

IBM Intelligent Operations Center  
Versão 1.0

*Centro de Informações do IBM  
Intelligent Operations Center*

**IBM**

## **Junho de 2011**

Esta edição se aplica ao IBM Intelligent Operations Center versão 1, release 0, modificação 0. Esta edição se aplica a todos os releases e modificações subsequentes, até indicado o contrário em novas edições.

Um formulário para comentário dos leitores encontra-se disponível no verso desta publicação. Se o formulário tiver sido removido, envie seus comentários para:

IBM Brasil - Centro de Traduções

Rodovia SP 101 km 09

CEP 13185-900

Hortolândia, SP

Brasil

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

© Copyright IBM Corporation 2011.

# Índice

## Capítulo 1. Visão Geral da Solução . . . 1

Público-Alvo . . . . .	2
Recursos. . . . .	2
Usuários e Benefícios . . . . .	3
Componentes . . . . .	4
Gerenciamento de Ocorrências . . . . .	6

## Capítulo 2. Instalando e Configurando. . 9

Preparando para Instalação . . . . .	9
Configuração do Sistema . . . . .	9
Requisitos de Hardware . . . . .	13
Requisitos de Software . . . . .	14
Pacotes de Mídia . . . . .	14
Instalando a Solução . . . . .	15
Preparando os Servidores. . . . .	16
Copiando Arquivos Necessários para Instalar e Implementar a Solução . . . . .	16
Extraindo Arquivos de Instalação e Instalando Dependências. . . . .	16
Implementando a Solução . . . . .	17
Implementando o Pacote a partir de uma Linha de Comandos. . . . .	19
Executando Tarefas de Implementação Específicas . . . . .	20
Instalando o Tivoli Service Request Manager . . . . .	20
Instalando Ferramentas Fornecidas com a Solução. . . . .	21
Configuração Pós-Instalação . . . . .	22
Configurando o Valor de Tempo Limite da Sessão do WebSphere Portal . . . . .	22
Configurando o Valor de Tempo Limite das Configurações de Cache da Sessão do Tivoli Access Manager WebSEAL . . . . .	23
Configurando a Conexão Única. . . . .	23
Criando uma Junção do WebSphere Application Server Network Deployment . . . . .	28
Configurando o WebSphere Application Server Network Deployment para Conexão Única LTPA. . . . .	30
Ativando Redirecionamento de Login . . . . .	30
Configurando a Porta e o Protocolo do Gateway de Serviços REST . . . . .	31
Excluindo Usuários de Amostra . . . . .	31
Verificando a Publicação de Ocorrências CAP . . . . .	32

## Capítulo 3. Protegendo a Solução . . . 33

Funções e Responsabilidades do Usuário . . . . .	34
Incluindo um Usuário ou Grupo . . . . .	36
Visualizando ou Modificando a Associação ao Grupo . . . . .	38
Visualizando ou Editando um Perfil de Usuário . . . . .	39
Excluindo um Usuário ou Grupo . . . . .	40
Grupos de Funções de Usuários e Permissões de Autorização . . . . .	40
Grupos de Categorias de Usuários e Permissões de Acesso a Dados . . . . .	41
Resumo das permissões do usuário . . . . .	42

Gerenciando um ACL de Junção do WebSphere Application Server Network Deployment . . . . .	43
Gerenciando um ACL da Junção do WebSphere Application Server Network Deployment Usando a Linha de Comandos . . . . .	43
Gerenciando um ACL da Junção do WebSphere Application Server Network Deployment Usando o Tivoli Access Manager WebSEAL Web Portal Manager . . . . .	44

## Capítulo 4. Integrando a Solução . . . 45

Exemplos de sistemas que podem ser integrados . . . . .	45
Pontos de integração e protocolos . . . . .	45
Eventos e KPIs . . . . .	45
Integrando ao Common Alerting Protocol . . . . .	48
Integrando a outros Protocolos . . . . .	55
Publicando Mensagens CAP. . . . .	56
Usando a Fila de Ocorrências de Entrada Definida para o IBM Intelligent Operations Center . . . . .	56
Publicador de Amostras . . . . .	56
Customizando KPIs . . . . .	60
Monitorar Modelos e KPIs . . . . .	61
Instâncias do Contexto de Monitoramento . . . . .	62
Modelando KPIs. . . . .	63
KPIs aninhados . . . . .	66
Definindo Relacionamentos Pai/Filho de KPI . . . . .	67
Comunicação de Ocorrência de KPI entre o IBM Business Monitor e o IBM Intelligent Operations Center . . . . .	67
Implementando Modelos de Monitor . . . . .	71
Valores de Exibição de KPI . . . . .	71
Armazenamento em Cache de KPIs . . . . .	73
KPIs de Amostra . . . . .	73

## Capítulo 5. Customizando a Solução 77

Customizando a Interface com o Usuário . . . . .	77
Localizando a Interface com o Usuário . . . . .	77
Lista de Portlets . . . . .	77
Customizando o Layout da Página . . . . .	79
Configurando o Mapa . . . . .	80
Especificando Dados de Configuração para Todo o Sistema. . . . .	81
Atualizando a Tabela SYSPROP. . . . .	84
Criando KPIs para Uso com o IBM Intelligent Operations Center . . . . .	84
Configurando o IBM Intelligent Operations Center para Receber Ocorrências. . . . .	85

## Capítulo 6. Gerenciando a Solução . . 87

Controlando os Servidores . . . . .	87
Iniciando os Servidores . . . . .	87
Iniciando a Análise do Tivoli Netcool/OMNIBus . . . . .	88
Parando os Servidores. . . . .	88
Consultando o Status dos Servidores . . . . .	89

Obtendo Ajuda para o Comando IOCControl . . . . .	89
Manutenção da Solução . . . . .	90
Ajustando o Desempenho . . . . .	90
Dicas de Manutenção . . . . .	90

**Capítulo 7. Usando a Interface da Solução . . . . . 93**

Efetuando Logon . . . . .	93
Efetuando Logoff . . . . .	93
Visualizando ou Editando o Perfil do Usuário . . . . .	94
Visualização Executivo . . . . .	95
Status . . . . .	96
Drill Down de Key Performance Indicator . . . . .	97
Coordenador - Alertas . . . . .	98
Contatos do Sametime . . . . .	100
Visualização Operações . . . . .	100
Mapa . . . . .	101
Usando os Controles de Mapa . . . . .	102
Incluindo um Evento . . . . .	103
Configurando o Mapa . . . . .	105
Ocorrências . . . . .	105

Gerenciando Eventos Existentes . . . . .	107
Incluindo um Evento . . . . .	107
Coordenador - Alertas . . . . .	108
Contatos do Sametime . . . . .	110

**Capítulo 8. Resolução de Problemas e Suporte . . . . . 111**

Resolvendo um Problema . . . . .	111
Procurando Bases de Conhecimento . . . . .	113
Entrando em Contato com o Suporte IBM . . . . .	114
Trocando Informações com a IBM . . . . .	115
Enviando Informações ao Suporte IBM . . . . .	115
Recebendo Informações do Suporte IBM . . . . .	115
Assinando Atualizações de Suporte . . . . .	116
Dicas de Resolução de Problemas . . . . .	117

**Capítulo 9. Referências . . . . . 119**

Biblioteca em PDF . . . . .	119
Informações Adicionais . . . . .	119
Aviso de Copyright e Marcas Registradas . . . . .	120

---

## Capítulo 1. Visão Geral da Solução

Muitas organizações e empreendimentos requerem supervisão e coordenação operacionais eficientes. Todos têm em comum a necessidade de reunir determinadas informações para que as pessoas certas possam tomar decisões precisas e rápidas, além de rastrear o efeito dessas decisões. O IBM® Intelligent Operations Center é uma solução de software projetada para facilitar a supervisão e coordenação efetivas das operações.

As autoridades se deparam com desafios comuns em seus sistemas principais e na execução de melhorias nos sistemas que estão interconectados. Autoridades prospectivas desejam aplicar as melhorias na eficiência e eficácia de sistemas principais mais inteligentes. Elas adotam novas maneiras de pensar e usar esses sistemas. O aplicativo de tecnologia da informação avançada pode ajudar as autoridades a melhor entenderem, preverem e responderem de forma inteligente aos padrões de comportamento e ocorrências.

Por exemplo, a IBM define uma cidade inteligente em termos de melhorias na qualidade de vida e bem-estar econômico que são alcançados por meio da aplicação de tecnologias de informações (TI) para planejar, projetar, construir e operar a infraestrutura da cidade. Uma cidade inteligente não possui necessariamente "a tecnologia mais recente." Trata-se de encontrar formas de usar a tecnologia para fazer o uso mais efetivo dos recursos existentes para melhorar a vida dos cidadãos da cidade.

O IBM Intelligent Operations Center usa o poder dos dados do mundo real gerados pelos sistemas de computador:

- Coletando e gerenciando os dados corretos
- Integrando e analisando esses dados
- Facilitando o acesso adequado às informações
- Ajustando sistemas para atingir resultados com base nos insights obtidos

Os benefícios dessa solução são para:

- Otimizar operações planejadas e não planejadas usando uma abordagem holística de relatório e monitoramento
- Construir a convergência de domínios em uma organização facilitando a comunicação e a colaboração
- Melhorar a qualidade do serviço e reduzir despesas coordenando ocorrências

Uma operação pode ser dividida em domínios individuais, que geralmente correspondem à estrutura de organização e ao conhecimento das pessoas envolvidas. Em uma cidade, o conhecimento é mantido em departamentos, por exemplo, em transportes, água e segurança pública.

Conforme a complexidade das operações em um domínio aumenta, uma solução mais customizada é requerida. O IBM Intelligent Operations Center tem uma série de pontos de integração diferentes em que a customização pode ocorrer. Esses pontos de integração e a infraestrutura incluída fornecem aos Parceiros de Negócios IBM, provedores de serviços e clientes a flexibilidade para construir uma solução ampla e poderosa.

---

## Público-Alvo

Este centro de informações destina-se a pessoas que estejam usando, instalando, administrando e executando a manutenção do IBM Intelligent Operations Center. Também contém documentação de implementação para customizar a solução e integrar os sistemas subjacentes externos que o IBM Intelligent Operations Center requer.

Esse centro de informações supõe que os usuários tenham conhecimento prévio ou proficiência no uso dos produtos componentes incluídos nesta solução. O treinamento para esses produtos do componente está fora do escopo deste centro de informações. Se o treinamento para esses produtos for necessário, pergunte ao integrador de sistemas ou ao representante IBM onde é possível obter informações sobre oportunidades de treinamento do componente base.

É possível localizar links para a documentação do produto do componente na seção “Informações Adicionais” na página 119.

---

## Recursos

O IBM Intelligent Operations Center fornece medição, monitoramento e modelagem de recursos que integram sistemas subjacentes em uma solução para melhorar a eficiência operacional, o planejamento e a coordenação.

O IBM Intelligent Operations Center é uma solução da família de produtos do IBM Smarter Cities Software Solutions. O IBM Intelligent Operations Center pode ser instalado em hardware (ou local) existente ou pode ser implementado na nuvem. O IBM Intelligent Operations Center pode ser instalado sozinho ou é possível instalá-lo com outras soluções da família de produtos IBM Smarter Cities Software Solutions.

O IBM Intelligent Operations Center é uma solução baseada em GUI com acesso baseado em função a eventos para uma organização e os domínios subjacentes. Ele possui gerenciamento de eventos, mapeamento integrado e recursos de colaboração. Ele também possui o recurso de regras de negócios e o relatório do indicador de desempenho chave (KPI) para uma maior eficácia. Essa funcionalidade fornece autoridades com a capacidade de integrar domínios para cooperação e tomada de decisão melhoradas.

### Gerenciamento de Eventos e de Incidentes

O IBM Intelligent Operations Center fornece um mecanismo de rastreamento e de relatório de ocorrências para permitir a identificação e compreensão de domínios subjacentes. É possível gerenciar ocorrências previstas, planejadas e atuais conforme se desenvolvem. Por exemplo, a substituição de canos que passam sob uma estrada é uma ocorrência planejada ou ordem de serviço envolvendo água e tráfego. Mau tempo chegando nas próximas 24 horas é uma ocorrência prevista. Um engarrafamento é uma ocorrência atual afetada pelas obras da estrada e pelo tempo.

Um sistema de informações geográficas (GIS) mapeia ocorrências visualmente, permitindo medir o impacto das ocorrências por meio de análise interativa de mapeamento e cenário.

## Relatório e monitoramento de status

O IBM Intelligent Operations Center fornece uma ferramenta para criar e exibir KPIs. Os KPIs podem ser atualizados como mudanças de dados subjacentes. É possível usar esta ferramenta para:

- Resumir o status de nível executivo para um único domínio ou entre domínios
- Destacar problemas e identificar problemas
- Investigar melhor, executando drill down dos detalhes do KPI

## Notificação Instantânea e Sistema de Mensagens

O IBM Intelligent Operations Center fornece uma área de trabalho em que é possível manter alertas para questões que necessitem de atenção. É possível usar essa área de trabalho para monitorar notícias e ocorrências, principalmente quando outros portlets que anunciam notícias não estão em visualização.

O IBM Lotus Sametime fornece uma ferramenta integrada de colaboração e comunicação que pode ser usada para mensagens instantâneas onde e quando necessário.

---

## Usuários e Benefícios

O IBM Intelligent Operations Center foi projetado para equipes envolvidas com o controle operacional em organizações, departamentos governamentais ou autoridades locais: executivos, supervisores e operadores.

A tabela a seguir descreve os usuários e benefícios associados ao uso do IBM Intelligent Operations Center.

*Tabela 1. Usuários e Benefícios do IBM Intelligent Operations Center*

Se você é um...	Este software pode ajudá-lo a...
Executivo	<ul style="list-style-type: none"><li>• Receber resumos de nível executivo dos eventos e incidentes através de mapas, painéis e alertas</li><li>• Determinar as medidas do sucesso organizacional com Key Performance Indicators (KPIs)</li><li>• Identificar e controlar problemas por meio de relatórios</li><li>• Direcionar prioridades e implementação de políticas usando os dados fornecidos</li></ul>
Supervisor	<ul style="list-style-type: none"><li>• Identificar e executar ações em conflitos e problemas mostrados em mapas, painéis e alertas</li><li>• Gerenciar ocorrências por meio da inclusão de novos eventos, edição de eventos existentes, cancelamento de eventos e escalação de eventos para incidentes</li><li>• Monitorar KPIs configurados</li><li>• Comunicar-se fácil e rapidamente a respeito de assuntos importantes</li></ul>

Tabela 1. Usuários e Benefícios do IBM Intelligent Operations Center (continuação)

Se você é um...	Este software pode ajudá-lo a...
Operador	<ul style="list-style-type: none"><li>• Monitorar status, criar e editar eventos e incidentes a serem mostrados em listas</li><li>• Notificar determinados gerentes ou executivos e emitir alertas</li><li>• Comunicar-se fácil e rapidamente em caso de emergências e outras situações que requerem respostas</li></ul>
Administrador de Usuários	<ul style="list-style-type: none"><li>• Incluir novos usuários e designá-los a grupos</li><li>• Garantir a segurança por meio de grupos de autorização baseados em função com as permissões apropriadas</li><li>• Configurar permissões adequadas à área de conhecimento e aos dados necessários</li></ul>

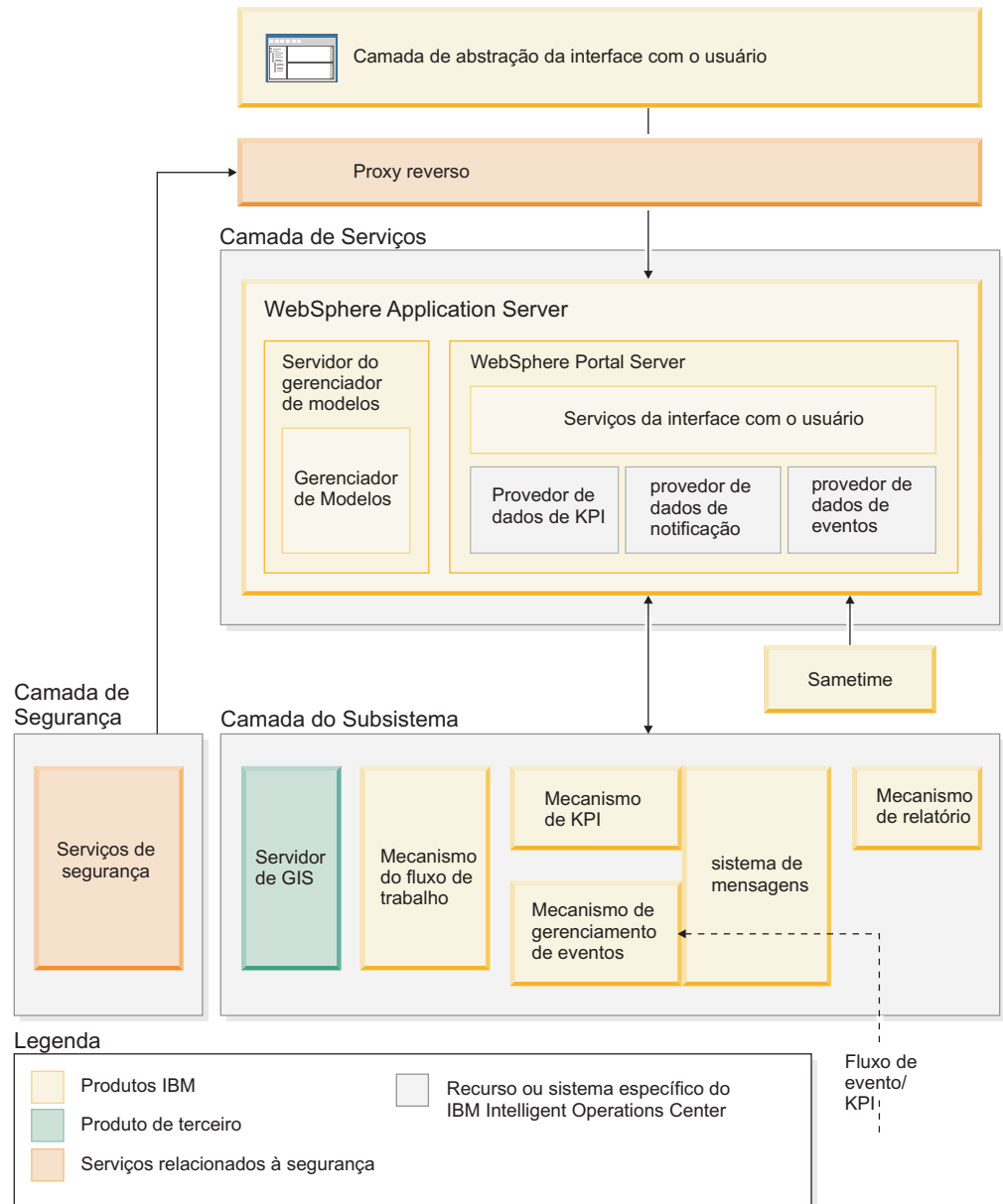
---

## Componentes

Em um alto nível, a estrutura do IBM Intelligent Operations Center pode ser dividida em componentes e subsistemas principais.

O diagrama a seguir mostra uma visualização de alto nível dos principais componentes do IBM Intelligent Operations Center.





## Camada de Abstração da Interface com o Usuário

O IBM Intelligent Operations Center fornece portais de parada única baseados na Web para informações de ocorrências, status geral e detalhes. A interface com o usuário (UI) apresenta informações customizadas em várias visualizações pré-configuradas em formatos comuns. Todas as informações são exibidas por meio de painéis de fácil utilização.

