2CPolicyGroup. Este grupo de diretivas provavelmente se aplica apenas a organizações que seguem o modelo de negócios B2C.
6. Estes grupos de ação e de recursos pertencem as diretivas que fazem parte do ManagementAndAdministrationPolicyGroup. Este grupo de diretivas provavelmente se aplica a todas as organizações.

## Diretivas em Nível do Recurso por Área de Negócios

### Pedidos

**Recursos de Dados: Pedido:**

- AllUsersExecuteAllUsersActionGroupCommandsOnOrderResource
- AllUsersExecuteOrderCreateCommandsOnStoreResource
- AllUsersExecuteOrderReadCommandsOnOrderResource
- AllUsersExecuteOrderPrepareCommandsOnOrderResource
- AllUsersExecuteOrderWriteCommandsOnOrderResource
- AllUsersExecuteScheduledOrderCancelOnOrderResource
- AllUsersExecuteReturnAgainstOrderOnOrderResource
- AllUsersExecuteOrderProcessOnOrderResource
- OrderManagersForOrgExecuteOrderManageCommandsOnOrderResource
- CustomerOrderManagersForOrgExecuteOrderProcessOnOrderResource
- ResellerAdministratorsForOrgExecuteOrderReadCommandsOnOrderDataResourceGroup
- ResellerAdministratorsForOrgExecuteOrderPrepareCommandsOnOrderDataResourceGroup
- ResellerAdministratorsForOrgExecuteOrderWriteCommandsOnOrderDataResourceGroup
- ResellerAdministratorsForOrgExecuteScheduledOrderCancelOnOrderDataResourceGroup

- ResellerAdministratorsForOrgExecuteOrderProcessOnOrderDataResourceGroup
- EmailOrderNotificationManagersForOrgExecuteCustomerServiceEmailOrderOnOrderResource

**Recursos de Dados: Lista de Requisitos:**

- AllUsersExecuteRequisitionListCreateCommandsOnStoreEntityResource
- AllUsersExecuteRequisitionListSharedReadCommandsOnSharedRequisitionListResource
- AllUsersExecuteRequisitionListExclusiveReadCommandsOnPrivateRequisitionListResource
- AllUsersExecuteRequisitionListWriteCommandsOnRequisitionListResource
- AllUsersExecuteRequisitionListSharedProcessCommandsOnSharedRequisitionListResource
- AllUsersExecuteRequisitionListExclusiveProcessCommandsOnPrivateRequisitionListResource

**Recursos de Dados: Item de Interesse:**

- AllUsersExecuteInterestItemReadCommandsOnInterestItemListResource
- AllUsersExecuteInterestItemWriteCommandsOnInterestItemListResource

**Recursos de Dados: RMA:**

- AllUsersExecuteRMACreateCommandsOnStoreResource
- AllUsersExecuteRMAReadCommandsOnRMAResource
- AllUsersExecuteRMAPrepareOnRMAResource
- AllUsersExecuteRMAWriteCommandsOnRMAResource
- AllUsersExecuteRMAProcessCommandsOnRMAResource
- RMAApproversForOrgExecuteRMAApproveCommandsOnRMAResource
- RMADisposersForOrgExecuteRMADisposeCommandsOnRMAResource
- RMAReceiversForOrgExecuteRMAReceiveCommandsOnRMAResource
- RMAManagersForOrgExecuteRMAManageCommandsOnRMAResource
- StoreAdministratorsForOrgExecuteRMACreditCommandsOnStoreEntityResource

**Beans de Dados: Pedido:**

- AllUsersDisplayOrderDatabeanResourceGroup
- AllUsersDisplayApprovalsOrderDataBeansResourceGroup
- AccountRepresentativesForOrgDisplayOrderDatabeanOnlyResourceGroup