## Camada de Segurança

Todo o acesso a informações é controlado pela camada de segurança por meio de funções organizacionais e categorias de dados. Esse controle impede acesso desautorizado enquanto ativa o fácil gerenciamento de autorizações.

## Camada de Serviços

A camada de serviços usa widgets comuns e uma estrutura de serviços da interface com o usuário comum para receber dados de ocorrências e passá-los por gerenciamento de ocorrências para o sistema de mensagens. Os provedores de dados do IBM Intelligent Operations Center estendem os serviços da interface com o usuário. Devido à ampla variedade de dados provenientes de sistemas operacionais subjacentes, os dados são normalizados de acordo com um modelo de referência semântica padrão, o qual fornece um dicionário comum para mapear relacionamentos. Esse modelo facilita a análise do efeito e a resposta para os eventos sem a necessidade de diversas conversões de informações. O gerenciador do modelo fornece acesso ao KPI e às informações de hierarquia de domínios subjacentes. A análise avançada pode ser executada nos dados, identificando otimizações e previsões que podem ajudar a orientar na tomada de decisões e no controle.

## Camada do Subsistema

A solução fornece uma camada de mediação para facilitar a troca de informações entre a solução e os sistemas operacionais dos domínios subjacentes. Os dados das várias origens configuráveis podem ser fornecidos por gateways para uma camada do subsistema, que pode gerar alertas, KPIs e eventos. Essa camada de integração ativa a comunicação bidirecional de mensagens em vários formatos, usando padrões abertos quando possível. Usando as ferramentas padrão de mercado para executar a transformação de origens para o modelo semântico de referência, os sistemas operacionais subjacentes não precisam ser alterados. O sistema emergencial e outros sistemas de resposta podem ser conectados ao IBM Intelligent Operations Center para os fluxos de trabalho adequados.

A estrutura do IBM Intelligent Operations Center suporta o seguinte:

- Um ponto central para compreender do estado das operações, gerenciar ocorrências e incidentes e conectar-se a domínios sob controle do centro de operações
- Integração com um sistema de informações geográficas (GIS) para mapear ocorrências e incidentes espacial e visualmente
- Criação e exibição de indicadores chaves de desempenho (KPIs), que são atualizados como mudanças de dados por meio de conexões com sistemas de domínios subjacentes
- Alertas entrando do campo, incluindo aqueles que requerem respostas emergenciais ou padrão
- Recursos de colaboração, por meio do sistema de mensagens instantâneas com IBM Lotus Sametime
- Um modelo de segurança baseado em função

---

## Gerenciamento de Ocorrências

A solução IBM Intelligent Operations Center foca a integração e otimização de informações dentro e entre diversos domínios em um hub central de operações, em tempo real e por longos períodos. O gerenciamento de ocorrências ativa um centro de operações para assimilar dados de diversos sistemas para prever e reagir constantemente a ocorrências e tendências significativas.

Ocorrências são itens de dados autocontidos que contêm informações básicas, mas completas às quais os destinatários podem responder. Ocorrências são colocadas em filas pelo IBM Intelligent Operations Center e são processadas pelo mecanismo de gerenciamento de ocorrências.

Ocorrências entram no IBM Intelligent Operations Center em diferentes formas baseadas na natureza do centro de operações. Alguns exemplos das formas de ocorrências são acionadores, limites, ocorrências complexas e ocorrências geradas manualmente.

Acionadores são ocorrências geradas por algo que está ocorrendo e geralmente requerem que uma ação seja executada pelo destinatário. São exemplos de acionadores:

- Acionamento de alarmes de incêndio ou fumaça
- Indisponibilidade de sistemas de tecnologia da informação
- Acionamento de alarmes de intrusão
- Ocorrências naturais captadas por sensores, como tremores de terra

O IBM Intelligent Operations Center pode receber informações sobre essas ocorrências de sistemas externos e convertê-las em alertas para destinatários. Em geral, é provável que indicadores de nível inferior seriam resumidos e somente passados ao IBM Intelligent Operations Center se precisassem de mais atenção. Por exemplo, todos os incêndios podem não ser relatados como ocorrências. No entanto, um incêndio que envolva diversas divisões do serviço de bombeiro e conhecimento da proteção ambiental, devido a material perigoso, precisaria ser relatado ao centro de operações.

Ocorrências limites ajudam a determinar quando as medidas obtidas de um sensor ou de outra fonte estão fora da faixa normal. Ocorrências de limite básicas são comparações entre duas ou mais medidas e relatam uma tendência. Ocorrências de limite mais sofisticadas podem comparar duas medidas com um limite criado por informações de histórico. São exemplos de ocorrências de limite:

- Alarmes de temperatura acima ou abaixo de um determinado valor
- Níveis de água altos ou baixos
- Qualidade da água e do ar fora de padrões ambientais
- Consumo excessivo de energia

O IBM Intelligent Operations Center pode gerenciar essas ocorrências na forma de indicadores chaves de desempenho (KPIs).

Ocorrências complexas reúnem informações a partir de diversos sistemas para determinar se um grupo de ocorrências relacionadas deve ser relatado. Por exemplo, a autoridade de pedágios rodoviários recebe uma ocorrência acionadora de seu sistema de monitoramento, indicando que a conexão com o sistema de autorização de cartão de crédito não está disponível, seguida por uma ocorrência de limite do sistema financeiro avisando que estão próximos do limite crédito para pagamentos não autorizados. A combinação desses dois problemas é muito mais grave do que os problemas individuais; sendo assim, uma ocorrência complexa é gerada como aviso e para a coordenação de uma solução.

Ocorrências que são inseridas manualmente são especialmente importantes para as cidades. Algumas dessas ocorrências são incidentes observados, como crimes e acidentes de trânsito. Outros exemplo de ocorrências inseridas manualmente são aquelas geradas a partir de chamadas emergenciais de cidadãos, de relatórios feitos

por oficiais das cidades ou de sistemas de gerenciamento que relatam sobre o status das cidades. Os tipos mais comuns de ocorrências inseridas manualmente são:

- Avisos de Mau Tempo
- Relatórios Criminais
- Incêndios
- Incidentes de tráfego rodoviário - acidentes, congestionamento, cargas incomuns
- Próximos eventos - shows de rock, corridas, desfiles

Processamento de ocorrências complexas permite que uma cidade identifique exceções nos sistemas da cidade facilmente, ocasionalmente para identificar tendências de dados não relacionados e para prever problemas futuros.

---

## Capítulo 2. Instalando e Configurando

O IBM Intelligent Operations Center fornece um assistente de implementação que instala o ambiente requerido pelo IBM Intelligent Operations Center. Após implementar o ambiente e o pacote do IBM Intelligent Operations Center, será necessário realizar algumas configurações adicionais.

---

### Preparando para Instalação

Antes de implementar o IBM Intelligent Operations Center, compreenda a configuração do sistema do IBM Intelligent Operations Center e assegure que os pré-requisitos sejam atendidos para o ambiente.

### Configuração do Sistema

O assistente de implementação do IBM Intelligent Operations Center instala e configura um ambiente com seis servidores de produção e um servidor usado durante o processo de instalação.

#### Servidor de gerenciamento de instalação

O servidor de gerenciamento de instalação é usado pelo instalador do IBM Intelligent Operations Center. Ele não é usado no ambiente de produção. O servidor de gerenciamento de instalação contém os scripts de instalação e configuração usado para implementar os outros servidores IBM Intelligent Operations Center.

#### Servidor de acesso

O servidor de acesso oferece segurança para a solução IBM Intelligent Operations Center. Quando o IBM Intelligent Operations Center é instalado, o servidor de acesso contém os produtos, componentes ou feature packs mostrados na Tabela 2.

*Tabela 2. Conteúdo do Servidor de acesso*

Produto, recurso ou feature pack	Portas padrão definidas durante a instalação
Tivoli Access Manager WebSEAL 6.1	Serviço HTTP: porta 80

#### Servidor de integração e aplicativo

O servidor de integração e aplicativo fornece serviços de aplicativo para a solução IBM Intelligent Operations Center. Quando o IBM Intelligent Operations Center é instalado, o servidor de integração e aplicativo contém os produtos, componentes ou feature packs mostrados na Tabela 3 na página 10.

Tabela 3. Conteúdo do Servidor de integração e aplicativo

Produto, recurso ou feature pack	Portas padrão definidas durante a instalação
Componentes IBM Model Server do IBM Integrated Information Core 1.4.0.1	Console administrativo do WebSphere Application Server: porta 9063 Servidor da Web: porta 9082
WebSphere Message Broker 7.0.0.1	Nenhuma
WebSphere MQ 7.0.1.3	MQ Listener: porta 1414
WebSphere Application Server Network Deployment 7.0.0.13	Console administrativo do WebSphere Application Server: porta 9060 Servidor HTTP: porta 9080
DB2 Enterprise Server Edition 9.7.0.2	Porta 50000
Web 2.0 Feature Pack for WebSphere Application Server 1.0.1	Nenhuma

## Servidor de portal

O servidor de portal oferece serviços de interface com o usuário para a solução IBM Intelligent Operations Center. Quando o IBM Intelligent Operations Center é instalado, o servidor de portal contém os produtos, componentes ou feature packs mostrados na Tabela 4

Tabela 4. Conteúdo do Servidor de portal

Produto, recurso ou feature pack	Portas padrão definidas durante a instalação
IBM HTTP Server 7.0.0.13	Serviço HTTP: porta 8080 Administrativo: porta 8008
WebSphere Portal Enable 7.0	Console administrativo: porta 10032 Servidor de portal: porta 10039
Lotus Sametime Entry 8.5.1	Serviço SMTP: porta 25 Serviço HTTP: porta 81 Serviço LDAP: porta 389 Serviço NRPC: porta 1352 Serviço de sistema de mensagens: porta 1533
Lotus Domino 8.5.1	Serviço SMTP: porta 25 Serviço HTTP: porta 81 Serviço LDAP: porta 389 Serviço NRPC: porta 1352 Serviço de sistema de mensagens: porta 1533

Tabela 4. Conteúdo do Servidor de portal (continuação)

Produto, recurso ou feature pack	Portas padrão definidas durante a instalação
IBM ILOG JViews Enterprise 8.7	Nenhuma
DB2 Enterprise Server Edition 9.7.0.2	Porta 50000

## Servidor analítico

O servidor analítico fornece serviços de análise de dados para a solução IBM Intelligent Operations Center. Quando o IBM Intelligent Operations Center é instalado, o servidor analítico contém os produtos, componentes ou feature packs mostrados na Tabela 5

Tabela 5. Conteúdo do Servidor analítico

Produto, recurso ou feature pack	Portas padrão definidas durante a instalação
IBM Cognos Business Intelligence 10.1	Console administrativo do WebSphere Application Server: porta 9061  HTTP para WebSphere Application Server: portas 9081, 9082, 9083
IBM ILOG CPLEX Optimization Studio 12.2	Nenhuma
IBM Business Monitor 7.0.0.3	Console administrativo do WebSphere Application Server: porta 9060  Servidor HTTP: porta 9080
WebSphere Application Server Network Deployment 7.0.0.13	Console administrativo do WebSphere Application Server: porta 9060  Servidor HTTP: porta 9080
DB2 Enterprise Server Edition 9.7.0.2	Porta 50000

## Servidor de gerenciamento e evento

O servidor de gerenciamento e evento gerencia ocorrências manipuladas pela solução IBM Intelligent Operations Center. Quando o IBM Intelligent Operations Center é instalado, o servidor de gerenciamento e evento contém os produtos, componentes ou feature packs mostrados na Tabela 6

Tabela 6. Conteúdo do Servidor de gerenciamento e evento

Produto, recurso ou feature pack	Portas padrão definidas durante a instalação
Tivoli Directory Server 6.2.0.1	Instância dsrdbm01: porta 389  Instância itimldap: porta 10389
Tivoli Directory Integrator 7.1	Porta 52562

Tabela 6. Conteúdo do Servidor de gerenciamento e evento (continuação)

Produto, recurso ou feature pack	Portas padrão definidas durante a instalação
Tivoli Access Manager 6.1	Servidor de política: porta 7135 Servidor de autorização: porta 7136
Tivoli Identity Manager 5.1.0.0	Console administrativo do WebSphere Application Server: porta 9061 Servidor HTTP: porta 9081
IBM Tivoli Monitoring 6.2.2.1	TEMS: porta 1918 TEPS: porta 1920
Tivoli Composite Application Manager 6.2.4	Nenhuma
Tivoli Netcool/Impact 5.1.1	Linha de comandos: porta 2000 BD de memória: porta 5435
Tivoli Netcool/OMNibus 7.3.0	Servidor de objeto: porta 4100 Agente de processo: porta 4200
WebSphere Application Server Network Deployment 7.0.0.13	Console administrativo do WebSphere Application Server: porta 9060 Servidor HTTP: porta 9080
WebSphere Application Server 6.0.0.23 (somente para uso do Tivoli Identity Manager )	Console administrativo do WebSphere Application Server: porta 9061 Servidor HTTP: porta 9081
DB2 Enterprise Server Edition 9.7.0.2	Instância db2inst1: porta 50000 Instância db2inst2: porta 50002

## Servidor de banco de dados

O servidor de banco de dados fornece serviços de repositório e modelagem para a solução IBM Intelligent Operations Center. Quando o IBM Intelligent Operations Center é instalado, o servidor de banco de dados contém os produtos, componentes ou feature packs mostrados na Tabela 7

Tabela 7. Conteúdo do Servidor de acesso

Produto, recurso ou feature pack	Portas padrão definidas durante a instalação
DB2 Enterprise Server Edition 9.7.0.2	Porta 50000



### Tarefas relacionadas

“Instalando a Solução” na página 15

A instalação do IBM Intelligent Operations Center envolve várias etapas. Um assistente de implementação é fornecido para implementar e instalar o ambiente necessário e o pacote do IBM Intelligent Operations Center.

## Requisitos de Hardware

Cada servidor e cliente IBM Intelligent Operations Center deve atender aos requisitos de hardware recomendados.

### Requisitos de Servidor

Cada servidor deve ter um processador x86 de 64 bits, incluindo um dos seguintes:

- Processadores AMD de 64 bits
- Processadores Intel Extended Memory 64 Technology (EM64T)

Cada IBM Intelligent Operations Center exige os valores de processador, memória e espaço em disco mostrados na Tabela 8.

*Tabela 8. Requisitos de Servidor do IBM Intelligent Operations Center*

Servidor	Número de processadores	Memória	Disco rígido
Servidor de acesso	4	16 GB	80 GB
Servidor analítico	8	16 GB	80 GB
Servidor de integração e aplicativo	8	16 GB	80 GB
Servidor de banco de dados	8	16 GB	80 GB
Servidor de gerenciamento e evento	8	16 GB	80 GB
Servidor de portal	8	16 GB	80 GB
Servidor de gerenciamento de instalação	2	8 GB	80 GB

### Observações:

- A pasta /tmp no servidor de gerenciamento de instalação deve ter pelo menos 35 GB de espaço disponível.
- Defina o espaço de troca para cada servidor como o dobro da memória física. Por exemplo, se um servidor possui 16 GB de memória, defina 32 GB de espaço de troca.

Pode ser necessário usar um hardware adicional caso planeje utilizar o Tivoli Service Request Manager com o IBM Intelligent Operations Center.

### Requisitos de Cliente

Cada cliente que acessa o IBM Intelligent Operations Center deve atender aos seguintes requisitos de hardware:

- Monitor com resolução mínima de 1280 x 800
- 2 GB de memória
- Acesso a rede com largura de banda suficiente para geração de um cliente Web complexo e atualização contínua de dados.

### **Conceitos relacionados**

“Instalando o Tivoli Service Request Manager” na página 20  
O Tivoli Service Request Manager pode ser usado opcionalmente com o IBM Intelligent Operations Center para gerenciar incidentes.

### **Tarefas relacionadas**

“Instalando a Solução” na página 15  
A instalação do IBM Intelligent Operations Center envolve várias etapas. Um assistente de implementação é fornecido para implementar e instalar o ambiente necessário e o pacote do IBM Intelligent Operations Center.

## **Requisitos de Software**

Cada cliente e servidor do IBM Intelligent Operations Center devem atender a requisitos mínimos de software.

**Importante:** Antes de instalar o IBM Intelligent Operations Center, os servidores do IBM Intelligent Operations Center devem estar com os seguintes itens instalados. Nenhum outro produto de software deve ser instalado nos servidores.

- Red Hat Enterprise Linux 5 Atualização 5 de 64 bits, com o serviço Secure Shell (SSH) instalado e aberto.

Além disso, um sistema Windows com Lotus Notes Client 8.5.1 é necessário para configurar a conexão única para uso do IBM Lotus Sametime com o IBM Intelligent Operations Center. O cliente Lotus Notes Client 8.5.1 está incluso no pacote do IBM Intelligent Operations Center. Instale o Lotus Notes Client utilizando as informações no centro de informações do Lotus Domino e do Lotus Notes.

Os clientes que acessarem o IBM Intelligent Operations Center deverão ter um dos seguintes navegadores:

- Internet Explorer 8.x (32 bits e 64 bits)
- Mozilla Firefox 3.0, 3.5 ou 3.6

Produtos de software adicionais podem ser necessários se desejar usar o Tivoli Service Request Manager com o IBM Intelligent Operations Center.

### **Conceitos relacionados**

“Instalando o Tivoli Service Request Manager” na página 20  
O Tivoli Service Request Manager pode ser usado opcionalmente com o IBM Intelligent Operations Center para gerenciar incidentes.

### **Tarefas relacionadas**

“Instalando a Solução” na página 15  
A instalação do IBM Intelligent Operations Center envolve várias etapas. Um assistente de implementação é fornecido para implementar e instalar o ambiente necessário e o pacote do IBM Intelligent Operations Center.

### **Informações relacionadas**

 Centro de Informações do Lotus Domino e Lotus Notes

## **Pacotes de Mídia**

O IBM Intelligent Operations Center pode ser encomendado como um pacote de DVDs ou pode ser obtido junto ao Passport Advantage.

O número do produto é 5725-D69.

### Tarefas relacionadas

“Instalando a Solução”

A instalação do IBM Intelligent Operations Center envolve várias etapas. Um assistente de implementação é fornecido para implementar e instalar o ambiente necessário e o pacote do IBM Intelligent Operations Center.

### Informações relacionadas

 Passport Advantage

---

## Instalando a Solução

A instalação do IBM Intelligent Operations Center envolve várias etapas. Um assistente de implementação é fornecido para implementar e instalar o ambiente necessário e o pacote do IBM Intelligent Operations Center.

### Antes de Iniciar

O IBM Intelligent Operations Center requer sete servidores. Esses servidores podem ser servidores de hardware físico, máquinas virtuais executando VMware ou servidores na nuvem. Seis desses servidores são usados no ambiente de produção; o sétimo é usado apenas no processo de instalação.

Antes de instalar o IBM Intelligent Operations Center, certifique-se que os servidores atendam ao requisitos de hardware e software.

Determine o ID de usuário e senha do administrador para cada servidor. Esses IDs do usuário e senhas devem ser especificados no assistente de implementação.

A implementação do IBM Intelligent Operations Center define vários IDs do usuário e senhas durante o processo de implementação. Antes de iniciar, determine quais IDs do usuário e senhas serão definidos. Os IDs de usuário e senha definidos pelo assistente de implementação são:

- O ID de usuário e senha do administrador raiz para o servidor de gerenciamento de instalação.
- O ID do administrador e senha do WebSphere Portal.