**Beans de Dados: Lista de Requisitos:**

AllUsersDisplaySharedRequisitionListDataBeansIfSameOrganizationalEntityAsCreator

**Beans de Dados: Item de Interesse:** AllUsersDisplayInterestItemDatabeanResourceGroup

**Beans de Dados: RMA:** AllUsersDisplayRMADatabeanResourceGroup

**Comércio (Contratos)**

**Recursos de Dados: Contrato:**

- ContractCreatorsForOrgExecuteContractCreateCommandsOnMemberResource
- ContractManagersForOrgExecuteContractManageCommandsOnContractResource
- ContractOperatorsForOrgExecuteContractDeployCommandsOnContractResource
- ContractViewersExecuteContractDisplayCommandsOnContractResource
- ContractOperatorsForOrgExecuteContractSubmitCommandsOnContractResource
- ContractManagersForOrgExecuteContractAccountManageCommandsOnAccountResource

## Recursos de Dados: Diretivas de Negócios:

- BusinessPolicyAdministratorsForOrgExecuteBusinessPolicyCreateCommandsOnStoreResource
- BusinessPolicyAdministratorsForOrgExecuteBusinessPolicyManageCommandsOnBusinessPolicyResource

## Recursos de Dados: Criação da Loja:

StoreCreatorsForOrgExecuteStoreCreationCommandsOnOrganizationResource

**Beans de Dados:** AccountHandlersForOrgDisplayTradingDatabeanResourceGroup

## Aprovações

### Recursos de Dados:

- AllUsersExecuteApproveCommandsOnApprovalResource
- FlowAdministratorExecutesFlowAdminCreateCommandsOnStoreEntityResource
- FlowAdministratorExecutesFlowadminDeleteCommandsOnFlowadminResource

**Beans de Dados:** FlowAdministratorsForOrgDisplayFlowadminDatabean

## Leilões

### Recursos de Dados:

- AuctionAdministratorsForOrgExecuteAuctionCreateCommandsOnStoreEntityResource
- AuctionAdministratorsForOrgExecuteAuctionManageCommandsOnAuctionResource
- AuctionManagersForOrgExecuteAdminRetractBidCommandsOnAuctionResource
- AuctionAdministratorsForOrgExecuteAuctionStyleCreateCommandsOnStoreEntityResource
- AuctionAdministratorsForOrgExecuteAuctionStyleManageCommandsOnAuctionStyleResource
- AuctionAdministratorsForOrgExecuteBidControlRuleCreateCommandsOnStoreEntityResource
- AuctionAdministratorsForOrgExecuteBidControlRuleManageCommandsOnBidControlRuleResource
- RegisteredApprovedUsersExecuteBidCreateCommandsOnAuctionResource
- RegisteredApprovedUsersExecuteBidManageCommandsOnBidResources
- RegisteredApprovedUsersExecuteAutoBidCreateCommandsOnAuctionResource
- RegisteredApprovedUsersExecuteAutoBidManageCommandsOnAutoBidResources

**Beans de Dados:** AuctionDatabeanOwnersDisplayAuctionDatabeans

## Inteligência de Negócios

### Recursos de Dados:

- BusinessAnalystsForOrgExecuteViewContextListCommandsOnStoreEntityResource
- IntelligenceReportViewersForOrgExecuteViewBusinessIntelligenceReportCommandsOnStoreEntityResource

## Associação

### Recursos de Dados: Usuário:

- MembershipAdministratorsForOrgExecuteUserAdminUpdateCommandsOnUserResource
- GuestsExecuteUserSelfRegistrationCommandsOnOrganizationResource
- NonRejectedUsersExecuteUserSelfRegistrationContinuationCommandsOnUserResource
- NonRejectedUsersExecuteNonRejectedUserCommands
- AllUsersDisplayUserDatabeanResourceGroup
- NonRejectedDisplayUserDatabeanResourceGroup

**Recursos de Dados: Organização:**

- OrgAdminConsoleMembershipAdministratorsForOrgExecuteOrgEntityPolicySubscriptionUpdateCommandsOnOrganizationResource
- OrgAdminConsoleMembershipAdministratorsForOrgExecuteOrganizationManageActionsOnOrganizationResource
- CSAMembershipAdministratorsForOrgExecuteUserAdminRegistrationCommandsOnOrganizationResource
- CSAMembershipAdministratorsExecuteUserAdminRegistrationCommands OnOrganizationResource
- MembershipAdministratorsForOrgExecuteOrgEntityRegistrationCommands OnOrganizationResource
- MembershipAdministratorsForOrgExecuteOrgEntityUpdateCommandsOnOrganizationResource
- GuestsExecuteResellerSelfRegistrationCommandsOnOrganizationResource
- NonRejectedUsersExecuteResellerSelfRegistrationContinuationCommandsOnOrganizationResource
- ChannelManagersExecuteOrgEntityLockCommandsOnOrgResource
- OrgAdminConsoleMembershipAdministratorsForOrgExecuteApproveGroupUpdateCommandsOnOrganizationResource