### Sobre Esta Tarefa

A instalação do IBM Intelligent Operations Center requer que as etapas importantes a seguir sejam concluídas:

1. Preparar os setes servidores.
2. Copiar as imagens dos produtos fornecidos com a mídia de instalação do IBM Intelligent Operations Center para um local temporário.
3. Copiar os arquivos de instalação do IBM Intelligent Operations Center para um local temporário
4. Executar o assistente de implementação do IBM Intelligent Operations Center para instalar e configurar o middleware requerido pela solução IBM Intelligent Operations Center e implementar o IBM Intelligent Operations Center.

### **Conceitos relacionados**

“Requisitos de Software” na página 14

Cada cliente e servidor do IBM Intelligent Operations Center devem atender a requisitos mínimos de software.

“Requisitos de Hardware” na página 13

Cada servidor e cliente IBM Intelligent Operations Center deve atender aos requisitos de hardware recomendados.

“Pacotes de Mídia” na página 14

O IBM Intelligent Operations Center pode ser encomendado como um pacote de DVDs ou pode ser obtido junto ao Passport Advantage.

“Configuração do Sistema” na página 9

O assistente de implementação do IBM Intelligent Operations Center instala e configura um ambiente com seis servidores de produção e um servidor usado durante o processo de instalação.

## **Preparando os Servidores**

Os servidores em que o IBM Intelligent Operations Center será instalado devem ser preparados antes da instalação do IBM Intelligent Operations Center.

### **Procedimento**

1. Desative firewalls e SELinux. Reinicie o sistema. Firewalls podem ser ativadas após a conclusão da instalação.
2. Certifique que os servidores possam se comunicar entre si. Essa verificação pode ser feita assegurando que o arquivo `hosts` contenha os nomes de todos os outros servidores. Também será possível testar as conexões durante o processo de instalação ou é possível efetuar ping de cada servidor antes de instalar o IBM Intelligent Operations Center.
3. Certifique-se de que os nomes de hosts de servidores estejam registrados em um DNS.

## **Copiando Arquivos Necessários para Instalar e Implementar a Solução**

Os arquivos necessários para instalar e implementar o IBM Intelligent Operations Center precisam ser copiados para os servidores antes de executar o assistente de implementação.

### **Procedimento**

1. Obtenha a mídia do IBM Intelligent Operations Center ou transfira-o por download.
2. Copie os arquivos na mídia do IBM Intelligent Operations Center ou no download do IBM Intelligent Operations Center para o servidor de gerenciamento de instalação. Os arquivos devem ser colocados em um único diretório, por exemplo `/images`.

## **Extraindo Arquivos de Instalação e Instalando Dependências**

Após copiar os arquivos necessários para um local temporário, extraia os arquivos de instalação. Em seguida, instale as dependências antes de implementar o IBM Intelligent Operations Center.

### **Procedimento**

1. No servidor de gerenciamento de instalação, navegue até o diretório onde os arquivos do IBM Intelligent Operations Center foram copiados.

2. Extraia o pacote de instalação do IBM Intelligent Operations Center no diretório onde os arquivos do IBM Intelligent Operations Center foram copiados, executando o seguinte comando:

```
# tar -zxvf ICOC_Installer_XXXXXXXX-XXXX.tar.gz
```

Em que *XXXXXXXX-XXXX* é um número exclusivo que indica o nível da compilação.

**Importante:** Ocorrerão erros durante a instalação caso o pacote seja copiado em um diretório diferente.

3. Obtenha o arquivo `libXp-1.0.0-8.i386.rpm` a partir da Red Hat Network e copie o arquivo no servidor de portal.
4. Instale o arquivo `libXp-1.0.0-8.i386.rpm` no servidor de portal, executando os comandos a seguir.

```
-bash-3.2# rpm -i libXp-1.0.0-8.i386.rpm
-bash-3.2# rpm -qa | grep libXp
libXp-1.0.0-8
```

5. Obtenha os arquivos a seguir a partir da Red Hat Network e copie-os para o servidor analítico.

```
compat-libstdc++-33-3.2.3-61.i386.rpm
kernel-headers-2.6.18-194.el5.i386.rpm
compat-glibc-headers-2.3.4-2.26.i386.rpm
compat-glibc-2.3.4-2.26.i386.rpm
libXmu-1.0.2-5.i386.rpm
libXp-1.0.0-8.i386.rpm
openmotif22-2.2.3-18.i386.rpm
```

6. Instale os arquivos no servidor analítico executando os seguintes comandos.

```
-bash-3.2# rpm -ivh compat-libstdc++-33-3.2.3-61.i386.rpm
-bash-3.2# rpm -ivh kernel-headers-2.6.18-194.el5.i386.rpm
-bash-3.2# rpm -ivh compat-glibc-headers-2.3.4-2.26.i386.rpm
-bash-3.2# rpm -ivh compat-glibc-2.3.4-2.26.i386.rpm
-bash-3.2# rpm -ivh libXmu-1.0.2-5.i386.rpm
-bash-3.2# rpm -ivh libXp-1.0.0-8.i386.rpm
-bash-3.2# rpm -ivh openmotif22-2.2.3-18.i386.rpm
```

#### Informações relacionadas

 Red Hat

## Implementando a Solução

O IBM Intelligent Operations Center oferece um assistente de implementação para instalar os produtos fornecidos com o IBM Intelligent Operations Center. O assistente de implementação também implementa o pacote do IBM Intelligent Operations Center.

### Antes de Iniciar

No servidor de gerenciamento de instalação, navegue até o diretório temporário onde copiou os arquivos de instalação do IBM Intelligent Operations Center. Em seguida, navegue até o diretório `/disk1`. Por exemplo, caso tenha copiado os arquivos para o diretório `/images`, navegue até `images/disk1`.

### Procedimento

1. Execute o comando a seguir:

```
chmod +x -R *
```

2. Inicie o assistente de implementação do IBM Intelligent Operations Center executando o comando a seguir:

```
./LinuxSetup
```

O primeiro painel apresentado introduz o assistente de implementação. Clicar em **Ajuda** em qualquer painel fornece informações gerais sobre o assistente de implementação e não informações específicas sobre a implementação do IBM Intelligent Operations Center.

3. Clique em **Avançar**.
4. Duas tarefas podem ser selecionadas. As **Tarefas da Arquitetura de Base** instalarão os produtos requeridos pelo IBM Intelligent Operations Center. As **Tarefas do Intelligent Operations Center** implementarão o pacote de soluções do IBM Intelligent Operations Center. Para instalar toda a solução do IBM Intelligent Operations Center selecione ambas opções.

**Importante:** O IBM Intelligent Operations Center não é suportado pela IBM como solução até que as **Tarefas da Arquitetura de Base** e as **Tarefas do Intelligent Operations Center** sejam concluídas.

5. Clique em **Avançar**.
6. Se a opção **Tarefas da Arquitetura de Base** foi selecionada, vários painéis serão exibidos com tarefas para instalar os produtos fornecidos pelo IBM Intelligent Operations Center. Se estiver instalando o IBM Intelligent Operations Center pela primeira vez nesses servidores, deixe todas as opções com a seleção padrão. Alguns itens poderão estar desativados. Não será possível selecionar ou desmarcar esses itens. Se um produto já estiver instalado no servidor, você poderá cancelar a seleção da instalação do produto. Clique em **Avançar** até que todos os itens da **Tarefa da Arquitetura de Base** tenham sido revisados e selecionados.
7. Se uma **Tarefa do Intelligent Operations Center** tiver sido selecionada, será apresentada uma opção para implementação do pacote IBM Intelligent Operations Center. Caso for selecionado, o assistente de implementação também irá implementar o pacote do IBM Intelligent Operations Center nos servidores. Selecione se deseja que a **Tarefa do Intelligent Operations Center** seja executada e clique em **Avançar**.
8. Nos painéis seguintes, insira o nome do host ou endereço IP, um ID de usuário de administrador e a senha do ID de cada servidor de destino. O sistema operacional estará desativado pois apenas Linux é suportado pelo IBM Intelligent Operations Center. Para salvar informações para possível uso futuro, selecione **Salvar estas informações de login**. Para testar se as informações fornecidas estão corretas, clique em **Testar Conexões**. Caso ocorra uma falha no teste de conexão, resolva o problema antes de prosseguir. Clique em **Avançar** após inserir os dados para cada servidor.
9. O assistente de implementação definirá dois IDs do usuário e senhas durante o processo de implementação: um ID de administrador e senha para o IBM Intelligent Operations Center e um ID de administrador e senha para o WebSphere Portal. Defina esses IDs de usuário e senhas nos painéis seguintes e clique em **Avançar** até que os IDs tenham sido definidos.
10. Será exibido um Painel de Resumo com todas as tarefas selecionadas e com a duração da execução de cada uma. Se desejar executar todas as tarefas, clique em **Implementar Tudo**. Caso deseje executar apenas determinadas tarefas, clique em **Implementar Tarefa** para cada tarefa que deseja executar. As tarefas selecionadas para implementação serão executadas. Uma mensagem será

exibida, indicando se a implementação foi concluída com sucesso ou se houve algum erro. Caso ocorram erros, corrija-os e execute as tarefas em questão novamente.

11. Caso **Tarefa do Intelligent Operations Center** não tenha sido selecionada, o pacote IBM Intelligent Operations Center poderá ser implementado ao re-executar o assistente de implementação e selecionar **Tarefa do Intelligent Operations Center**. Como alternativa, o pacote do IBM Intelligent Operations Center pode ser instalado a partir de uma linha de comandos.

## Resultados

A solução IBM Intelligent Operations Center é instalada.

### Conceitos relacionados

“Requisitos de Hardware” na página 13

Cada servidor e cliente IBM Intelligent Operations Center deve atender aos requisitos de hardware recomendados.

“Requisitos de Software” na página 14

Cada cliente e servidor do IBM Intelligent Operations Center devem atender a requisitos mínimos de software.

“Pacotes de Mídia” na página 14

O IBM Intelligent Operations Center pode ser encomendado como um pacote de DVDs ou pode ser obtido junto ao Passport Advantage.

“Configuração do Sistema” na página 9

O assistente de implementação do IBM Intelligent Operations Center instala e configura um ambiente com seis servidores de produção e um servidor usado durante o processo de instalação.

### Tarefas relacionadas

“Implementando o Pacote a partir de uma Linha de Comandos”

O pacote da solução IBM Intelligent Operations Center pode ser implementado após a implementação da arquitetura base. Se o assistente de implementação não puder implementar completamente o pacote de soluções do IBM Intelligent Operations Center ou se a opção **Tarefas do Intelligent Operations Center** não tiver sido selecionada no assistente de implementação, o pacote de soluções do IBM Intelligent Operations Center pode ser implementado a partir de uma linha de comandos.

## Implementando o Pacote a partir de uma Linha de Comandos

O pacote da solução IBM Intelligent Operations Center pode ser implementado após a implementação da arquitetura base. Se o assistente de implementação não puder implementar completamente o pacote de soluções do IBM Intelligent Operations Center ou se a opção **Tarefas do Intelligent Operations Center** não tiver sido selecionada no assistente de implementação, o pacote de soluções do IBM Intelligent Operations Center pode ser implementado a partir de uma linha de comandos.

### Procedimento

1. Faça login no servidor de gerenciamento e evento como raiz. Opcionalmente, faça login no servidor de gerenciamento e evento como administrador e utilize o comando **sudo** para executar os comandos necessários caso não consiga efetuar login como raiz.
2. Remova o diretório /opt/IBM/iss.
3. Extraia o arquivo IOC.tar no diretório /opt/IBM. Os arquivos devem residir no diretório /opt/IBM/iss quando extraídos.

4. Navegue até o diretório `/opt/IBM/ISP/ioc/binary`.  
`-bash-3.2# cd /opt/IBM/ISP/ioc/binary/`
5. Execute este comando:  
`-bash-3.2# ./install.sh admin password`  
Em que *admin* e *password* são o ID de usuário do administrador e a senha especificados quando o assistente de implementação do IBM Intelligent Operations Center foi executado.
6. Se um erro for exibido, consulte mais detalhes no arquivo `install.log`. Corrija quaisquer erros. Execute o comando novamente.

## O que Fazer Depois

Efetue login no portal no servidor de portal para verificar se o IBM Intelligent Operations Center foi implementado com sucesso. A página **Intelligent Operations Center** será exibida.

## Executando Tarefas de Implementação Específicas

Tarefas de implementação específicas podem ser executadas para reinstalar partes da solução ou para executar uma tarefa de implementação que possa ter falhado.

Para executar uma ou mais tarefas de implementação, execute o assistente de implementação e selecione as tarefas a serem executadas.

### Tarefas relacionadas

“Implementando a Solução” na página 17

O IBM Intelligent Operations Center oferece um assistente de implementação para instalar os produtos fornecidos com o IBM Intelligent Operations Center. O assistente de implementação também implementa o pacote do IBM Intelligent Operations Center.

## Instalando o Tivoli Service Request Manager

O Tivoli Service Request Manager pode ser usado opcionalmente com o IBM Intelligent Operations Center para gerenciar incidentes.

O Tivoli Service Request Manager é fornecido com o pacote de mídia do IBM Intelligent Operations Center. Ele não é instalado pelo assistente de implementação do IBM Intelligent Operations Center.

**Restrição:** A versão do Tivoli Service Request Manager fornecida com o pacote do IBM Intelligent Operations Center pode ser usada apenas com o IBM Intelligent Operations Center. Ele não pode ser usado de maneira independente ou com qualquer outro aplicativo.

Para obter os requisitos do sistema e instruções de instalação para o Tivoli Service Request Manager, consulte o centro de informações do Tivoli Service Request Manager. O Tivoli Service Request Manager deve ser instalado em um servidor diferente dos servidores do IBM Intelligent Operations Center.



### **Conceitos relacionados**

“Configuração do Sistema” na página 9

O assistente de implementação do IBM Intelligent Operations Center instala e configura um ambiente com seis servidores de produção e um servidor usado durante o processo de instalação.

“Requisitos de Hardware” na página 13

Cada servidor e cliente IBM Intelligent Operations Center deve atender aos requisitos de hardware recomendados.

“Requisitos de Software” na página 14

Cada cliente e servidor do IBM Intelligent Operations Center devem atender a requisitos mínimos de software.

### **Informações relacionadas**

 Centro de Informações do Tivoli Service Request Manager

## **Instalando Ferramentas Fornecidas com a Solução**

Kits de ferramentas e ferramentas de desenvolvimento estão incluídas com o IBM Intelligent Operations Center. Eles são usados na customização do IBM Intelligent Operations Center.

Com a exceção do Rational Application Developer, eles são fornecidos no DVD ou na imagem do IBM Intelligent Operations Center Developer's Toolkit. O Rational Application Developer está incluído com o IBM Intelligent Operations Center em DVDs ou imagens separados.

### **Lotus Sametime Client**

Para obter informações sobre como instalar e usar o Lotus Sametime Client, consulte o centro de informações do Lotus Domino e do Lotus Notes.

### **WebSphere Message Broker Toolkit**

Para obter informações sobre a instalação e uso do WebSphere Message Broker Toolkit, consulte o centro de informações do WebSphere Message Broker.





### **IBM Business Monitor Development Toolkit**

Para obter informações sobre a instalação e uso do IBM Business Monitor Development Toolkit, consulte o centro de informações do IBM Business Monitor.

### **Rational Application Developer**

Para obter informações sobre como instalar e usar o Rational Application Developer, consulte o centro de informações do Rational Application Developer.

### Informações relacionadas

-  Centro de Informações do Lotus Domino e Lotus Notes
-  Centro de Informações do WebSphere Message Broker
-  Centro de Informações do IBM Business Monitor
-  Centro de Informações do Rational Application Developer

---

## Configuração Pós-Instalação

Após implementar o IBM Intelligent Operations Center, etapas adicionais serão necessárias para configurar a solução.

Para que IBM Lotus Sametime possa ser utilizado com o WebSphere Portal, a conexão única também deve ser configurada. A conexão única também deve ser configurada entre o IBM Lotus Sametime e Tivoli Access Manager WebSEAL.

### Configurando o Valor de Tempo Limite da Sessão do WebSphere Portal

O valor de tempo de limite da sessão do WebSphere Portal precisa ser configurado para impedir que um usuário seja desconectado durante uma sessão. Esse valor deve corresponder ao valor de tempo limite das configurações de cache do Tivoli Access Manager WebSEAL.

#### Procedimento

1. Abra um Console administrativo do WebSphere Application Server em `https://server:port/ibm/console`. Substitua *server* e *port* pelos valores padrão ou pelos valores que foram configurados, o que se aplicar. Para obter informações adicionais sobre os números da porta padrão, consulte “Configuração do Sistema” na página 9.
2. Clique em **Servidores > Tipo de Servidor - WebSphere Application Servers > WebSphere Portal > Gerenciamento de Sessões**.
3. Para **Tempo limite da sessão**, selecione **Configurar tempo limite** e insira o valor de tempo limite necessário em minutos. Por exemplo, 540 minutos (9 horas).
4. Clique em **OK**.
5. Salve as alterações na configuração principal.
6. Reinicie o WebSphere Portal executando os comandos a seguir.  

```
/opt/IBM/WebSphere/wp_profile/bin/stopServer.sh WebSphere_Portal  
/opt/IBM/WebSphere/wp_profile/bin/startServer.sh WebSphere_portal
```

### Conceitos relacionados

“Configuração do Sistema” na página 9

O assistente de implementação do IBM Intelligent Operations Center instala e configura um ambiente com seis servidores de produção e um servidor usado durante o processo de instalação.

### Tarefas relacionadas

“Configurando o Valor de Tempo Limite das Configurações de Cache da Sessão do Tivoli Access Manager WebSEAL”

O valor de tempo limite das configurações de cache da sessão do Tivoli Access Manager WebSEAL devem ser configuradas para o mesmo valor do tempo limite da sessão do WebSphere Portal.

## Configurando o Valor de Tempo Limite das Configurações de Cache da Sessão do Tivoli Access Manager WebSEAL

O valor de tempo limite das configurações de cache da sessão do Tivoli Access Manager WebSEAL devem ser configuradas para o mesmo valor do tempo limite da sessão do WebSphere Portal.

### Procedimento

1. Efetue login no servidor de acesso como root.
2. Em uma sessão de terminal, edite o arquivo `/opt/pdweb/etc/webseald-default.conf` e altere o valor de `timeout` na seção `SESSION CACHE SETTINGS` para o mesmo valor do tempo limite de sessão do WebSphere Portal.

**Importante:** O valor `SESSION CACHE SETTINGS timeout` é especificado em segundos. O tempo limite da sessão do WebSphere Portal é especificado em minutos. Se o tempo limite da sessão do WebSphere Portal for 540 minutos (9 horas), o valor de `SESSION CACHE SETTINGS timeout` correspondente seria 32400.

3. Reinicie o Tivoli Access Manager WebSEAL executando o seguinte comando.  
`/usr/bin/pdweb restart`

### Tarefas relacionadas

“Configurando o Valor de Tempo Limite da Sessão do WebSphere Portal” na página 22

O valor de tempo de limite da sessão do WebSphere Portal precisa ser configurado para impedir que um usuário seja desconectado durante uma sessão. Esse valor deve corresponder ao valor de tempo limite das configurações de cache do Tivoli Access Manager WebSEAL.

## Configurando a Conexão Única

O IBM Intelligent Operations Center usa Tivoli Directory Server como seu LDAP para armazenar informações do usuário. Para que ocorra a interação correta com o IBM Lotus Sametime, é necessário ativar conexão única para a solução.

Na solução IBM Intelligent Operations Center, o Tivoli Access Manager WebSEAL autentica usuários ao acessar o IBM Intelligent Operations Center.

A conexão única dentro da solução requer configuração em duas áreas:

- Configuração da conexão única entre WebSphere Portal e IBM Lotus Sametime.
- Configuração da conexão única entre Tivoli Access Manager WebSEAL e IBM Lotus Sametime.

Uma junção é usada para conectar o Tivoli Access Manager WebSEAL, o WebSphere Portal e o WebSphere Application Server Network Deployment por meio do WebSphere Trust Associated Interpreter. Uma junção também é utilizada para conectar o Tivoli Access Manager WebSEAL e o IBM Lotus Sametime para permitir o uso do IBM Lotus Sametime em um navegador.

A conexão única entre WebSphere Portal, IBM Lotus Sametime e outros servidores utilizam um token IBM LTPA para compartilhar credenciais do usuário.

## Configurando a Conexão Única do IBM Lotus Sametime e WebSphere Portal

Configure a conexão única entre IBM Lotus Sametime e WebSphere Portal para que o IBM Lotus Sametime possa ser usada com o IBM Intelligent Operations Center.

### Antes de Iniciar

Antes de configurar a conexão única, os itens a seguir devem ser instalados com sucesso.

- Arquitetura base do IBM Intelligent Operations Center
- Pacote de soluções do IBM Intelligent Operations Center
- O JRE correcto para o portlet IBM Lotus Sametime.

Você também deve ter acesso aos seguintes itens:

- WebSphere Portal em `http://nome_do_host_do_portal:10039/wps/portal`
- IBM Lotus Sametime em `http://nome_do_host_do_sametime.nome_do_domínio:81/`

e, que *portal\_hostname* é o nome do host do WebSphere Portal, *sametime\_hostname* é o nome do host para o IBM Lotus Sametime, e *domain\_name* é o nome do domínio para o IBM Lotus Sametime.

### Procedimento

1. “Importando o Token WebSphere Portal SSO LPTA”
2. “Verificando as Alterações de Configuração” na página 25

#### Importando o Token WebSphere Portal SSO LPTA:

Execute as etapas a seguir para importar o token WebSphere Portal SSO LPTA no servidor Lotus Domino.

### Procedimento

1. Instale o Lotus Notes Client 8.5.1 em um sistema Windows usando as instruções no centro de informações do Lotus Domino e do Lotus Notes.
2. Copie o ID de administrador do IBM Lotus Sametime e o arquivo-chave LTPA do servidor de portal para o sistema que está executando o Lotus Notes Client. O local padrão do ID do administrador é `/local/notesdata/admin.id`. O local padrão do arquivo-chave LTPA é `/opt/IBM/iss/portal.ltpa`.
3. Abra o Lotus Notes Client.
4. Alterne para o arquivo `admin.id` utilizando **Switch ID**.
5. Faça login utilizando o ID de administrador copiado do servidor de portal. A senha padrão é `passwd0rd`.
6. Abra o arquivo `names.nsf`.

7. Clique em **Web > Web configurations > Web SSO Configurations > Web SSO Configuration for Ltpa Token**.
8. Clique em **Edit Document**.
9. Clique em **Keys... > Import WebSphere LTPA Key**.
10. Clique em **OK** para sobrescrever a configuração.
11. Insira o caminho completo para o arquivo LTPA no sistema Windows.
12. Insira a senha para o arquivo LTPA configurado quando o arquivo LTPA foi exportado.
13. Configure **Map names in LTPA tokens** para Enabled.
14. Configure **DNS Domain** para o nome de domínio configurado em WebSphere Portal. Por exemplo, `.suaempresa.com`.
15. Clique em **Salvar e Fechar**.
16. Reinicie o servidor Lotus Domino a partir do console Lotus Domino utilizando **restart server** ou a partir do menu **Iniciar > Programas**.
17. Pare o servidor WebSphere Portal com o seguinte comando.  

```
"/opt/IBM/WebSphere/AppServer/bin/stopServer.sh WebSphere_Portal -username wpsadmin -password wpspwd
```

 Em que `wpsadmin` e `wpspwd` são o ID e senha de administrador do WebSphere Portal definidos quando o IBM Intelligent Operations Center foi implementado.
18. Remova todos os arquivos temporários do WebSphere Portal executando o seguinte comando.  

```
rm -rf /opt/IBM/WebSphere/wp_profile/wstemp/
```
19. Reinicie o WebSphere Portal executando o seguinte comando.  

```
/opt/IBM/WebSphere/AppServer/bin/startServer.sh WebSphere_Portal
```

#### Informações relacionadas

 Centro de Informações do Lotus Domino e Lotus Notes

#### Verificando as Alterações de Configuração:

Siga as etapas a seguir para verificar suas alterações de configuração.

#### Procedimento

1. Abra o portal IBM Intelligent Operations Center.
2. Acesse a **Lista de Contatos do Sametime**.
3. Confirme que o usuário com login efetuado está sendo exibido como on-line.

### Configurando a Conexão Única do IBM Lotus Sametime e do Tivoli Access Manager WebSEAL

A Conexão única deve ser configurada para o Tivoli Access Manager WebSEAL para que o IBM Lotus Sametime possa ser utilizado com o IBM Intelligent Operations Center.

#### Procedimento

1. "Ativando Tunelamento HTTP"
2. "Modificando o Arquivo `stlinks.js`" na página 26
3. "Ativando Proxy Reverso" na página 27
4. "Criando uma Junção Tivoli Access Manager WebSEAL" na página 27
5. "Reiniciando o Servidor IBM Lotus Sametime" na página 28

#### Ativando Tunelamento HTTP:

Siga as etapas a seguir para ativar o tunelamento HTTP.

### Procedimento

1. No sistema Windows execute o Lotus Domino Administrator. Para obter informações sobre como executar o Lotus Domino Administrator, consulte o centro de informações do Lotus Domino e Lotus Notes.
2. Acesse o banco de dados do STCConfig.nsf.
3. Abra o formulário **CommunityConnectivity**.
4. Altere a **Porta de Tunelamento HTTP** para 81.
5. Altere o **Nome do Host de Tunelamento HTTP** para o nome do host do IBM Lotus Sametime.
6. Assegure que **O tunelamento HTTP é suportado?** seja true.
7. Abra o documento **BroadcastGateway**.
8. Altere a **Porta de Tunelamento HTTP** para 81.
9. Altere o **Nome do Host de Tunelamento HTTP** para o nome do host do IBM Lotus Sametime.
10. Assegure que **Suporte a tunelamento HTTP** seja true.
11. Abra o documento **MeetingServices**.
12. Altere a **Porta de Tunelamento HTTP** para 81.
13. Altere o **Nome do Host de Tunelamento HTTP** para o nome do host do IBM Lotus Sametime.
14. Assegure que o **Suporte a tunelamento HTTP ativado** seja true.
15. Feche as guias e salve as alterações.
16. No Lotus Domino Administrator, abra a guia **Configuração**.
17. Selecione o **Documento de Servidor Atual** na seção **Servidor**.
18. Abra a guia **Portas**.
19. Abra a guia **Portas da Internet**.
20. Abra a guia **Web**.
21. Altere o **Número de porta TCP/IP** para 8088.
22. Feche as guias e salve as alterações.
23. Edite o arquivo /local/notesdata/sametime.ini.
24. Certifique-se de que ConfigurationPort seja 8088 como no exemplo a seguir.  
ConfigurationPort=8088

### Informações relacionadas

 Centro de Informações do Lotus Domino e Lotus Notes

### Modificando o Arquivo stlinks.js:

Execute as etapas a seguir para modificar o arquivo stlinks.js.

### Procedimento

1. Edite o arquivo /local/notesdata/domino/html/sametime/stlinks/stlinks.js.
2. Certifique-se de que os valores a seguir estejam configurados.

```
var ll_RProxyName="http://nome_do_host_webseal";
var ll_AffinityId="junção";
isTAM_env = true;
racingConnTimeout = 5000;
```

Em que *nome\_do\_host\_webseal* é o nome de host do Tivoli Access Manager WebSEAL e *junção* é o nome da junção que será criado com o Tivoli Access Manager WebSEAL.

3. Salve o arquivo.

#### Tarefas relacionadas

“Criando uma Junção Tivoli Access Manager WebSEAL”

Siga as etapas a seguir para criar a junção em Tivoli Access Manager WebSEAL.

#### Ativando Proxy Reverso:

Execute as etapas a seguir para ativar um proxy reverso.

#### Procedimento

1. Efetue login no portal IBM Lotus Sametime Administration no servidor de portal. O nome do usuário é notesadmin e a senha, passwd. A URL para o portal IBM Lotus Sametime Administration será similar a seguinte. Substitua *seu\_nome\_de\_domínio\_do\_sametime* com o valor apropriado para sua instalação  
`http://seu_nome_de_domínio_do_sametime:81/stcenter.nsf?Login`
2. Clique em **Configuração > Conectividade**.
3. Em **Rede de Serviços de Comunidades**, selecione **Ativar o Sametime Connect para que clientes de navegadores tentem fazer o tunelamento HTTP do Community Server após tentar outras opções**.
4. Em **Suporte a Proxy Reverso** selecione **Ativar descoberta de proxy reverso no cliente**.
5. Para **Alias do Servidor (Isto é o que o proxy reverso está usando para encaminhar mensagens HTTP(S) para o servidor)**, insira o nome da junção do Tivoli Access Manager WebSEAL que você criará na próxima etapa.
6. Clique em **Atualizar**.

#### Tarefas relacionadas

“Criando uma Junção Tivoli Access Manager WebSEAL”

Siga as etapas a seguir para criar a junção em Tivoli Access Manager WebSEAL.

#### Criando uma Junção Tivoli Access Manager WebSEAL:

Siga as etapas a seguir para criar a junção em Tivoli Access Manager WebSEAL.

#### Procedimento

1. Copie a chave LPTA do servidor de portal no servidor de acesso.
2. Execute o comando a seguir no servidor de acesso para efetuar login no console de comandos pdadmin do Tivoli Access Manager WebSEAL.  
`pdadmin -a sec_master -p passwd`

3. Execute o comando a seguir no servidor de acesso.

```
pdadmin> server task default_webseald_server_name create -t tcp -h sametime_host_name  
-p 81 -i -j -A -F path_to_LTPA_key -Z LTPA_key_password /st
```

Em que:

- *server\_name* é o nome de host completo do servidor Tivoli Access Manager WebSEAL.
- *sametime\_host\_name* é o nome do host do servidor IBM Lotus Sametime no servidor de portal.
- *path\_to\_LTPA\_key* é o caminho em que a chave LTPA foi copiada no servidor de acesso.

- *LTPA\_key\_password* é a senha do arquivo-chave LTPA.

**Importante:** Não especifique o parâmetro `-w`. Especificar `-w` pode fazer com que certas solicitações geradas pelo IBM Lotus Sametime não sejam transmitidas pela junção. A chave LTPA usada na junção é a mesma chave LTPA usada pelo servidor IBM Lotus Sametime no documento Web SSO Configuration. A chave IBM Lotus Sametime LPTA foi especificada ao configurar a conexão única do WebSphere Portal.

```
server task default-webseald-rhel21.yourco.com create -t tcp -h rhel21.yourco.com
-p 81 -i -j -A -F /root/portal.ltpa -Z pw123456 /st
```

### Reiniciando o Servidor IBM Lotus Sametime:

Execute as etapas a seguir para interromper e reiniciar o IBM Lotus Sametime.

#### Procedimento

1. Pare o servidor IBM Lotus Sametime executando os seguintes comandos.

```
su - notes
cd /local/notesdata
/opt/ibm/lotus/bin/server -q
```

2. Reinicie o servidor IBM Lotus Sametime executando os seguintes comandos.

```
su - notes
cd /local/notesdata
/opt/ibm/lotus/bin/server
```

## Criando uma Junção do WebSphere Application Server Network Deployment

É necessário criar uma junção e ACL do WebSphere Application Server Network Deployment para que usuários possam acessar o IBM Intelligent Operations Center. É necessário criar uma junção padrão. Isto pode ser feito utilizando uma linha de comandos ou por meio do Tivoli Access Manager Web Portal Manager.

#### Conceitos relacionados

“Gerenciando um ACL de Junção do WebSphere Application Server Network Deployment” na página 43

Um administrador pode usar um comando ou o Tivoli Access Manager Web Portal Manager para gerenciar usuários e grupos definidos na junção do WebSphere Application Server Network Deployment.

### Criando uma Junção do WebSphere Application Server Network Deployment Usando a Linha de Comandos

Uma junção padrão e ACL podem ser criadas executando uma série de comandos.

#### Procedimento

1. No servidor de acesso, efetue login no terminal do servidor Tivoli Access Manager WebSEAL usando os seguintes comandos.

```
# pdadmin
login
```

Use `sec_master` para o ID do usuário e `passwd` para a senha.

2. Execute o comando a seguir para criar uma junção padrão.

```
server task default-webseald-WebSEAL_Host_Name create -b supply -c iv-creds -t tcp -h Nome_do_Host_do_WAS -p Porta_do_WAS /Nome_da_junção
```

3. Para incluir outro WebSphere Application Server na mesma junção, execute o comando a seguir.

```
server task default-webseald-nome_do_host_WebSEAL add -h nome_do_Host_WAS -p Porta_WAS /Nome_da_Junção
```



4. Execute o comando a seguir para criar uma ACL.  
`acl create nome_da_ACL`
5. Execute o comando a seguir para anexar a ACL à junção.  
`acl attach /WebSEAL/nome_do_Host_WebSEAL/nome_da_junção nome_da_ACL`

## Criando uma Junção do WebSphere Application Server Network Deployment Usando o Tivoli Access Manager WebSEAL Web Portal Manager

Uma junção padrão e ACL podem ser criadas ao usar o Tivoli Access Manager WebSEAL Web Portal Manager.

### Procedimento

1. Acesse o Tivoli Access Manager WebSEAL Web Portal Manager na seguinte URL.  
`http://Nome_do_Host_do_Gerenciador_de_Portal_da_Web:9060/ibm/console`  
Use `sec_master` para o ID do usuário e `passwd` para a senha.
2. Clique em **Tivoli Access Manager > Web Portal Manager > WebSEAL > Junção e Listas**.
3. Efetue login com o ID do usuário `sec_master` e senha `passwd`.
4. Clique em **Criar**.
5. Insira os dados a seguir.
  - Ponto de Junção:** O nome do ponto de junção. O nome deve começar com uma barra (/).
  - Host de Destino:** O nome de host do WebSphere Application Server.
  - Porta TCP:** O número da porta WebSphere Application Server. Este valor normalmente é 9080.
  - Cabeçalho de Identidade do Cliente:** Especifique Credencial do Usuário.
  - Tipo:** Especifique Fornecimento.
6. Clique em **Criar**.
7. Para incluir outro WebSphere Application Server na junção, clique em **Incluir** na página Listar Junções. Em seguida insira as informações de WebSphere Application Server **Host de Destino** e **Porta TCP**.
8. Clique em **Criar**.
9. Clique em **Tivoli Access Manager > Web Portal Manager > ACL**.  
Use `sec_master` para o ID do usuário e `passwd` para a senha.
10. Clique em **Criar**.
11. Insira um valor para o **Nome da ACL**.
12. Clique em **Criar**.
13. Clique em **Tivoli Access Manager > Web Portal Manager > Espaço de Objetos > Procurar Espaço de Objetos**.  
Use `sec_master` para o ID do usuário e `passwd` para a senha.
14. Expanda a visualização **Espaço de Objetos** e acesse `/WebSEAL/nome_do_host_WebSEAL-default/nome_da_junção`.
15. Selecione o `nome_da_junção` criado anteriormente.
16. Clique em **Anexar** próximo ao campo **ACL Anexada**.
17. Selecione o nome da ACL criada anteriormente na lista.
18. Clique em **Aplicar**.

## Configurando o WebSphere Application Server Network Deployment para Conexão Única LTPA

Por padrão, o IBM Intelligent Operations Center está configurado para usar TAI++ como a solução de conexão única para o WebSphere Application Server Network Deployment. Como alternativa, Lightweight Third-Party Authentication (LTPA) pode ser usada para conexão única do WebSphere Application Server Network Deployment.

### Sobre Esta Tarefa

Para usar LTPA para conexão única, a chave LTPA deve ser importada para o WebSphere Application Server Network Deployment.

### Procedimento

1. No servidor de portal, localize o arquivo de chave LTPA. Por padrão, o arquivo é `/opt/IBM/iss/portal.ltpa`.
2. Copie o arquivo de chave LTPA para o servidor de integração e aplicativo. Por exemplo, para o diretório `/tmp`.
3. Efetue login no console do WebSphere Application Server Network Deployment no servidor de integração e aplicativo. A URL será semelhante à seguinte.  
`http://hostname:9060/admin`

em que *hostname* é o nome do host do WebSphere Application Server Network Deployment.

4. Clique em **Segurança Global > LTPA**.
5. Insira a senha da chave LTPA em **Senha** e **Confirmar Senha**.
6. Insira o nome de arquivo completo onde o arquivo de chave LTPA foi copiado na etapa 2 em **Nome de Arquivo de Chave Completo**. Por exemplo, `/tmp/portal.ltpa`.
7. Clique em **Importar Chaves**.
8. Clique em **Salvar** para salvar a configuração.
9. Clique em **Administração do Sistema > Nós**.
10. Clique em **Sincronizar** para sincronizar a chave entre o WebSphere Application Server Network Deployment e os nós.
11. Reinicie o Gerenciador de Implementação, o agente do nó e os servidores.

## Ativando Redirecionamento de Login

O Tivoli Access Manager WebSEAL precisa ser configurado para redirecionar o usuário para o portal padrão do IBM Intelligent Operations Center após login.

### Sobre Esta Tarefa

Quando uma sessão do usuário atinge o tempo limite e o Tivoli Access Manager WebSEAL autentica o usuário novamente, o usuário pode não ser redirecionado corretamente para o IBM Intelligent Operations Center após autenticação bem-sucedida.

Para configurar o redirecionamento automático, faça o seguinte.

## Procedimento

1. Efetue login no servidor de acesso.
2. Edite o arquivo de configuração do Tivoli Access Manager WebSEAL no diretório /opt/pdweb/etc. O nome do arquivo estará no formato `webseald-webseal_instance_name.config`, em que `webseal_instance_name` é o nome da instância do Tivoli Access Manager WebSEAL.
3. Em `[enable-redirects]`, remova o caractere # antes de `forms-auth`.
4. Para `login-redirect-page`, especifique a URL para a qual o usuário será redirecionado após login. Especifique a URL como um caminho relativo do IBM Intelligent Operations Center. Por exemplo, `/wpsv70/wps/myportal`.
5. Salve as mudanças.
6. Pare e reinicie o servidor do Tivoli Access Manager WebSEAL executando o comando a seguir.  

```
pdweb restart
```

## Configurando a Porta e o Protocolo do Gateway de Serviços REST

Altere os valores de protocolo e porta do Gateway de Serviços REST para processamento correto do indicador chave de desempenho (KPI).

### Sobre Esta Tarefa

Configure a porta e o protocolo do Gateway de Serviços REST usando o console administrativo do WebSphere Application Server (perfil `qmwas`) no servidor analítico.