**Recursos de Dados: Grupo de Membros:**

- OrgAdminConsoleMembershipAdministratorsForOrgExecuteMemberGroupMemberUpdateCommandsOnUserResource
- OrgAdminConsoleMembershipAdministratorsForOrgExecuteMemberGroupMemberUpdateCommandsOnMemberGroupResource
- MemberGroupAdministratorsForOrgExecuteMemberGroupCreateCommandsOnMemberResource
- MemberGroupManagersForOrgExecuteMemberGroupManageCommandsOnMemberGroupResource

**Recursos de Dados: Endereço:**

- NonRejectedUsersExecuteAddressManageCommandsOnUserResource
- MembershipAdministratorsForOrgExecuteAddressManageCommandsOnMemberResource

**Recursos de Dados: Função:**

- MembershipAdministratorsForOrgExecuteRoleUnassignCommandsOnUserResource
- OrganizationRoleAdministratorsExecuteRoleManageCommandsOnOrganizationResource
- MembershipAdministratorsForOrgExecuteUserRoleAssignCommandsOnOrganizationResource

**Recursos de Dados: Atributo dos Membros:**

- OrgAdminConsoleMembershipAdministratorsForOrgExecuteMemberAttributeCommandsOnOrgResource
- AllUsersExecuteMemberAttributeCommandsOnUserResource

**Beans de Dados:**

- MembershipViewersForOrgDisplayMembershipDatabeanResourceGroup
- MembershipAdministratorsForOrgDisplayOrganizationDatabeanResourceGroup
- MembershipAdministratorsForOrgDisplayUserDatabeanResourceGroup
- EmployeesDisplayOrganizationSpecificDatabeanResourceGroup

**Marketing****Recursos de Dados: Campanhas:**

- CampaignManagersForOrgExecuteCampaignRelatedCreateCommandsOnStoreEntityResource
- CampaignManagersForOrgExecuteCampaignUpdateCommandsOnCampaignResource
- CampaignManagersForOrgExecuteInitiativeUpdateCommandsOnInitiativeResource



- CampaignManagersForOrgExecuteEMarketingSpotUpdateCommandsOnEMarketingSpotResource
- CampaignManagersForOrgExecuteCollateralUpdateCommandsOnCollateralResource

#### **Recursos de Dados: Atividades de E-mail:**

- EmailActivityEditorsForOrgExecuteEmailActivitySaveCommandsOnEmailActivity DataResourceGroup
- EmailActivityEditorsForOrgExecuteEmailActivitySaveCommandsOnStoreEntity DataResourceGroup
- EmailActivityEditorsForOrgExecuteEmailActivityDeleteCommandsOnEmailActivity DataResourceGroup
- EmailActivityConfigurationEditorsForOrgExecuteEmailActivityConfigurationSaveCommands OnEmailActivityDataResourceGroup
- EmailActivityConfigurationEditorsForOrgExecuteEmailActivitySaveCommandsOnStoreEntity DataResourceGroupAllUsersExecuteEmailOptOutDataResourceGroup

**Beans de Dados: Campanhas:** CampaignManagersForOrgDisplayCampaignDataBeanResourceGroup

#### **Beans de Dados: Atividades de E-mail:**

- EmailUserReceiveDataBeanPolicy
- EmailActivityDataBeanPolicy
- EmailConfigurationDataBeanPolicy

**Beans de Dados: E-promotions:** EpromotionDisplayDataBeanPolicy

## **Catálogo**

#### **Recursos de Dados:**

- CatalogManagersForOrgExecuteStoreCategoryManageCommandsOnCatalogResource
- CatalogManagersForOrgExecuteCatalogManageCommandsOnCatalogResource
- CatalogGroupManagersForOrgExecuteCatalogGroupManageCommandsOnCatalogGroupResource
- CatalogEntryManagersForOrgExecuteStoreCatalogEntryManageCommandsOnStoreEntityResource
- CatalogGroupManagersForOrgExecuteProductSetAddCommandsOnCatalogResource
- CatalogGroupManagersForOrgExecuteProductSetManageCommandsOnProductSetResource
- CatalogEntryManagersForOrgExecuteCatalogEntryManageCommandsOnCatalogEntryResource
- CatalogEntryManagersForOrgExecuteCatalogEntryRelationManageCommandsOnCatalogResource
- CatalogEntryManagersForOrgExecuteCatalogStoreManageCommandsOnStoreEntityResource

#### **Beans de Dados:**

- ProductAdministratorsForOrgDisplayProductDataBeansResourceGroup
- CatalogGroupViewersForOrgDisplayCatalogGroupDataBeansResourceGroup
- CatalogListViewersForOrgDisplayCatalogListDataBeansResourceGroup

## **Conectividade e Notificação**

#### **Recursos de Dados:**

- BackendOrderAdministratorsForOrgExecuteBackendOrderStatusCreateCommandsOnOrderDataResource
- BackendPickPackersForOrgExecuteBackendPickPackListCommandsOnFulfillmentCenterDataResource
- MessagingUpdateAdministratorsForOrgExecuteMessagingUpdateCommandsOnStoreEntityResource

## Aquisição

### Recursos de Dados:

- ProcurementAdministratorsForOrgExecuteProcurementAuthenticationAndRegistration OnOrganizationResource
- ProcurementShoppingCartManagersExecuteProcurementShoppingCartManageOnOrderResource

## Cupons

### Recursos de Dados:

- CouponAdministratorsForOrgExecuteCouponPromotionCreateCommandsOnStoreEntityResource
- CouponAdministratorsForOrgExecuteCouponPromotionDeleteCommandsOnCouponPromotionResource
- AllUsersExecuteCouponRedemptionCommandsOnCouponWalletResource
- AllUsersExecuteCouponDeleteCommandsOnCouponWalletResource
- CouponAdministratorsForOrgExecuteCouponPromotionUpdateCommandsOnStoreEntityResource
- AllUsersExecuteCouponSaveCommandsOnCouponWalletResource

**Beans de Dados:** CouponAdministratorsForOrgDisplayECouponPromotionBeans

## Perfil de Cliente

### Recursos de Dados:

CustomerProfileEditorsForOrgExecuteSegmentManageCommandsOnStoreEntityResource

**Beans de Dados:** CustomerProfileEditorsForOrgDisplaySegmentationDatabeansResourceGroup

## Descontos

### Recursos de Dados:

- DiscountAdministratorsForOrgExecuteDiscountCreateCommandsOnStoreEntityResource
- DiscountAdministratorsForOrgExecuteDiscountDeployCommandsOnCalculationCodeResource
- DiscountAdministratorsForOrgExecuteDiscountAssociateCommandsOnCalculationCodeResource

**Beans de Dados:** DiscountViewersForOrgDisplayDiscountDatabeans

## Gerenciamento de Estoque

### Recursos de Dados:

- FulfillmentCenterManagersForOrgExecuteFulfillmentCenterCreateCommandsOn OrganizationResource
- FulfillmentCenterManagersForOrgExecuteFulfillmentCenterManageCommandsOn FulfillmentCenterResource
- PickBatchInventoryManagersForOrgExecuteReleaseReadyShipCommandsOn FulfillmentCenterResource
- VendorInventoryManagersForOrgExecuteVendorManageCommandsOnVendorResource
- VendorInventoryManagersForOrgExecuteVendorCreateCommandsOnStoreEntityResource
- ExpectedInventoryManagersForOrgExecuteInventoryManageCommandsOnStoreEntityResource
- PickPackGeneratorsForOrgExecutePickPackGenerateCommandsOnFulfillmentCenterResource
- InventoryAdjustersForOrgExecuteInventoryAdjustCommandsOnStoreEntityResource
- ReturnReasonsManagersForOrgExecuteReturnReasonsCommandsOnStoreEntityResource
- FulfillmentCenterManagersForOrgExecuteFulfillmentCenterReleaseOnFulfillmentCenter ReleaseDataResourceGroup
- SharedFulfillmentCenterPickBatchInventoryManagersExecuteReleaseReadyShipCommands OnFulfillmentCenterDataResource