## Procedimento

1. Abra **Serviços > Serviços Rest > Provedores de Serviços Rest**.
2. Selecione **http://** para **Protocolo**.
3. Insira 9080 para **Porta**.
4. Salve as mudanças.

## Excluindo Usuários de Amostra

O IBM Intelligent Operations Center é fornecido com usuários de amostra. Esses usuários devem ser excluídos após a instalação do IBM Intelligent Operations Center.

### Sobre Esta Tarefa

Para excluir os usuários pré-definidos, faça o seguinte.

## Procedimento

1. No servidor de portal, faça login no WebSphere Portal.
2. No portal **Administração**, clique em **Acessar > Usuários e Grupos**.
3. Clique no ícone excluir para os seguintes usuários:
  - rnuetz
  - akelly
  - lsmith
  - swilliams
  - jbarnes

- scollins
- tdelorne

**Importante:** Não exclua os usuários necessários a seguir. Se forem excluídos, o IBM Intelligent Operations Center não operará corretamente.

- wpsadmin
- wasadmin
- wpsbind
- admin
- notesadmin

#### **Informações relacionadas**

Funções e Responsabilidades do Usuário

O IBM Intelligent Operations Center implementa segurança para limitar acesso a recursos e dados baseados em funções de usuários.

## **Verificando a Publicação de Ocorrências CAP**

É possível criar ocorrências de amostra e publicar mensagens Common Alerting Protocol (CAP) no IBM Intelligent Operations Center.

Para obter informações sobre como criar ocorrências de amostra e como publicar mensagens CAP de amostra, consulte o link no final do tópico.

#### **Conceitos relacionados**

“Publicando Mensagens CAP” na página 56

O IBM Intelligent Operations Center fornece o portlet Publicador de Amostras como ferramenta de teste automatizado, além de oferecer recursos de publicação adicional como serviço.

---

## Capítulo 3. Protegendo a Solução

A segurança é importante porque o IBM Intelligent Operations Center é fundamental para as operações essenciais. Para assegurar segurança, é importante gerenciar usuários da solução e fornecer a todos os usuários o nível correto de acesso dentro do IBM Intelligent Operations Center.

A autenticação do usuário é associada a direitos de autorização que fornecem ao usuário acesso aos recursos e dados apropriados. O IBM Intelligent Operations Center suporta integração com a infraestrutura de segurança existente para conexão única.

As permissões do usuário são gerenciadas por meio de usuários e grupos do WebSphere Portal Server. O Servidor de portal é projetado no Tivoli Directory Server como o banco de dados Lightweight Directory Access Protocol (LDAP) para o IBM Intelligent Operations Center.

**Nota:** O sistema de segurança fornecido com o IBM Intelligent Operations Center pode acomodar muitos grupos de usuários, funções e permissões. Acomodar muitos grupos de usuários, funções e permissões pode levar a um regime de segurança difícil de gerenciar. É recomendado que os administradores restrinjam o número de grupos e permissões.

### Funções e Permissões do Usuário

A associação de um grupo de usuários baseada em função fornece uma forma de controlar o acesso ao IBM Intelligent Operations Center. Os usuários de um grupo têm acesso somente aos recursos da solução correspondentes à sua função. Se um membro de um grupo de usuários baseado em função também ajuda os usuários a focarem tarefas apropriadas. As funções padrão são: Executivo, Supervisor e Operador.

Para incluir um usuário no IBM Intelligent Operations Center:

1. Escolha um grupo adequado à função do usuário na organização e torne o usuário um membro desse grupo.
2. Conclua um perfil para o usuário incluindo pelo menos o ID de usuário, nome e senha.

### Categorias de Dados e Permissões

A segurança dos dados armazenados nos bancos de dados no IBM Intelligent Operations Center é gerenciada por meio da implementação de acesso baseado em função nos bancos de dados. O acesso a um recurso do IBM Intelligent Operations Center não significa que todos os dados estejam disponíveis para o usuário. A segurança dos dados é aplicada no nível do servidor para assegurar que os usuários visualizem somente os dados adequados. As categorias padrão são: Geofísico, Transporte, Meteorológico, Ambiental, Infraestrutura, Químico, Biológico, Segurança, Resgate, Incêndio, Saúde e Outro.

## WebSphere Portal

O WebSphere Portal é um componente da solução do IBM Intelligent Operations Center. Fornece uma plataforma que pode ser escalonada para acomodar o conjunto de usuários necessário. Também fornece acesso baseado em função que pode ser ajustado para refletir a estrutura de organização necessária. O conjunto de documentação para o IBM WebSphere Portal não está incluído na solução. Em vez da documentação do IBM Intelligent Operations Center, ele aponta para a documentação do WebSphere Portal, onde relevante. É possível visualizar, criar e excluir usuários ou grupos de usuários com o portlet **Gerenciar Usuários e Grupos**. Também é possível alterar associações do grupo. Um link é fornecido no final deste tópico para a documentação do WebSphere Portal neste portlet.

### Informações relacionadas

 [Documentação do IBM WebSphere Portal](#)

---

## Funções e Responsabilidades do Usuário

O IBM Intelligent Operations Center implementa segurança para limitar acesso a recursos e dados baseados em funções de usuários.

Um usuário que deseja usar um recurso específico deve se tornar um membro de um grupo de funções de usuários que dê a ele o nível de acesso de login necessário para usar esse recurso. Um usuário torna-se um membro de um grupo de funções de usuários por um administrador de usuários. A tabela a seguir mostra como funções da vida real podem ser mapeadas para níveis de acesso de login no IBM Intelligent Operations Center.

*Tabela 9. Funções e Níveis de Acesso de Login do IBM Intelligent Operations Center*

Função	Responsabilidades	Nível de acesso de login
Executivo	<ul style="list-style-type: none"><li>• Define os requisitos e limites de entrada para ocorrências, incidentes e Key Performance Indicators (KPIs)</li><li>• Visualiza resumos visuais, detalhes e relatórios de alto nível abrangendo:<ul style="list-style-type: none"><li>– KPIs</li><li>– Ocorrências</li></ul></li><li>• Comunica decisões ligadas a políticas, direção a longo prazo e decisões de alto nível</li></ul>	Executivo de Toda a Cidade
Gerente	<ul style="list-style-type: none"><li>• Gerencia ocorrências e incidentes</li><li>• Produz e monitora relatórios de KPI</li><li>• Emite alertas</li><li>• Analisa ocorrências em busca de mudanças de status ou requisitos de ação</li><li>• Toma decisões sobre medidas corretivas a curto prazo</li></ul>	Supervisor de Toda a Cidade

Tabela 9. Funções e Níveis de Acesso de Login do IBM Intelligent Operations Center (continuação)

Função	Responsabilidades	Nível de acesso de login
Operador	<ul style="list-style-type: none"> <li>• Monitora informações sobre ocorrências</li> <li>• Monitora alertas</li> <li>• Visualiza detalhes</li> <li>• Emite comunicações</li> <li>• Atualizar dados de ocorrências ou incidentes com mais informações, por exemplo:                             <ul style="list-style-type: none"> <li>– Relatórios por telefone</li> <li>– Opiniões da equipe de construção ou manutenção</li> </ul> </li> </ul>	Operador de Toda a Cidade
Administrador de Usuários	Administra todos os aspectos dos usuários, incluindo a definição de grupos, designação de permissões a grupos e designação de usuários a grupos. Fornece o nível de acesso correto ao usuários. O nível de acesso é designado com base na associação ao grupo.	Administrador de Usuários
Administrador de TI	Cria e administra contas de usuários, gerencia o servidor de portal incluindo a manutenção, segurança e upgrades do servidor, além de resolver problemas do servidor. Assegura desempenho ideal de todos os processos e procedimentos operacionais. Responsável para administrar o ambiente de TI e a solução.	Administrador de Usuários
Administrador de Segurança	Gerencia e mantém o sistema de segurança, fazendo a integração de todos os aplicativos de segurança. Geralmente considerado uma especialização do Administrador de TI.	Administrador de Usuários
Integrador de Sistemas	Customiza a solução para um cliente, incluindo modelagem de KPI, criação de política de impacto, integração a sistemas existentes e criação de novos provedores de dados, se necessário.	Administrador de Usuários

Antes de customizar funções e definir usuários para sua organização, familiarize-se com o sistema de segurança do IBM Intelligent Operations Center.

## Usuários de Amostra

No IBM Intelligent Operations Center, usuários de amostra genéricos são definidos com responsabilidades e permissões de acesso correspondentes. Alguns são definidos como exemplos, enquanto que outros são necessários para administração da solução, conforme mostrado na tabela a seguir.

Tabela 10. Usuários de Amostra Definidos em IBM Intelligent Operations Center

ID do usuário	Função	Nível de acesso de login
<b>Usuários necessários</b>		
admin		Administrador de Usuários

Tabela 10. Usuários de Amostra Definidos em IBM Intelligent Operations Center (continuação)

ID do usuário	Função	Nível de acesso de login
notesadmin		Administrador de Usuários
wasadmin		Administrador de Usuários
wpsadmin		Administrador de Usuários
wpsbind		Administrador de Usuários
<b>Usuários de exemplo</b>		
tdelorne	Executivo de Toda a Cidade	Executivo de Toda a Cidade
colins	Supervisor de Toda a Cidade	Supervisor de Toda a Cidade
akelly	Operador de Toda a Cidade	Operador de Toda a Cidade
Williams	Supervisor de Transporte	Supervisor de Tráfego
smith	Operador de Transporte	Operador de Tráfego
rnuez	Supervisor de Utilidade de Água	Supervisor de Água
jbarnes	Operador de Utilidade de Água	Operador de Água

Quando estiver pronto para definir seus próprios usuários, exclua os usuários de exemplo. Você não deve excluir os usuários necessários. Eles são necessários para a operação correta do IBM Intelligent Operations Center.

**Importante:** Para os usuários necessários, substitua as senhas padrão designando novas senhas. Para obter informações sobre como atualizar IDs de usuários e senha, consulte a Documentação do IBM WebSphere Portal.

## Incluindo um Usuário ou Grupo

Selecione um grupo e crie um perfil do usuário para incluir um novo usuário no IBM Intelligent Operations Center. Selecione um nome de grupo para incluir um novo grupo.

### Sobre Esta Tarefa

Primeiro selecione um grupo de funções do usuário para configurar o nível correto de permissões de acesso ao incluir um novo usuário. Em seguida, complete os campos da página **Gerenciamento de Perfil** para que o IBM Intelligent Operations Center tenha as informações necessárias para incluir o novo usuário. Siga o link no final do tópico para obter informações adicionais sobre o que é possível inserir nos campos na página **Gerenciamento de Perfil**.

### Procedimento

1. Efetue login em <http://portalServer/wps/myportal> como um usuário administrativo.
2. Clique em **Administração** na barra de navegação na parte superior da página.
3. Clique em **Acesso** no menu da barra lateral.
4. Clique em **Usuários e Grupos** no submenu.



5. Se estiver incluindo um novo usuário, selecione uma função concedendo ao usuário a associação a um grupo. Procure o grupo clicando em **Todos os Grupos de Usuários do Portal** para obter uma lista de grupos e clique no grupo requerido.
6. Clique em **Novo Usuário** ou **Novo Grupo**.
7. Se estiver criando um grupo de usuários, insira um nome para o grupo de usuários.
8. Se estiver incluindo um novo usuário, certifique-se de inserir todos os campos requeridos no perfil do usuário, conforme indicado pelos asteriscos.
9. Clique em **OK** para enviar o novo perfil ou grupo.

## Resultados

Uma mensagem confirma se o envio foi bem sucedido. Um novo perfil de usuário é criado e exibido na lista de grupos ou um novo grupo é exibido. O novo usuário é autorizado a acessar o IBM Intelligent Operations Center de acordo com as permissões designadas para o grupo de funções selecionado.

## O que Fazer Depois

- Dê ao novo usuário associação de grupos de categorias de dados de acordo com as permissões de dados necessárias.
- Se um novo grupo tiver sido incluído, inclua o grupo ao ACL da junção do WebSphere Application Server Network Deployment.
- Se um novo grupo tiver sido incluído, as permissões de autorização também deve ser configuradas para o grupo. As permissões de autorização definem quais recursos e dados membros do grupo podem ver e modificar. Para obter informações sobre como configurar as permissões de autorização, consulte a Documentação do Produto IBM WebSphere Portal 7 e procure as informações sobre como designar acesso às páginas.

**Nota:** Para economizar tempo, é possível duplicar designações de grupos para um novo usuário com base em um usuário existente. Selecione o novo usuário e clique no ícone **Duplicar**. Selecione o usuário existente para duplicar associação ao grupo.

### Tarefas relacionadas

“Visualizando ou Modificando a Associação ao Grupo”

Visualize ou modifique a associação ao grupo para gerenciar as permissões de acesso dos usuários no IBM Intelligent Operations Center.

“Gerenciando um ACL da Junção do WebSphere Application Server Network Deployment Usando a Linha de Comandos” na página 43

Os usuários e grupos podem ser incluídos no ACL da junção do WebSphere Application Server Network Deployment executando uma série de comandos.

“Gerenciando um ACL da Junção do WebSphere Application Server Network Deployment Usando o Tivoli Access Manager WebSEAL Web Portal Manager” na página 44

Os usuários e grupos podem ser incluídos no ACL da junção do WebSphere Application Server Network Deployment usando o Tivoli Access Manager WebSEAL Web Portal Manager.

### Referências relacionadas

“Grupos de Funções de Usuários e Permissões de Autorização” na página 40

Cada usuário tem associação designada de um ou mais grupos de funções de usuários. Um conjunto de permissões de autorização para acessar recursos no IBM Intelligent Operations Center está associado a cada grupo de funções de usuários.

### Informações relacionadas

 [Documentação do IBM WebSphere Portal](#)

---

## Visualizando ou Modificando a Associação ao Grupo

Visualize ou modifique a associação ao grupo para gerenciar as permissões de acesso dos usuários no IBM Intelligent Operations Center.

### Sobre Esta Tarefa

Selecione o grupo correspondente à função ou categoria de dados para a qual deseja visualizar ou alterar a associação. A associação de um grupo de funções fornece aos usuários acesso às partes da solução apropriadas a essa função. A associação de um grupo de categorias fornece aos usuários acesso às ocorrências, indicadores chaves de desempenho (KPIs) e alertas associados a essa categoria.

Passa o mouse sobre um ícone para visualizar a ajuda instantânea que indica o propósito do ícone.

### Procedimento

1. Efetue logon em `http://portalServer/wps/myportal` como um usuário administrativo.
2. Clique em **Administração** na barra de navegação na parte superior da página.
3. Clique em **Acesso** no menu da barra lateral.
4. Clique em **Usuários e Grupos** no submenu.
5. Clique em **Todos os Grupos de Usuários do Portal** para obter uma lista de grupos e clique no grupo que precisar. Os membros do grupo serão listados.
6. É possível executar as ações a seguir em relação à associação ao grupo:
  - Visualizar a associação de outros grupos clicando em **Visualizar associação** para o ID do usuário.
  - Incluir um usuário ou usuários ao grupo clicando em **Incluir membro** e selecionando o usuário ou usuários a serem incluídos.
  - Remover um usuário do grupo clicando em **Remover** para o ID do usuário.

### Tarefas relacionadas

“Incluindo um Usuário ou Grupo” na página 36

Selecione um grupo e crie um perfil do usuário para incluir um novo usuário no IBM Intelligent Operations Center. Selecione um nome de grupo para incluir um novo grupo.

### Referências relacionadas

“Grupos de Funções de Usuários e Permissões de Autorização” na página 40

Cada usuário tem associação designada de um ou mais grupos de funções de usuários. Um conjunto de permissões de autorização para acessar recursos no IBM Intelligent Operations Center está associado a cada grupo de funções de usuários.

“Grupos de Categorias de Usuários e Permissões de Acesso a Dados” na página 41

O IBM Intelligent Operations Center controla acesso a tipos de dados com base na associação ao grupo de categorias de usuários.

### Informações relacionadas

 Documentação do IBM WebSphere Portal

---

## Visualizando ou Editando um Perfil de Usuário

Visualize ou edite o perfil de um usuário para configurar ou reconfigurar qualquer dos atributos do perfil do usuário, inclusive a senha. Não é possível alterar o ID do usuário.

### Sobre Esta Tarefa

Selecione o usuário da lista de usuários do portal autenticados para abrir o perfil do usuário e alterar os detalhes do perfil. Cada usuário também pode alterar seu próprio perfil.

Passa o mouse sobre um ícone para visualizar a ajuda instantânea que indica o propósito do ícone.

### Procedimento

1. Efetue logon em `http://portalServer/wps/myportal` como um usuário administrativo.
2. Clique em **Administração** na barra de navegação superior.
3. Clique em **Acessar** item no menu da barra lateral.
4. Clique em **Usuários e Grupos** no submenu.
5. Clique em **Todos os Usuários Autenticados do Portal** para obter uma lista de usuários.
6. Clique no ícone de edição para o usuário para exibir a página **Gerenciamento de Perfil**. Os campos do atributo para o perfil do usuário são exibidos.
7. Se desejar alterar a senha, insira uma nova senha nos campos **Nova Senha:** e **Confirmar Senha:**.
8. É possível inserir, editar ou excluir informações em qualquer um dos campos restantes.
9. Clique em **OK** para enviar as mudanças que você fez.

### Resultados

O perfil do usuário é atualizado com as mudanças enviadas.

## Informações relacionadas

 [Documentação do IBM WebSphere Portal](#)

---

## Excluindo um Usuário ou Grupo

Exclua um usuário ou grupo do IBM Intelligent Operations Center.

### Sobre Esta Tarefa

Para excluir um usuário, selecione o usuário na lista de usuários autenticados do portal e exclua. Para excluir um grupo, selecione o grupo na lista de grupos de usuários do portal e exclua.

Passa o mouse sobre um ícone para visualizar a ajuda instantânea que indica o propósito do ícone.

### Procedimento

1. Efetue logon em `http://portalServer/wps/myportal` como um usuário administrativo.
2. Clique em **Administração** na barra de navegação superior.
3. Clique em **Acesso** no menu da barra lateral.
4. Clique em **Usuários e Grupos** no submenu:
  - Clique em **Todos os Grupos de Usuários do Portal** para exibir uma lista de grupos.
  - Clique em **Todos os Usuários Autenticados do Portal** para exibir uma lista de usuários.
5. Clique no ícone **Excluir** que corresponde ao usuário ou grupo que você deseja excluir.

### Resultados

O usuário ou grupo que você exclui não existe mais no IBM Intelligent Operations Center. A exclusão de um grupo não exclui os membros do grupo.

## Informações relacionadas

 [Documentação do IBM WebSphere Portal](#)

---

## Grupos de Funções de Usuários e Permissões de Autorização

Cada usuário tem associação designada de um ou mais grupos de funções de usuários. Um conjunto de permissões de autorização para acessar recursos no IBM Intelligent Operations Center está associado a cada grupo de funções de usuários.

Um administrador de usuários designa uma função a um usuário tornando o usuário um membro do grupo de funções de usuários correspondente. A tabela a seguir lista as permissões de autorização para cada grupo de funções de usuários fornecido com o IBM Intelligent Operations Center. Para cada grupo de funções de usuários, uma permissão de autorização é definida para cada recurso no IBM Intelligent Operations Center.