- SharedFulfillmentCenterPickPackGeneratorsExecutePickPackGenerateCommandsOnFulfillmentCenterResource
- SharedFulfillmentCenterManagersExecuteFulfillmentCenterReleaseCommandsOnFulfillmentCenterReleaseDataResourceGroup

#### **Beans de Dados:**

- ReturnReasonsManagersForOrgDisplayReturnReasonsOrderManagementDataBeansResourceGroup
- ExpectedInventoryManagersForOrgDisplayExpectedInventoryDataBeansResourceGroup
- VendorInventoryManagersForOrgDisplayVendorInventoryDataBeansResourceGroup
- ProductFindInventoryManagersForOrgDisplayProductFindInventoryDataBeansResourceGroup
- FulfillmentCenterManagersForOrgDisplayFulfillmentCenterDataBeansResourceGroup
- PickBatchInventoryManagersForOrgDisplayPickBatchInventoryDataBeansResourceGroup
- ReceiverOrderManagersForOrgDisplayReceiverOrderManagementDataBeansResourceGroup
- ReturnsAdminOrderManagersForOrgDisplayReturnsAdminOrderManagementDataBeansResourceGroup
- SuperUserOrderManagersForOrgDisplaySuperUserOrderManagementDataBeansResourceGroupFulfillmentManagersForOrgDisplayReleaseOrderItemsDatabeanResourceGroup

## **Gerenciamento de Pedidos**

#### **Recursos de Dados:**

- CustomerOrderManagersForOrgExecuteCustomerServiceOrderWriteCommands OnOrderResource
- CustomerOrderManagersForOrgExecuteCustomerServiceOrderCreateCommands OnStoreEntityResource
- CustomerOrderManagersForOrgExecuteCustomerServiceReturnWriteCommands OnRMAResource
- CustomerOrderManagersForOrgExecuteCustomerServiceReturnCreateCommands OnStoreEntityResource
- CustomerOrderManagersExecuteCustomerWriteCommandsOnUserResource
- CustomerOrderManagersForDefaultOrgExecuteCustomerServiceCustomerWriteCommandsOnUserDataResourceGroupwithGuestRegisterType

#### **Beans de Dados:**

- CustomerOrderManagersForOrgDisplayCustomerOrderManagementDatabeans
- MemberOrderManagersForDefaultOrgDisplayGuestMemberDatabeans
- MemberOrderManagersDisplayOrganizationSpecificDatabeans
- MemberOrderManagersDisplayUserDatabeanResourceGroup
- UserOrderManagersForDefaultOrgDisplayGuestMemberDatabeans
- UserOrderManagersDisplayOrganizationSpecificDatabeans
- UserOrderManagersDisplayUserDatabeanResourceGroup
- LogisticsManagersForOrgDisplayOrdersAndReturnsListsDatabeans
- ReturnsManagersForOrgDisplayReturnsListsDatabeans

## **Pagamentos**

#### **Recursos de Dados:**

- AccountManagersForOrgExecuteAccountCreateCommandsOnOrganizationResource
- AccountAdministratorsForOrgExecuteAccountManageCommandsOnAccountResource
- AccountViewersForOrgExecutePaymentSummaryGenerateCommandsOnAccountResource
- AccountViewersForOrgExecuteStorePaymentAdminCommandsOnStoreEntityResource

- AllUsersExecutePaymentOrderWriteCommandsOnOrderResource

## Editor de Diretivas

### Recursos de Dados:

- StoreAdministratorsForOrgExecuteACPolicyCreateCommandsOnOrganizationResource
- StoreAdministratorsForOrgExecuteACPolicyEditCommandsOnACPolicyResource
- StoreAdministratorsForOrgExecuteACViewPoliciesForUpdateActionsOnOrganizationResource
- StoreAdministratorsForOrgExecuteACViewApplicablePoliciesActionsOnOrganizationResource
- DescendantStoreAdministratorsExecuteACViewPoliciesForOrgActionsOnOrganizationResource