Tabela 11. Recursos do IBM Intelligent Operations Center e Permissões de Autorização de Grupos de Funções de Usuários Associadas

Tipo de recurso	Nome do recurso	Permissão de autorização, por grupo de funções de usuários			
		Executivo de Toda a Cidade	Supervisor de Toda a Cidade	Operador de Toda a Cidade	Administrador de Usuários
Portal	Usuário e Grupos	Nenhuma	Nenhuma	Nenhuma	Permissão de Administrador
Página	Executivo	Permissão de Usuário	Permissão de Usuário	Nenhuma	Permissão de Administrador
Portlet	Status	Permissão de Usuário	Permissão de Usuário	Nenhuma	Permissão de Administrador
Portlet	Drill Down de Key Performance Indicator	Permissão de Usuário	Permissão de Usuário	Nenhuma	Permissão de Administrador
Portlet	Coordenador - Alertas	Permissão de Usuário	Permissão de Usuário	Permissão de Usuário	Permissão de Administrador
Portlet	Contatos do Sametime	Permissão de Usuário	Permissão de Usuário	Permissão de Usuário	Permissão de Administrador
Portlet	Operações	Nenhuma	Permissão de Usuário	Permissão de Usuário	Permissão de Administrador
Portlet	Mapa	Nenhuma	Permissão de Usuário	Permissão de Usuário	Permissão de Administrador
Página	Ocorrências	Nenhuma	Permissão de Usuário	Permissão de Usuário	Permissão de Administrador
Portlet	Resumo das permissões do usuário	Nenhuma	Nenhuma	Nenhuma	Permissão de Administrador
Portlet	Publicador de Amostras	Nenhuma	Nenhuma	Nenhuma	Permissão de Administrador
Portlet	Intelligent Operations Center - Sobre	Nenhuma	Nenhuma	Nenhuma	Permissão de Administrador

**Nota:** Permissões de portal são designadas com base em grupos Lightweight Directory Access Protocol (LDAP).

#### Tarefas relacionadas

“Incluindo um Usuário ou Grupo” na página 36

Selecione um grupo e crie um perfil do usuário para incluir um novo usuário no IBM Intelligent Operations Center. Selecione um nome de grupo para incluir um novo grupo.

“Visualizando ou Modificando a Associação ao Grupo” na página 38

Visualize ou modifique a associação ao grupo para gerenciar as permissões de acesso dos usuários no IBM Intelligent Operations Center.

## Grupos de Categorias de Usuários e Permissões de Acesso a Dados

O IBM Intelligent Operations Center controla acesso a tipos de dados com base na associação ao grupo de categorias de usuários.

Um usuário que precisa acessar uma categoria específica de dados deve se tornar um membro do grupo de categorias de usuários que fornece permissão a eles para acessar esses dados. Um usuário torna-se um membro de um grupo de categorias de usuários por um administrador de usuários. A tabela a seguir lista os grupos de categorias de usuários fornecidos com o IBM Intelligent Operations Center para categorizar ocorrências, Indicadores Chaves de Desempenho (KPIs) e alertas. Por exemplo, se um usuário deseja ver ocorrências ou KPIs relacionadas a água, o usuário deve ser um membro do grupo Infraestrutura, cujo ID do grupo é `ioc_base_infrastructure`.

*Tabela 12. Grupos de Categorias de Usuários para Acesso a Dados*

<b>Grupo de categorias de usuários</b>	<b>Descrição</b>	<b>ID do grupo</b>
CBRNE	Ameaça ou ataque químico, biológico, radiológico, nuclear ou explosivo de grande dimensão	<code>ioc_base_chemical</code> , <code>ioc_base_biological</code> , <code>ioc_base_radiological</code> , <code>ioc_base_nuclear</code>
Ambiental	Ambiente: poluição e outras questões ambientais	<code>ioc_base_environmental</code>
Incêndio	Supressão de incêndio e resgate	<code>ioc_base_fire</code>
Geo	Geofísico (incluindo deslizamentos)	<code>ioc_base_geophysical</code>
Saúde	Medicina e saúde pública	<code>ioc_base_health</code>
Infra	Infraestrutura: Utilidade pública, telecomunicações, outra infraestrutura que não seja de transporte	<code>ioc_base_infrastructure</code>
Met	Meteorologia (incluindo enchentes)	<code>ioc_base_meteorological</code>
Resgate	Resgate e recuperação	<code>ioc_base_rescue</code>
Proteção	Emergência geral e segurança pública	<code>ioc_base_safety</code>
Segurança	Cumprimento da lei, segurança local/privada, da pátria e militar	<code>ioc_base_security</code>
Transporte	Transporte público e privado	<code>ioc_base_transportation</code>
Outro	Outras ocorrências, KPIs ou alertas	<code>ioc_base_other</code>

#### **Tarefas relacionadas**

“Visualizando ou Modificando a Associação ao Grupo” na página 38  
Visualize ou modifique a associação ao grupo para gerenciar as permissões de acesso dos usuários no IBM Intelligent Operations Center.

#### **Informações relacionadas**

 [Documentação do IBM WebSphere Portal](#)

---

## **Resumo das permissões do usuário**

Use o portlet Resumo das permissões do usuário para visualizar as permissões associadas ao IBM Intelligent Operations Center para qualquer usuário.

### **O que é o portlet Resumo das permissões do usuário?**

O portlet Resumo das permissões do usuário é fornecido como uma ferramenta de teste. É possível inserir um ID de usuário para exibir detalhes das permissões do IBM Intelligent Operations Center para o usuário.

## O que o portlet Resumo das permissões do usuário exibe?

Insira o ID do usuário para o qual deseja visualizar os detalhes de permissão. O resumo fornece as seguintes informações:

- Uma lista completa de todos os grupos de categorias disponíveis no IBM Intelligent Operations Center.
- Uma lista das permissões de categorias designadas ao usuário especificado.
- Uma lista de todos os grupos dos quais o usuário especificado é membro.
- Uma lista que exibe cada grupo de categorias e que indica o valor true se o usuário especificado for um membro do grupo ou, caso contrário, o valor false.

Para obter informações adicionais sobre permissões de usuários, acesse o IBM Intelligent Operations Center e procure protegendo a solução.

---

## Gerenciando um ACL de Junção do WebSphere Application Server Network Deployment

Um administrador pode usar um comando ou o Tivoli Access Manager Web Portal Manager para gerenciar usuários e grupos definidos na junção do WebSphere Application Server Network Deployment.

Novos grupos incluídos no ACL da junção do WebSphere Application Server Network Deployment precisam ser incluídos também no IBM Intelligent Operations Center.

### Conceitos relacionados

“Criando uma Junção do WebSphere Application Server Network Deployment” na página 28

É necessário criar uma junção e ACL do WebSphere Application Server Network Deployment para que usuários possam acessar o IBM Intelligent Operations Center. É necessário criar uma junção padrão. Isto pode ser feito utilizando uma linha de comandos ou por meio do Tivoli Access Manager Web Portal Manager.

## Gerenciando um ACL da Junção do WebSphere Application Server Network Deployment Usando a Linha de Comandos

Os usuários e grupos podem ser incluídos no ACL da junção do WebSphere Application Server Network Deployment executando uma série de comandos.

### Procedimento

1. No servidor de acesso, efetue login no terminal do servidor do Tivoli Access Manager WebSEAL usando os comandos a seguir:

```
# pdadmin  
login
```

Insira `sec_master` para o ID do usuário e `passwd` para a senha.

2. Para mostrar as propriedades da ACL, execute o comando a seguir:  
`object show /WebSEAL/WebSeal_hostname-WebSEAL_instance_name/ACL_name`
3. Para incluir novos grupos, execute o comando a seguir:  
`acl modify ACL_name set group group_name Tdrx`
4. Para incluir novos usuários, execute o comando a seguir:  
`acl modify ACL_name set user user_name Tdrx`

#### Tarefas relacionadas

“Incluindo um Usuário ou Grupo” na página 36

Selecione um grupo e crie um perfil do usuário para incluir um novo usuário no IBM Intelligent Operations Center. Selecione um nome de grupo para incluir um novo grupo.

## Gerenciando um ACL da Junção do WebSphere Application Server Network Deployment Usando o Tivoli Access Manager WebSEAL Web Portal Manager

Os usuários e grupos podem ser incluídos no ACL da junção do WebSphere Application Server Network Deployment usando o Tivoli Access Manager WebSEAL Web Portal Manager.

### Procedimento

1. Acesse o Tivoli Access Manager WebSEAL Web Portal Manager na seguinte URL:  
`http://Nome_do_Host_do_Gerenciador_de_Portal_da_Web:9060/ibm/console`  
Insira o ID de usuário de administrador e a senha criados quando o IBM Intelligent Operations Center foi instalado.
2. Clique em **Tivoli Access Manager > Web Portal Manager > ACL > Listar ACL**.  
Insira `sec_master` para o ID do usuário e `passwd` para a senha.
3. Selecione o ACL que deseja alterar.
4. Clique em **Criar**.
5. Para criar um novo grupo, use as subetapas a seguir:
  - a. Altere o **Tipo de Entrada** para Grupo.
  - b. Insira o novo nome do grupo em **Nome da Entrada**.
  - c. Selecione as seguintes permissões: **Passar, Excluir, Ler e Executar**.
  - d. Clique em **Aplicar**.
6. Para criar um novo usuário, use as subetapas a seguir:
  - a. Altere o **Tipo de Entrada** para Usuário.
  - b. Insira o novo nome do usuário em **Nome da Entrada**.
  - c. Selecione as seguintes permissões: **Passar, Excluir, Ler e Executar**.
  - d. Clique em **Aplicar**.

### Resultados

O nome usuário ou grupo é incluído no ACL.

#### Tarefas relacionadas

“Incluindo um Usuário ou Grupo” na página 36

Selecione um grupo e crie um perfil do usuário para incluir um novo usuário no IBM Intelligent Operations Center. Selecione um nome de grupo para incluir um novo grupo.



---

## Capítulo 4. Integrando a Solução

Produtos e serviços podem ser integrados ao IBM Intelligent Operations Center usando ocorrências.

As ocorrências comunicadas ao IBM Intelligent Operations Center devem estar no Protocolo de Alerta Comum. Essas ocorrências podem estar relacionadas a Key Performance Indicators (KPIs) monitorados pelo IBM Intelligent Operations Center ou podem não estar relacionados com KPIs.

---

### Exemplos de sistemas que podem ser integrados

Produtos e serviços podem ser integrados ao IBM Intelligent Operations Center.

Os exemplos de sistemas e serviços incluem:

- Sistemas que relatam problemas de segurança pública.
- Sistemas que relatam sobre ocorrências de tráfego.
- Sistemas que relatam sobre a qualidade e uso da água.
- Sistemas que fornecem dados sobre indisponibilidades e status de ordens de serviço relacionadas.

Esses sistemas devem poder se comunicar com o IBM Intelligent Operations Center e enviar ocorrências e medidas no protocolo suportado à fila de ocorrências de entrada do IBM Intelligent Operations Center.

#### Conceitos relacionados

“Usando a Fila de Ocorrências de Entrada Definida para o IBM Intelligent Operations Center” na página 56

Ocorrências CAP podem ser publicadas no IBM Intelligent Operations Center direcionando as mesmas à instância do WebSphere Message Broker incluída.

“Integrando ao Common Alerting Protocol” na página 48

O Protocolo de Alerta Comum (CAP) é usado para trocar informações de ocorrências entre o IBM Intelligent Operations Center e sistemas externos.

---

### Pontos de integração e protocolos

Os produtos e serviços podem ser integrados ao IBM Intelligent Operations Center por meio do WebSphere Message Broker. As definições de processamento para os Key Performance Indicators (KPIs) são criadas usando o Rational Application Developer e o Kit de Ferramentas dos Desenvolvedores do IBM Business Monitor. KPIs são monitorados pelo IBM Business Monitor.

#### Eventos e KPIs

O IBM Intelligent Operations Center usa eventos e Key Performance Indicators (KPIs) para determinar como as informações são exibidas.

Os eventos são recebidos pelo IBM Intelligent Operations Center. Esses eventos podem ser exibidos no portlet do Ocorrências e podem afetar a exibição do portlet do Mapa.

As definições de KPI determinam como os eventos serão exibidos. Por exemplo, se um limite de KPI for excedido, o evento pode ser sinalizado com uma urgência ou gravidade maior. Os eventos sem as definições de KPI correspondentes serão exibidos com as informações recebidas.

As definições de KPI também determinam a exibição do portlet de status.

Ocorrências devem ser recebidas pelo IBM Intelligent Operations Center no formato Protocolo de Alerta Comum (CAP). O processamento de KPIs é definido usando o Rational Application Developer com o kit de ferramentas do IBM Business Monitor instalado.

#### **Conceitos relacionados**

“Visualização Executivo” na página 95

Use a visualização Executivo para obter uma visualização consolidada dos Key Performance Indicator (KPIs) e alertas associados aos KPIs. A visualização Executivo permite que usuários com responsabilidade entre organizações monitorem, gerenciem e respondam a mudanças de status com relação às áreas chaves de desempenho e bem estar organizacional.

“Visualização Operações” na página 100

Use a visualização Operações para manter o reconhecimento das ocorrências. É direcionada para operadores, gerentes ou outros eventos atuais de monitoramento e eventos futuros do planejamento.

“Customizando KPIs” na página 60

Indicadores chaves de desempenho (KPIs) podem ser criados e modificados usando o IBM Business Monitor e o IBM Business Monitor Development Toolkit.

#### **Política para Atualizações de KPI**

A política IBM Intelligent Operations Center determina se uma ocorrência recebida é uma atualização de ocorrência KPI e em seguida envia-a para processamento para gerar uma atualização KPI ou um alerta, dependendo dos parâmetros. Uma ocorrência de KPI é determinada por `<code>KPI</code>` no bloco de alerta do XML de Protocolo de Alerta Comum.

Se a ocorrência for confirmada como uma atualização de KPI, a política verifica os parâmetros de KPI e gera um XML de ocorrência de KPI para enviar ao IBM Business Monitor para processamento.

A tabela a seguir mostra uma atualização de ocorrência de KPI de amostra.

*Tabela 13. Propriedades de Ocorrência de KPI de Amostra*

<b>Propriedade</b>	<b>Valor</b>
Emissor	security@rtp.city.gov
Tipo de Ocorrência	Tempo de Resposta Policial
Status da Ocorrência	Real - Acionável por todos os destinatários-alvo
Escopo da Ocorrência	Público - Para divulgação geral para todos os tipos de público
Categoria	Segurança
Gravidade	Grave
Certeza	Provável
Urgência	Imediato
Tipo de mensagem	Alerta- informações iniciais que requerem atenção por destinatários alvo

Tabela 13. Propriedades de Ocorrência de KPI de Amostra (continuação)

Propriedade	Valor
Descrição	Assalto
Data / hora de envio	2011-04-18T02:28:10-05:00

A tabela a seguir mostra os parâmetros de KPI de amostra associados à atualização da ocorrência de KPI na Tabela 13 na página 46.

Tabela 14. Parâmetros de Ocorrência KPI de Amostra

Parâmetro	Valor
Número do Relatório	1111
Distrito	1o distrito
Respondido	2011-02-15T15:05:07-05:00

### Conceitos relacionados

“Status” na página 96

Use o portlet Status para visualizar o status dos Key Performance Indicator (KPIs) de uma única organização ou de várias organizações.

“Coordenador - Alertas” na página 98

Use o portlet Coordenador - Alertas para visualizar as mensagens de alerta e os seus detalhes.

### Política para a Correlação de Ocorrências

A política de correlação de ocorrência determina se o IBM Intelligent Operations Center identifica ocorrências que afetam umas às outras devido a seu horário ou proximidade.

A correlação de ocorrências depende do intervalo de tempo e do local no qual elas ocorrem, definidos da seguinte forma:

- O intervalo de tempo de uma ocorrência é definida pelos valores de data e hora de início e os valores de data e hora expirados para a ocorrência. O intervalo de tempo padrão para a correlação de ocorrências é configurado para dentro de duas horas.
- O local de uma ocorrência é definido pelas coordenadas da latitude e longitude e o raio do círculo de uma área associada à ocorrência. Nem todas as ocorrências estão associados a uma área e um raio, o valor padrão é 0. A distância padrão para a correlação de ocorrências está configurada para dentro de 5 milhas.

Se uma ocorrência recebida atender a ambos os critérios de correlação, será gerado um alerta no portlet do Coordenador - Alertas. É possível que duas ou mais ocorrências atendam aos critérios da correlação. Os critérios da correlação de ocorrências podem ser configurados na tabela SYSPROP do IBM Intelligent Operations Center. A distância, o intervalo de tempo e a unidade de distância podem ser especificados.

### Conceitos relacionados

“Coordenador - Alertas” na página 98

Use o portlet Coordenador - Alertas para visualizar as mensagens de alerta e os seus detalhes.

“Especificando Dados de Configuração para Todo o Sistema” na página 81

A tabela IBM Intelligent Operations Center SYSPROP armazena os dados de configuração do IBM Intelligent Operations Center.

## Integrando ao Common Alerting Protocol

O Protocolo de Alerta Comum (CAP) é usado para trocar informações de ocorrências entre o IBM Intelligent Operations Center e sistemas externos.

O CAP é um formato genérico para trocar alertas de emergência e avisos públicos por várias redes. Ele fornece um formato de mensagem aberto, não proprietário digital para todos os tipos de alertas e notificações. O CAP é compatível com técnicas emergentes, como serviços da Web, enquanto oferece recursos aprimorados. Esses recursos incluem:

- Destino geográfico flexível usando formatos de latitude e longitude e outras representações geoespaciais em três dimensões
- Sistema de mensagens multilingual e multiaudiência
- Horários e expirações efetivos e em fases
- Recursos aprimorados de atualização e cancelamento de mensagens
- Suporte do modelo para estruturar mensagens de aviso completas e efetivas
- Criptografia digital e compatibilidade de assinatura
- Recursos de imagens digitais e de áudio

Ocorrências são mensagens de dados autocontidos que podem ser enviadas ou consumidas por todos os componentes. Os eventos podem ser publicados em filas de tópicos e lidos por todos os sistemas de TI de assinatura potencialmente interessados. O CAP ajuda a padronizar o conteúdo da ocorrência de forma que diversos domínios possam enviar e receber ocorrências em um formato comum usando convenções comuns. O padrão define os campos obrigatórios e opcionais no registro da ocorrência e os valores aceitáveis para esses campos. O gerenciamento do processamento de ocorrências pode mediar entre formatos de legado e o formato padronizado. O CAP pode ser estendido para tratar de operações do dia a dia, além de situações de emergência.

No mínimo, as ocorrências devem conter:

- Um identificador de ocorrência exclusivo que contenha:
  - Remetente (sistema ou pessoa)
  - Organização remetente da ocorrência
  - Número de série dentro do sistema remetente
  - Registro de data e hora da criação da ocorrência
- Informações que permitem aos destinatários definir e priorizar respostas:
  - Urgência - rapidez com que os destinatários devem responder ao alerta
  - O nível de ameaça à vida e à propriedade
  - Certeza - valor de probabilidade. Em 100%, significa que a ocorrência foi observada; em 0%, não é esperado que a ocorrência aconteça
  - Horários previstos para ocorrências que podem acontecer futuramente

- A duração de ocorrências relatadas anteriormente e cuja continuação está sendo reportada
- Duração prevista das ocorrências que representam uma situação que não pode ser corrigida rapidamente
- Ações e diretivas recomendadas e obrigatórias
- Informações que permitem que a ocorrência seja correlacionada:
  - Referências ao modelo de semântica da cidade (caso exista)
  - Coordenadas geoespaciais
  - Referência à ocorrência de pré-requisito ou a uma ocorrência que foi a causa precipitadora
  - Identificadores exclusivos de recursos para todos os envolvidos
- Descrições em texto legível
  - Descrição do local
  - Descrição da atividade

O uso do CAP ajuda a minimizar a troca de dados por ocorrência. Como as ocorrências são formatadas em XML, o formato de dados pode ser gravado e lido por vários sistemas, evitando assim a troca de dados insignificantes ou dados que criem confusão perigosa.

O IBM Intelligent Operations Center fornece armazenamento persistente de alertas CAP e uma interface padrão para apresentá-los.

Apesar de toda a estrutura CAP ser aceita pelo IBM Intelligent Operations Center, somente alguns dados são usados pelo IBM Intelligent Operations Center ao calcular indicadores chaves de desempenho (KPI).

O IBM Intelligent Operations Center usa o WebSphere Message Broker para integrar ocorrências usando o CAP.

O IBM Intelligent Operations Center suporta o OASIS Protocolo de Alerta Comum Versão 1.2.

#### **Conceitos relacionados**

“Utilizando CAP para Ocorrências KPI” na página 53

O WebSphere Message Broker, que é fornecido como parte do IBM Intelligent Operations Center, aceita mensagens de ocorrências CAP e usa os dados em cálculos de indicadores-chave de desempenho (KPIs).

“Usando o CAP para Eventos não KPI” na página 55

Dados CAP também podem ser usados para fornecerem dados sobre ocorrências não associadas aos cálculos de KPI.

“Configurando o IBM Intelligent Operations Center para Receber Ocorrências” na página 85

Mensagens de filas de ocorrências externas são recebidas pelo IBM Intelligent Operations Center em uma fila de entrada. As mensagens devem seguir o Common Alerting Protocol.

#### **Informações relacionadas**

 OASIS Common Alerting Protocol Versão 1.2

#### **Estrutura CAP**

Cada mensagem de alerta CAP consiste em um segmento <alert> que pode conter um ou mais segmentos <info>. Cada segmento <info> pode incluir um ou mais

segmentos <area>. Na maioria dos casos, as mensagens do CAP com <msgType> com valor *alert* incluem pelo menos um elemento <info>.

Os itens a seguir são elementos de mensagem principais.

- <alert>  
O segmento <alert> oferece informações básicas sobre a mensagem atual: seu propósito, sua origem e seu status. Ele também possui um identificador exclusivo para a mensagem e links para quaisquer outras mensagens relacionadas. Um segmento <alert> pode ser usado por si só para confirmação e cancelamento de mensagens ou outras funções de sistema; no entanto, a maioria dos segmentos de alerta incluem pelo menos um segmento <info>.
- <info>  
O segmento <info> descreve uma ocorrência prevista ou real de acordo com sua urgência (tempo disponível para preparação), gravidade (intensidade do impacto) e certeza (confiança na observação ou previsão). Ele também oferece descrições em categorias e texto da ocorrência em questão. O segmento <info> também pode fornecer instruções para resposta apropriada pelos destinatários da mensagem, além de outros detalhes, como por exemplo duração do risco, parâmetros técnicos, informações de contato e links a fontes de informação adicionais. Use diversos segmentos <info> para descrever parâmetros diferentes, como diferentes faixas de probabilidade ou intensidade ou para fornecer as informações em diversos idiomas.
- <resource>  
O segmento <resource> oferece uma referência opcional em relação as informações adicionais relacionadas ao segmento <info>. Ele pode indicar um ativo digital, tal como uma imagem ou um arquivo de áudio.
- <area>  
O segmento <area> descreve uma área geográfica ao qual o segmento <info> se aplica. Descrições em texto e em código (como códigos postais) são suportadas, mas as representações ideais usam formas geoespaciais, polígonos e círculos, além de uma altitude ou intervalo de altitude expresso em termos padrão de latitude, longitude e altitude, de acordo com os dados geoespaciais especificados.

### Conceitos relacionados

“Utilizando CAP para Ocorrências KPI” na página 53

O WebSphere Message Broker, que é fornecido como parte do IBM Intelligent Operations Center, aceita mensagens de ocorrências CAP e usa os dados em cálculos de indicadores-chave de desempenho (KPIs).

“Usando o CAP para Eventos não KPI” na página 55

Dados CAP também podem ser usados para fornecerem dados sobre ocorrências não associadas aos cálculos de KPI.

### Tipos de Ocorrência

Diversos tipos de ocorrências CAP são suportadas pelo IBM Intelligent Operations Center.

### Ocorrência Real/Prevista

Essas mensagens são mensagens não solicitadas enviadas por vários domínios sobre condições anormais ou exceções. Essas mensagens também abordam violações de key performance indicator (KPI) onde uma ocorrência foi criada.

## Confirmação

Uma confirmação é uma mensagem CAP com os seguintes valores de campo no elemento <alerta>:

- O valor <msgType> está configurado como **ACK** que significa que o remetente confirma o recebimento e aceitação da mensagem identificada em <references>.
- O campo <references> contém os identificadores de mensagem estendidos (no formato sender, identifier, sent) e uma mensagem ou mensagens CAP indicadas pela confirmação.

•

**Nota:** O elemento <info> é opcional para uma confirmação.

## Aconselhamento

Um aconselhamento é uma mensagem CAP com os seguintes valores de campo no elemento <alert>:

- O valor de <msgType> é **Alert**.
- Valor de <note> é **Advisory**.
- O elemento <references> deve conter os identificadores da mensagem CAP pai (causa-raiz) da ocorrência.

Por exemplo, quando a empresa de distribuição de água receber uma previsão de **Chuvvas Fortes** do departamento de meteorologia, a empresa de distribuição de água distribui um alerta de **Aconselhamento para Enchentes** para todos os outros domínios. Neste caso, **Chuvvas Fortes** é o pai de **Aconselhamento para Enchentes**.

## Resposta

Uma resposta é uma mensagem CAP com os seguintes valores de campo no elemento <alert>:

- O valor de <msgType> é **Alert**.
- Valor de <note> é **Response**.
- O elemento <references> deve conter os identificadores da mensagem CAP para a qual esta é uma resposta

Por exemplo, quando um operador da cidade enviar **Aconselhamento para Indisponibilidade de Energia na Cidade** para vários domínios, esses domínios enviam uma resposta de volta para o aconselhamento após realizar uma análise de impacto em suas funções individuais.

## Diretiva

Uma diretiva é semelhante ao aconselhamento; no entanto, seu elemento <info> inclui um <eventCode> que traz informações sobre as ações a serem tomadas pelo domínio remoto.

A diretiva é uma mensagem CAP com os seguintes valores de campo no elemento <alert>:

- O valor de <msgType> é **Alert**.
- O valor <note> é **Directive**.
- O elemento <references> deve conter os identificadores da mensagem CAP pai (causa-raiz) desta ocorrência. Este campo é opcional. Caso um valor seja

especificado, ele determina o relacionamento entre as ocorrências e as diretivas emitidas que correspondam a essas ocorrências.

- O elemento <instruction> é obrigatório para diretivas. Ele deve conter uma ação recomendada, solicitada ou obrigatória que deve ser tomada pelo destinatário da diretiva.

## Incidente

Incidentes são usados para intercalar diversas mensagens referentes aos diferentes aspectos do mesmo incidente. Mensagens de incidente do CAP agem como um contêiner de todas as ocorrências relacionadas a um incidente específico. Essas ocorrências podem estar presentes em diferentes domínios.

Um aconselhamento é promovido a incidente quando domínios retornam respostas sobre o aconselhamento, indicando impactos em diversos domínios, exigindo ações coordenadas. O elemento <incident> em todas as ocorrências relacionadas são preenchidos com o valor <identifier> da ocorrência do incidente. Ocorrências relacionadas são aquelas em que o valor <references> é o mesmo que o valor <identifier> da ocorrência de incidente.

Um incidente é uma mensagem CAP com os seguintes valores de campo em <alert>:

- O valor de <msgType> é **Alert**.
- O valor de <note> é **Incident**.
- O elemento <references> deve conter os identificadores da mensagem CAP pai (causa-raiz) desta ocorrência
- O elemento <incidents> deve conter seu próprio identificador

## Atualização

Uma atualização consiste em uma mensagem CAP com os seguintes valores de campo no elemento <alert>:

- O elemento <msgType> está configurado como **update**, o que significa que esta atualização suplanta as mensagens anteriores identificadas no elemento <references>.
- O elemento <references> contém os identificadores de mensagem estendidos (no formato sender, identifier, sent) e uma mensagem ou mensagens CAP indicadas pela atualização.

## Cancelar

Um cancelamento é uma mensagem CAP com os seguintes valores de campo no elemento <alert>:

- O elemento <msgType> está configurado como **Cancel**, o que significa que esta mensagem cancela as mensagens anteriores identificadas no elemento <references>.
- O elemento <references> contém os identificadores de mensagem estendidos (no formato sender, identifier, sent) e uma mensagem ou mensagens CAP indicadas pelo cancelamento.
- O elemento <note> contém uma explicação sobre o motivo ou maneira com que este alerta foi cancelado.



## Fechar

Fechar é uma mensagem CAP com os seguintes valores de campo no elemento <alert>:

- O elemento <msgType> está configurado como **Update**.
- O elemento <note> está configurado como **Close**.
- O elemento <references> contém os identificadores de mensagem estendidos (no formato sender, identifier, sent) e uma mensagem ou mensagens CAP que devem ser fechadas.

### Informações relacionadas

 OASIS Common Alerting Protocol Versão 1.2

## Utilizando CAP para Ocorrências KPI

O WebSphere Message Broker, que é fornecido como parte do IBM Intelligent Operations Center, aceita mensagens de ocorrências CAP e usa os dados em cálculos de indicadores-chave de desempenho (KPIs).

A Tabela 15 lista os elementos de dados utilizados em cálculos de KPI:

Tabela 15. Elementos CAP Usados em Cálculos de KPIs no IBM Intelligent Operations Center

Necessário ou Opcional	Elemento de Dados (normativo)	Descrição
Necessário	Message_ID (identificador)	Identificador exclusivo da mensagem
Necessário	Sender_ID (remetente)	Identificador exclusivo do remetente
Necessário	SentDateTime (enviado)	Data e hora da ocorrência Por exemplo: 2011-02-07T 16:49:00-05:00
Necessário	MessageStatus (status)	Um dos seguintes valores: <ul style="list-style-type: none"><li>• Real</li><li>• Exercício</li><li>• Sistema</li><li>• Teste</li><li>• Rascunho</li></ul>
Necessário	MessageType (tipo mensagem)	Um dos seguintes valores: <ul style="list-style-type: none"><li>• Alerta</li><li>• Atualização</li><li>• Cancelar</li><li>• Confirmação</li><li>• Erro</li></ul>
Opcional	Source (origem)	Origem da mensagem
Necessário	Scope (escopo)	Contém o valor Público
Necessário	Code (código)	Contém o KPI de valor para ocultar essa ocorrência da lista do portlet Ocorrências.

Tabela 15. Elementos CAP Usados em Cálculos de KPIs no IBM Intelligent Operations Center (continuação)

Necessário ou Opcional	Elemento de Dados (normativo)	Descrição
Necessário	EventCategory (categoria)	Um dos seguintes valores: <ul style="list-style-type: none"> <li>• Geo</li> <li>• Met</li> <li>• Proteção</li> <li>• Segurança</li> <li>• Resgate</li> <li>• Incêndio</li> <li>• Saúde</li> <li>• Amb</li> <li>• Transport</li> <li>• Infra</li> <li>• CBRNE</li> <li>• Outro</li> </ul>
Necessário	EventType (ocorrência)	Descrição da ocorrência. Por exemplo: Police_Department_Budget
Necessário	Urgency (urgência)	Um dos seguintes valores: <ul style="list-style-type: none"> <li>• Imediato</li> <li>• Esperado</li> <li>• Futuro</li> <li>• Passado</li> <li>• Desconhecido</li> </ul>
Necessário	Severity (gravidade)	Um dos seguintes valores: <ul style="list-style-type: none"> <li>• Extrema</li> <li>• Grave</li> <li>• Moderado</li> <li>• Baixa</li> <li>• Desconhecido</li> </ul>
Necessário	Certainty (certeza)	Um dos seguintes valores: <ul style="list-style-type: none"> <li>• Observada</li> <li>• Provável</li> <li>• Possível</li> <li>• Improvável</li> <li>• Desconhecido</li> </ul>
Opcional	EventCode (código ocorrência)	Pares de valores de nome para definir o tipo de ocorrência.
Opcional	OnsetDateType (início)	Data e hora de início da ocorrência. Por exemplo: 2011-02-08T16:49:00-05:00
Opcional	SenderName (nome do remetente)	Nome da entidade que iniciou o alerta. Por exemplo: Departamento de Polícia
Opcional	EventDescription (descrição)	Descrição detalhada da ocorrência
Opcional	Parameter (parâmetro)	Dados adicionais associados à ocorrência.

Tabela 15. Elementos CAP Usados em Cálculos de KPIs no IBM Intelligent Operations Center (continuação)

Necessário ou Opcional	Elemento de Dados (normativo)	Descrição
Opcional	AreaGeocode (código geográfico)	Campo que pode ser usado para fornecer informações quando o KPI depender de informações de local

Para obter informações adicionais, consulte a especificação OASIS do Protocolo de Alerta Comum

O exemplo a seguir é uma ocorrência relatando um acidente de carro.

```
<?xml version="1.0" encoding="UTF-8"?>
<cap:alert xmlns:cap="urn:oasis:names:tc:emergency:cap:1.2"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="urn:oasis:names:tc:emergency:cap:1.2 CAP-v1.2-os.xsd ">
  <cap:identifier>1112</cap:identifier>
  <cap:sender>Transporte</cap:sender>
  <cap:sent>2011-02-17T15:00:00-05:00</cap:sent>
  <cap:status>Real</cap:status>
  <cap:msgType>Alerta</cap:msgType>
  <cap:scope>Público</cap:scope>
  <cap:code>KPI</cap:code>
  <cap:info>
    <cap:category>Transporte</cap:category>
    <cap:event>Traffic_Accident</cap:event>
    <cap:urgency>Desconhecido</cap:urgency>
    <cap:severity>Extrema</cap:severity>
    <cap:certainty>Desconhecida</cap:certainty>
    <cap:eventCode>
      <cap:valueName>OwningOrg</cap:valueName>
      <cap:value>Polícia</cap:value>
    </cap:eventCode>
    <cap:onset>2011-02-17T15:00:00-05:00</cap:onset>
    <cap:senderName>Transporte</cap:senderName>
    <cap:description>Colisão de um único carro</cap:description>
    <cap:parameter>
      <cap:valueName>accident number</cap:valueName>
      <cap:value>1112</cap:value>
    </cap:parameter>
  </cap:info>
</cap:alert>
```

#### Informações relacionadas

 [OASIS Common Alerting Protocol Versão 1.2](#)

### Usando o CAP para Eventos não KPI

Dados CAP também podem ser usados para fornecerem dados sobre ocorrências não associadas aos cálculos de KPI.

Dados CAP recebidos pelo IBM Intelligent Operations Center não associados a KPIs definidos serão incluídos nos portlets Ocorrências e Mapa no IBM Intelligent Operations Center.

## Integrando a outros Protocolos

Produtos e serviços que não suportam o Protocolo de Alerta Comum (CAP) podem ser integrados ao IBM Intelligent Operations Center.

Para integração com o IBM Intelligent Operations Center usando outros protocolos, um adaptador deve ser gravado para converter esses protocolos no CAP.

---

## Publicando Mensagens CAP

O IBM Intelligent Operations Center fornece o portlet Publicador de Amostras como ferramenta de teste automatizado, além de oferecer recursos de publicação adicional como serviço.

Além do IBM Intelligent Operations Center, existem dois níveis de serviço fornecidos com o IBM Intelligent Operations Center:

- Servlet de Publicador
- Classe do utilitário de Publicador

## Usando a Fila de Ocorrências de Entrada Definida para o IBM Intelligent Operations Center

Ocorrências CAP podem ser publicadas no IBM Intelligent Operations Center direcionando as mesmas à instância do WebSphere Message Broker incluída.

Clientes de publicação podem ser configurados para apontarem diretamente para a fila de entrada de ocorrências CAP do WebSphere Message Broker ou podem usar os recursos JMS do WebSphere Application Server definidos no servidor de portal. Esses recursos JMS apontam para a fila do WebSphere Message Broker que recebe ocorrências CAP. Os recursos JMS são criados quando o IBM Intelligent Operations Center é instalado. Os recursos são:

Queue Connection Factory  
Name: ioc.mb.con.factory  
JNDI Name: jms/ioc.mb.con.factory

Queue  
Name: ioc.cap.in.q  
JNDI Name: jms/ioc.cap.in.q

### Conceitos relacionados

“Configurando o IBM Intelligent Operations Center para Receber Ocorrências” na página 85

Mensagens de filas de ocorrências externas são recebidas pelo IBM Intelligent Operations Center em uma fila de entrada. As mensagens devem seguir o Common Alerting Protocol.

## Publicador de Amostras

Use o portlet Publicador de Amostras para publicar ocorrências Common Alerting Protocol (CAP) no IBM Intelligent Operations Center.

### O que é o Portlet Publicador de Amostras?

O portlet Publicador de Amostras é uma ferramenta de teste automatizada destinada a um administrador que gerencia ou verifica a solução. Funciona como um aplicativo cliente para testar a publicação de mensagens CAP no IBM Intelligent Operations Center. O portlet Publicador de Amostras pode eliminar o requisito para criar manualmente um aplicativo cliente de teste.

## O que o portlet Publicador de Amostras exibe?

Na guia **Ocorrências de Amostra** do portlet Publicador de Amostras você poderá preencher um formulário para projetar ocorrências com XML. Envie o formulário para ativar um fluxo de ocorrências CAP de amostra no sistema.

O portlet Publicador de Amostras também contém uma guia **Nova Ocorrência** para criar novas ocorrências quando não for necessário editar o XML. Preencha o formulário na guia **Nova Ocorrência** para enviar os detalhes da ocorrência CAP. Se quiser criar novas ocorrências com propriedades com base nas propriedades de uma ocorrência existente, insira o ID para a ocorrência existente no campo **ID do Alerta CAP**.

O portlet Publicador de Amostras contém uma guia **Notificações** para testar o subsistema de notificações do IBM Intelligent Operations Center. Na guia **Notificações**, é possível preencher um formulário para enviar uma notificação de alerta para grupos especificados. O campo **Enviar ao Grupo** deve corresponder um dos grupos de usuários existentes, por exemplo, CitywideExecutives, porque somente alertas correspondentes são exibidos na lista de portlets Coordenador - Alertas.

## Valores Aleatórios

Na guia **Ocorrências de Amostra**, se você selecionar a caixa de seleção **Escolher Ocorrências a Esmo**, o portlet altera automaticamente as propriedades das ocorrências que publica da seguinte forma:

- **ID:** O portlet gera uma sequência de ID exclusiva para cada ocorrência, pois os IDs de ocorrência devem ser exclusivos no IBM Intelligent Operations Center.
- **Registro de data e hora:** O portlet incrementa o valor do registro de data e hora para cada ocorrência enviada para que cada ocorrência na sequência seja recebida em horários diferentes.
- **Local:** O portlet escolhe a latitude e longitude a esmo para cada ocorrência, dentro de uma faixa, para estar em conformidade com o formato necessário para latitude, longitude e raio; por exemplo, 32.9525,-115.5527 5. A configuração do raio não é alterada.