**Beans de Dados:** StoreAdministratorsForOrgExecuteUserGroupSearchViews

## Consultor de Produto

### Beans de Dados:

- ProductAdvisorStatisticiansForOrgDisplayProductAdvisorStatisticsDatabeans
- SalesAssistantStatisticiansForOrgDisplaySalesAssistantStatisticsDatabeans
- ProductAdvisorManagersDisplayPAWCBEDatabeanResourceGroup
- GuidedSellManagersDisplayGSWCBEDatabeanResourceGroup

## RFQ

### Recursos de Dados:

- RFQBuyersExecuteRFQCreateCommandsOnStoreEntityDataResourceGroup
- RFQBuyersManageRFQResourcesTheyOwn
- RFQBuyersManageRFQResponsesForRFQsTheyOwn
- RFQAdministratorsAdministerRFQs
- RFQAdministratorsManageRFQResponses
- RFQSalesManagersForOrgCreateRFQResponse
- RFQSalesManagersExecuteRFQResponseManageCommandsOnRFQResponseResource
- RFQSalesManagersExecuteRFQResponseAdminCommandsOnRFQWithPublicAccessTypeResourceGroup
- RFQSalesManagersExecuteRFQResponseAdminCommandsOnRFQResourceGroup

### Beans de Dados:

- RFQBuyersDisplayRFQDataBeanResourceGroupTheyOwn
- RFQBuyersDisplayRFQResponseDataBeansViewabletoRFQOwnerResourceGroup
- RFQSalesViewersDisplayRFQResponseDataBeanResourceGroup
- RFQSalesViewersDisplayRFQDataBeanWithPublicAccessTypeResourceGroup
- RFQSalesViewersDisplayRFQDataBeanResourceGroup

## Regras

### Recursos de Dados:

StoreAdministratorsForOrgExecutePersonalizationRuleServiceAdministrationCommandsOnStoreEntityResource

### Beans de Dados:

StoreAdministratorsForOrgDisplayPersonalizationRuleServiceAdministrationDataBeanResourceGroup

## Planejador

### Recursos de Dados:

- StoreAdministratorsForOrgExecuteScheduledJobManageCommandsOnStoreEntityResource
- StoreAdministratorsForOrgExecuteScheduledJobManageCommandsOnUserResource

**Beans de Dados:** StoreAdministratorsForOrgDisplaySchedulerDataBeansResourceGroup

## Commerce Accelerator

### Recursos de Dados:

- B2CCSAViewUsersForOrgExecuteB2CCSAViewActionsOnStoreEntityResource
- B2BCSAViewUsersForOrgExecuteB2BCSAViewActionsOnStoreEntityResource
- CHSCSAViewUsersForOrgExecuteCHSCSAViewActionsOnStoreEntityResource
- RHSCSAViewUsersForOrgExecuteRHSCSAViewActionsOnStoreEntityResource
- CPSCSAViewUsersForOrgExecuteCPSCSAViewActionsOnStoreEntityResource
- RPSCSAViewUsersForOrgExecuteRPSCSAViewActionsOnStoreEntityResource
- HCPCSAViewUsersForOrgExecuteHCPCSAViewActionsOnStoreEntityResource
- MHSCSAViewUsersForOrgExecuteMHSCSAViewActionsOnStoreEntityResource
- MPSCSAViewUsersForOrgExecuteMPSCSAViewActionsOnStoreEntityResource
- SCPCSAViewUsersForOrgExecuteSCPCSAViewActionsOnStoreEntityResource
- SHSCSAViewUsersForOrgExecuteSHSCSAViewActionsOnStoreEntityResource
- SPSCSAViewUsersForOrgExecuteSPSCSAViewActionsOnStoreEntityResource

## Envio

### Recursos de Dados:

ShippingMembershipAdministratorsForOrgExecuteShippingManageCommandsOnStoreDataResourceGroup

**Beans de Dados:** ShippingMembershipAdministratorsForOrgDisplayShippingDataBeanResourceGroup

## Taxação

### Recursos de Dados:

TaxationAdministratorsForOrgExecuteTaxationManageCommandsOnStoreDataResourceGroup

**Beans de Dados:** TaxationAdministratorsForOrgDisplayTaxationDataBeanResourceGroup

## Ajuda Ativa/Espaços de Trabalho Colaborativos/Atendimento ao Cliente

### Recursos de Dados: Ajuda Ativa:

- LiveHelpAgentsForOrgExecuteLiveHelpRetrieveCommandsOnUserDataResources
- LiveHelpAgentsForOrgExecuteLiveHelpRetrieveCommandsOnOrderDataResources

### Recursos de Dados: Atendimento ao Cliente:

CustomerCareAdministratorsForOrgExecuteCustomerCareQueueManageCommandsOnStoreResource

**Beans de Dados: Ajuda Ativa:** LiveHelpAgentsForOrgDisplayCustomerCareDataBeanResourceGroup

### Beans de Dados: Espaços de Trabalho Colaborativos:

CollaborativeWorkspaceAdministratorsForOrgDisplayCollaborativeWorkspaceDataBeanResourceGroup

## Estado da Loja

### Recursos de Dados:

- ChannelManagersExecuteStoreStateChangeCommandsOnStoreResource
- AdministrativeRolesForOrgExecuteStoreStateChangeCommandsOnStoreResource
- AdministratorsForOrgAccessStoreWithCloseOrSuspendStateResourceGroup
- AllUsersAccessStoreWithOpenStateResourceGroup

## Gerenciamento da Loja

### Recursos de Dados: Entrega de Relatório:

ReportDeliveryManagersForOrgExecuteSetupReportDeliveryCommandsOnStoreDataResourceGroup

### Recurso de Dados: Loja:

- StoreFrontManagersForOrgExecuteStoreFrontRelatedUpdateOnStoreEntityResource
- StoreProfileManagersForOrgExecuteStoreProfileRelatedUpdateOnStoreEntityResource

---

## Grupos de Diretivas de Controle de Acesso Padrão

Os grupos de diretivas de controle de acesso padrão que são fornecidos com o WebSphere Commerce são os seguintes:

- Grupo de Diretivas de Gerenciamento e de Administração: Este grupo de diretivas contém todas as diretivas de gerenciamento de membros e de administração de loja.
- Grupo de Diretivas de Gerenciamento de Compradores Guest: Este grupo de diretivas contém todas as diretivas que estão relacionadas ao gerenciamento de compradores guest.
- Grupo de Diretivas de Compras Comuns: Este grupo de diretivas contém todas as diretivas relacionadas a compras que são comuns ao consumidor direto e aos cenários de B2B.
- Grupo de Diretivas B2C: Este grupo de diretivas contém todas as diretivas de compras específicas do consumidor direto.
- Grupo de Diretivas B2B: Este grupo de diretivas contém todas as diretivas de compras específicas de B2B.

**Nota:** O Grupo de Diretivas de Gerenciamento e de Administração é o principal grupo de diretivas que geralmente deve ser aplicado a todas as organizações. Sempre que uma organização se torna assinante de qualquer grupo de diretivas, este grupo de diretivas também deve se tornar assinante. Para uma organização que possui uma loja, dependendo do tipo de loja, além do Grupo de Diretivas de Gerenciamento e de Administração, ela também deve ser assinante do Grupo de Diretivas de Compras Comuns, do Grupo de Diretivas B2C e do Grupo de Diretivas B2B. O Grupo de Diretivas de Gerenciamento de Compradores Guest apenas deve se tornar assinante da organização que possui compradores guest, que é a Organização Padrão em um cenário comum.

---

## Avisos

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

É possível que a IBM não ofereça os produtos, serviços ou recursos discutidos nesta publicação em outros países. Consulte um representante IBM local para obter informações sobre produtos e serviços disponíveis atualmente em sua área. Qualquer referência a produtos, programas ou serviços IBM não significa que apenas os produtos, programas ou serviços IBM possam ser utilizados. Qualquer produto, programa ou serviço funcionalmente equivalente, que não infrinja nenhum direito de propriedade intelectual da IBM ou outros direitos legalmente protegidos, poderá ser utilizado em substituição a este produto, programa ou serviço. Entretanto, a avaliação e verificação da operação de qualquer produto, programa ou serviço não-IBM são de responsabilidade do Cliente.

Qualquer referência a um programa licenciado IBM não significa que apenas o programa licenciado da IBM possa ser utilizado. Qualquer produto, programa ou serviço funcionalmente equivalente, que não infrinja nenhum direito de propriedade intelectual da IBM poderá ser utilizado em substituição a este produto, programa ou serviço. A avaliação e verificação da operação em conjunto com outros produtos, exceto aqueles expressamente designados pela IBM, são de inteira responsabilidade do Cliente.

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

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

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

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

O parágrafo a seguir não se aplica a nenhum país em que tais disposições não estejam de acordo com a legislação local:

A INTERNATIONAL BUSINESS MACHINES CORPORATION FORNECE ESTA PUBLICAÇÃO "NO ESTADO EM QUE SE ENCONTRA", SEM GARANTIA DE NENHUM TIPO, SEJA EXPRESSA OU IMPLÍCITA, INCLUINDO, MAS NÃO SE LIMITANDO ÀS GARANTIAS IMPLÍCITAS DE NÃO-VIOLAÇÃO, MERCADO OU ADEQUAÇÃO A UM DETERMINADO PROPÓSITO. Alguns países não

permitem a exclusão de garantias expressas ou implícitas em certas transações; portanto, esta disposição pode não se aplicar ao Cliente.

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

Referências nestas informações a Web sites não-IBM são fornecidas apenas por conveniência e não representam de forma alguma um endosso a estes Web sites. Os materiais contidos nestes Web sites não fazem parte dos materiais deste produto IBM e a utilização destes Web sites é de inteira responsabilidade do Cliente.

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

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

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

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

O programa licenciado descrito neste documento e todo o material licenciado disponível são fornecidos pela IBM sob os termos do Contrato com o Cliente IBM, do Contrato de Licença do Programa Internacional IBM ou de qualquer outro contrato equivalente.

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

As informações relativas a produtos não-IBM foram obtidas junto aos fornecedores dos respectivos produtos, de seus anúncios publicados ou de outras fontes disponíveis publicamente. A IBM não testou estes produtos e não pode confirmar a precisão de seu desempenho, compatibilidade nem qualquer outra reivindicação relacionada a produtos não-IBM. Dúvidas sobre os recursos de produtos não-IBM devem ser encaminhadas diretamente a seus fornecedores.

Todas as declarações relacionadas aos objetivos e intenções futuras da IBM estão sujeitas a alterações ou cancelamento sem aviso prévio e representam apenas metas e objetivos.



Estas informações contêm exemplos de dados e relatórios utilizados nas operações diárias de negócios. Para ilustrá-los da forma mais completa possível, os exemplos podem incluir nomes de indivíduos, empresas, marcas e produtos. Todos estes nomes são fictícios e qualquer semelhança com nomes e endereços utilizados por uma empresa real é mera coincidência.

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

---

## Licença de Copyright

Estas informações contêm programas de aplicativos de exemplo na linguagem fonte, ilustrando as técnicas de programação em diversas plataformas operacionais. Você pode copiar, modificar e distribuir estes programas de exemplo sem a necessidade de pagar a 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 a qual os programas de exemplo são criadas. Estes exemplos não foram testados completamente em todas as condições. Portanto, a IBM, não pode garantir ou implicar a confiabilidade, manutenção ou função destes programas. Você 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 interfaces de programação de aplicativos da IBM.

---

## Marcas Comerciais

O logotipo IBM e os termos a seguir são marcas comerciais da International Business Machines Corporation nos Estados Unidos e/ou em outros países:

AIX	AS/400	DB2
@server	IBM	iSeries
OS/2	OS/400	SecureWay
WebSphere	400	

Domino é uma marca comercial da Lotus Development Corporation nos Estados Unidos e/ou em outros países.

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

Java, JavaBeans e todas as marcas comerciais baseadas em Java são marcas comerciais ou marcas registradas da Sun Microsystems, Inc. nos Estados Unidos e em outros países.

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







Impresso em Brazil