## Criando Ocorrências de Amostra com XML

Na guia **Ocorrências de Amostra**, é possível selecionar um modelo de ocorrência CAP de amostra que é possível usar para visualizar, modificar e publicar ocorrências.

## Sobre Esta Tarefa

Inicialmente, escolha uma categoria de ocorrência. As categorias representam as áreas principais nas quais as ocorrências estão divididas.

Tabela 16. Categorias de Evento

Categoria	Descrição
CBRNE	Ameaça ou ataque químico, biológico, radiológico, nuclear ou explosivo de grande dimensão
Ambiental	Poluição e outra ocorrência ambiental
Incêndio	Supressão de incêndio e resgate
Geográfico	Ocorrência geofísica, incluindo desmoronamento de terras

Tabela 16. *Categorias de Evento (continuação)*

<b>Categoria</b>	<b>Descrição</b>
Saúde	Ocorrência médica e de saúde pública
Infraestrutura	Utilidade pública, telecomunicação ou outra ocorrência de infraestrutura não de transporte
Meteorológico	Ocorrência meteorológica, incluindo inundação
Resgate	Resgate e recuperação
Proteção	Emergência geral e segurança pública
Segurança	Cumprimento da lei, segurança local/privada, da pátria e militar
Transporte	Transporte público e privado
Outro	Outras ocorrências

### **Procedimento**

1. Clique na guia **Ocorrências de Amostra**.
2. Na lista **Categoria**, selecione uma categoria de ocorrência.
3. Na lista **Ocorrência de Amostra**, selecione uma ocorrência. No campo **Mensagem de Ocorrência**, o XML para a mensagem CAP pré-gravada correspondente é inserida automaticamente.
4. Como opção, no campo **Mensagem de Ocorrência**, edite o XML para a mensagem CAP pré-gravada.
5. No campo **Contagem de Instâncias de Ocorrências**, selecione o número de mensagens necessárias. É possível enviar uma única mensagem CAP ou uma sequência de mensagens automatizadas.
6. Como opção, selecione a caixa de seleção **Escolher Ocorrências a Esmo**. Se você selecionar **Escolher Ocorrências a Esmo**, quando uma sequência de mensagens CAP for publicada, determinadas propriedades têm valores aleatórios designados automaticamente.
7. Clique em **Enviar Ocorrência**.

### **Resultados**

O Publicador de Amostras preenche o IBM Intelligent Operations Center com ocorrências e pode acionar KPIs.

### **Criando Novas Ocorrências CAP sem XML**

Na guia **Nova Ocorrência**, é possível preencher um formulário para criar novas ocorrências CAP sem usar XML.

### **Sobre Esta Tarefa**

É possível usar o formulário para criar uma nova ocorrência ou uma ocorrência baseada nos valores de uma ocorrência existente. Ao criar uma ocorrência baseada em uma ocorrência existente, você usa o valor do Identificador CAP para fazer referência à ocorrência existente. Se não souber o valor do Identificador CAP para uma ocorrência existente, é possível usar o valor do Incidente em seu lugar. Quaisquer valores inseridos no formulário substituem os valores da ocorrência CAP existente.

### **Procedimento**

1. Clique na guia **Nova Ocorrência**.

2. Para especificar uma origem para a ocorrência, ao lado de Origem, clique em uma das seguintes opções:
  - Para criar uma nova ocorrência com valores baseados nos valores inseridos no formulário, clique em **Novo**.
  - Para criar uma ocorrência com valores baseados em uma ocorrência existente na tabela de ocorrências CAP e usar o Identificador CAP, clique em **Existente**.
  - Para criar uma ocorrência com valores baseados em uma ocorrência existente na tabela de ocorrências CAP e usar o valor do Incidente, clique em **Incidente**.
3. No campo **ID**, insira um ID dependendo de se você está criando uma nova ocorrência ou uma ocorrência existente baseada no valor do Identificador CAP ou do Incidente:
  - Se estiver criando uma nova ocorrência, como opção insira um valor para **ID**. Se você não inserir um valor, um identificador exclusivo é gerado.
  - Se estiver criando uma ocorrência baseada em um valor de Identificador CAP existente, insira o valor do Identificador CAP para **ID**. Quaisquer valores inseridos no formulário substituem os valores da ocorrência CAP existente.
  - Se estiver criando uma ocorrência baseada em um valor de Incidente existente, insira o valor do Incidente para **ID**. Quaisquer valores inseridos no formulário substituem os valores da ocorrência CAP existente.
4. No campo **Título**, insira um título.
5. Na lista **Categoria**, selecione uma categoria.
6. Na lista **Urgência**, selecione a urgência.
7. Na lista **Gravidade**, selecione a gravidade.
8. Na lista **Certeza**, selecione a certeza.
9. No campo **Descrição**, insira uma descrição.
10. No campo **Remetente**, insira uma descrição do remetente da ocorrência.
11. No campo **Contagem de Instâncias de Ocorrências**, selecione o número de mensagens necessárias. É possível enviar uma única mensagem CAP ou uma sequência de mensagens automatizadas.
12. Como opção, selecione a caixa de seleção **Escolher Ocorrências a Esmo**. Se você selecionar **Escolher Ocorrências a Esmo**, quando uma sequência de mensagens CAP for publicada, determinadas propriedades têm valores aleatórios designados automaticamente.
13. Clique em **Enviar Ocorrência**.

## Testando Notificações

É possível usar a guia **Nova Notificação** para criar notificações de teste para testar o subsistema de notificações no IBM Intelligent Operations Center.

## Sobre Esta Tarefa

Na guia **Nova Notificação**, preencha o formulário para enviar um alerta para grupos especificados. Assegure que um dos valores inseridos no campo **Enviado a Grupos** corresponda a um dos grupos dos quais você é membro, por exemplo, Executivos de Toda a Cidade ou Operadores de Toda a Cidade. A razão para isso é que somente alertas correspondentes sejam exibidos na lista de portlets Coordenador - Alertas da Cidade. Ao criar um alerta na guia **Nova Notificação**, o serviço Publicador não é usado. Em vez disso, o novo alerta é gravado diretamente

na tabela NOTIFICATION e a lista de portlets Coordenador - Alertas da Cidade é notificada para se atualizar.

### Procedimento

1. Clique na guia **Nova Notificação**.
2. Para criar um alerta, na lista **Tipo**, selecione **Alerta**.
3. Como opção, na lista **Categoria**, selecione uma categoria.
4. Como opção, no campo **Título**, insira um título.
5. Como opção, no campo **Descrição**, insira uma descrição.
6. Como opção, no campo **Remetente**, insira uma descrição do remetente da ocorrência.
7. Como opção, no campo **Enviado para Grupos**, insira uma lista de grupos separada por ponto e vírgula para os quais enviar o alerta.
8. Como opção, execute uma das etapas conforme necessário:
  - No campo **Refere-se a Alertas**, insira uma lista de identificadores de ocorrências CAP separada por ponto e vírgula aos quais o novo alerta se refere.
  - No campo **Refere-se a KPIs**, insira uma lista de KPIs separada por ponto e vírgula aos quais o novo alerta se refere.
9. Clique em **Enviar Notificação**.

---

## Customizando KPIs

Indicadores chaves de desempenho (KPIs) podem ser criados e modificados usando o IBM Business Monitor e o IBM Business Monitor Development Toolkit.

Este centro de informações descreve como criar e modificar KPIs para usar com o IBM Intelligent Operations Center usando o Kit de Ferramentas de Desenvolvimento do IBM Business Monitor. O Kit de Ferramentas de Desenvolvimento do IBM Business Monitor pode ser instalado com o Rational Application Developer, que também é fornecido com o IBM Intelligent Operations Center. O IBM Business Monitor Development Toolkit também pode ser instalado com o WebSphere Integration Developer.

Antes de definir ou modificar um KPI, você deve entender o alerta Protocolo de Alerta Comum (CAP) no qual o KPI será baseado. Por exemplo, se estiver definindo o KPI de rastreamento de uma fonte de água, será necessário conhecer os elementos do CAP que contêm os elementos que precisam ser rastreados, como o nome da fonte da água e a profundidade da água em pés.

Após um KPI ser incluído ou modificado, ele deve ser implementado no servidor do IBM Business Monitor.

Para obter informações adicionais sobre a utilização do IBM Business Monitor e do IBM Business Monitor Development Toolkit, consulte o centro de informações do IBM Business Monitor.



### **Conceitos relacionados**

“KPIs de Amostra” na página 73

KPIs de amostra são fornecidos com o IBM Intelligent Operations Center. Esses KPIs são projetados para fornecer orientação para implementação de diferentes tipos de KPIs usando o Kit de Ferramentas de Desenvolvimento do IBM Business Monitor. Modelos de monitor de amostra são fornecidos para proteção de água, transporte e pública.

“Criando KPIs para Uso com o IBM Intelligent Operations Center” na página 84 Indicadores Chaves de Desempenho (KPIs) são tratados por ocorrências dentro do IBM Intelligent Operations Center. Eles são usados para direcionar dados estatísticos que podem ser usados para analisar tendências ou para indicar áreas problemáticas.

### **Tarefas relacionadas**

“Implementando Modelos de Monitor” na página 71

Após definir indicadores chaves de desempenho (KPIs) e seus modelos de monitor, os modelos de monitor precisam ser implementados no IBM Business Monitor em execução no servidor analítico do IBM Intelligent Operations Center.

### **Referências relacionadas**

“Instalando Ferramentas Fornecidas com a Solução” na página 21

Kits de ferramentas e ferramentas de desenvolvimento estão incluídas com o IBM Intelligent Operations Center. Eles são usados na customização do IBM Intelligent Operations Center.

### **Informações relacionadas**

 Centro de Informações do IBM Business Monitor

## **Monitorar Modelos e KPIs**

Um modelo de monitor define métricas e Key Performance Indicators (KPIs), suas dependências em ocorrências recebidas, condições que requerem ações de negócios e ocorrências de saída relatando as condições que podem acionar ações de negócios.

Um modelo de monitor pode conter os seguintes submodelos:

- Modelo de detalhes do monitor
- Modelo de KPI
- Modelo dimensional
- Modelo visual
- Modelo da ocorrência

O modelo de detalhes do monitor contém a maioria das informações do modelo de monitor.

Os modelos de monitor de amostra fornecidos pelo IBM Intelligent Operations Center não usam os modelos visual ou dimensional.

O modelo de detalhes do monitor define um ou mais contextos de monitoramento. Um contexto de monitoramento define as informações a serem coletadas e monitoradas de uma ou mais ocorrências recebidas. Para o IBM Intelligent Operations Center, entidades monitoradas são alertas CAP. As informações coletadas desses alertas são usadas para calcular um KPI.

O modelo de KPI contém um ou mais contextos de KPI. Eles definem os KPIs e seus acionadores e ocorrências associados. Os contextos de KPI podem processar

ocorrências recebidas, avaliar acionamentos de tempo de espera recorrentes e enviar ocorrências de saída. Por exemplo, o contexto pode verificar se um KPI está fora do intervalo definido e enviar uma notificação.

O modelo da ocorrência refere-se a todas as definições de entrada e saída da ocorrência usadas no modelo de monitor. Ele se refere a esquemas que descrevem a estrutura de partes individuais da ocorrência.

#### **Conceitos relacionados**

“KPIs de Amostra” na página 73

KPIs de amostra são fornecidos com o IBM Intelligent Operations Center. Esses KPIs são projetados para fornecer orientação para implementação de diferentes tipos de KPIs usando o Kit de Ferramentas de Desenvolvimento do IBM Business Monitor. Modelos de monitor de amostra são fornecidos para proteção de água, transporte e pública.

#### **Informações relacionadas**

 Centro de Informações do IBM Business Monitor

## **Instâncias do Contexto de Monitoramento**

Uma instância do contexto de monitoramento é informações coletadas em um ponto específico do tempo dentro de um contexto de monitoramento.

Para o IBM Intelligent Operations Center, uma instância do contexto de monitoramento é análoga para um alerta CAP. Quando um alerta CAP for recebido, uma instância do contexto de monitoramento é criada ou reutilizada e as métricas nesse contexto são preenchidas com os valores de alerta CAP baseados no contexto de monitoramento.

Um contexto de monitoramento pode ser definido para criar uma nova instância para cada alerta CAP ou reutilizar uma instância existente. Por exemplo, se desejar que um KPI calcule o nível médio de água, semanalmente, para um determinado recurso, com amostras diárias do nível de água, você criará uma nova instância de contexto do monitor para cada alerta CAP. Cada instância conterá o nível de água diário e o KPI fará a média das medidas pelo período de sete dias.

KPIs são calculadas usando as métricas definidas para um contexto de monitoramento. Ao definir um KPI de agregação, você especifica o contexto de monitoramento e a métrica usada como entrada para a função de agregação de KPI. Quando o KPI é avaliado, os valores de métrica para as instâncias de contexto de monitoramento são usados pela função de agregação para calcular o valor de KPI.

### Conceitos relacionados

“KPIs de Amostra” na página 73

KPIs de amostra são fornecidos com o IBM Intelligent Operations Center. Esses KPIs são projetados para fornecer orientação para implementação de diferentes tipos de KPIs usando o Kit de Ferramentas de Desenvolvimento do IBM Business Monitor. Modelos de monitor de amostra são fornecidos para proteção de água, transporte e pública.

### Informações relacionadas

 Centro de Informações do IBM Business Monitor

## Modelando KPIs

Modele KPIs usando o Rational Application Developer ou o WebSphere Integration Developer com o IBM Business Monitor Developers Toolkit instalado. O Rational Application Developer e o IBM Business Monitor Developers Toolkit são incluídos como parte do IBM Intelligent Operations Center.

### Sobre Esta Tarefa

KPIs são modeladas usando o Rational Application Developer ou o WebSphere Integration Developer com o IBM Business Monitor Developers Toolkit. Para obter mais informações sobre o uso dessas ferramentas, consulte os centros de informações para esses produtos.

Modelos de monitoramento podem ser encontrados nos projetos de monitoramento de negócios. Modelos e projetos são criados utilizando os assistentes de monitoramento de negócios do Rational Application Developer fornecidos pelo IBM Business Monitor Developers Toolkit.

Para realizar a modelagem do KPI, execute as etapas a seguir.

### Procedimento

1. Entenda o alerta CAP a ser recebido pelo IBM Intelligent Operations Center.
2. Compreenda o propósito do KPI. O KPI irá gerar uma ação caso um limite seja atingido ou ultrapassado? O KPI será utilizado para calcular dados históricos ou estatísticos?
3. Determine o nome para o contexto de monitoramento. A convenção de nomenclatura do IBM Intelligent Operations Center consiste em usar o tipo de ocorrência CAP como nome. As amostras fornecidas pelo IBM Intelligent Operations Center criam contextos de monitoramento separados para cada mensagem de alerta CAP enviada ao IBM Business Monitor.
4. No Rational Application Developer com o IBM Business Monitor Developers Toolkit instalado, defina a ocorrência recebida, chave e conjunto de métricas para o contexto do monitor. A ocorrência recebida define a mensagem de alerta CAP monitorada pelo contexto, uma chave que define a instância de contexto de maneira exclusiva e as métricas que definem as informações extraídas da mensagem de alerta CAP.
5. Especifique o esquema CAP da ocorrência. O esquema deve existir no projeto de monitoramento. O IBM Intelligent Operations Center fornece uma cópia do esquema CAP v1.2 no projeto de modelagem `icoc_sample_monitor_models` de amostra.
6. Especifique o nome e ID para cada ocorrência recebida do monitor de negócios. IDs de ocorrências não podem conter espaços ou caracteres especiais. Por padrão, o ID é criado a partir do nome com sublinhados em vez

de espaços em branco. Todas as amostras fornecidas pelo IBM Intelligent Operations Center usam IDs de elemento padrão.

7. Especifique o esquema. O esquema define a estrutura da ocorrência recebida para o IBM Business Monitor.
8. Defina os filtros desejados para as mensagens CAP. Por exemplo, limite o monitoramento a tipos ou gravidades específicas das ocorrências.
9. Especifique as métricas a serem extraídas da mensagem CAP.
10. Defina uma chave de contexto que identificará a instância do contexto de monitoramento de maneira exclusiva. Valores da chave são especificados pela ocorrência recebida quando o contexto de monitoramento é criado.
11. Especifique se as ocorrências recebidas devem ser correlacionadas.
12. Especifique o contexto KPI. Um contexto KPI é um contêiner para KPIs e seus acionadores e ocorrências associados. Diferentemente de um contexto de monitoramento, um contexto KPI não contém chaves ou métricas. Um contexto KPI deve ser criado como um contêiner antes de criar quaisquer KPIs.
13. Crie o KPI no contexto de KPI definido anteriormente.
14. Especifique o tipo de KPI: **Decimal** ou **Duração**.
15. Defina as faixas, valores e indicadores de cor de KPI. A maioria dos KPIs de amostra do IBM Intelligent Operations Center define, três faixas e cores associadas.

*Tabela 17. Definições de Faixa e de Cor de KPI de Amostra*

Nome	Cor	RGB
aceitável	verde	e4f2d1
atenção	amarelo	fee881
tomar medidas	vermelho	e68b88

16. Defina como o valor de KPI é calculado. Os valores de KPI são determinados em uma de duas maneiras. Se o valor vier de uma métrica usando uma função de agregação, o KPI é referido como um KPI de agregação. Se o valor for calculado com base em outros KPIs ou em funções XPath definidas pelo usuário, o KPI é referido como um KPI de expressão.

Nas amostras do IBM Intelligent Operations Center, os KPIs de nível mais baixo (aqueles sem filhos) são definidos como KPIs de agregação. Os KPIs de nível superior (KPIs com filhos) são definidos como KPIs de expressão.

Os valores de KPIs de agregação são calculados a partir de métricas preenchidas com dados enviados nas mensagens de alerta CAP enviadas ao servidor do IBM Business Monitor. Uma função de agregação é então executada nesses dados. As funções de agregação incluem:

- average
- maximum
- minimum
- sum
- number of occurrences
- standard deviation

Os valores são expressos como medidas quantificáveis. Por exemplo, tempo de resposta médio a crime (5 minutos, 7 segundos) ou nível médio de água (100,5).

Os valores de KPI de expressão são calculados a partir de faixas e cálculos de KPI. Nas amostras do IBM Intelligent Operations Center, os KPIs pai têm cálculos que fazem com que o KPI seja avaliado para um valor igual a 0, 1 ou 2, dependendo dos valores de seus KPIs filhos. Um valor igual a 0 é mapeado para a faixa aceitável, 1 para a faixa de cuidado e 2 para a faixa de agir. As amostras usam expressões de cálculos para configurar o valor de KPI para a urgência mais alta de seus filhos.

17. Opcional: Especifique o filtro de tempo para um KPI de agregação. Os KPIs de agregação podem ter filtros de tempo opcionais que limitam o período de tempo durante o qual o valor de KPI é calculado. O período de tempo pode ser um intervalo de repetição (por exemplo, o último período concluído ou atual), um intervalo de rolagem ou um intervalo fixo. Todos os KPIs de agregação de amostra do IBM Intelligent Operations Center definiram filtros de tempo.
18. Opcional: Especifique um filtro de dados para o KPI. Por exemplo, se o tempo de resposta médio a crime for ser calculado para a Delegacia de Polícia Um e nenhuma outra delegacia, um filtro de dados pode ser usado para remover todos os outros contextos de monitoramento.
19. Defina como os valores de KPI são atualizados, incluindo acionadores, ocorrências inseridas no servidor do IBM Business Monitor e ocorrências de saída do IBM Intelligent Operations Center.
20. Teste o KPI.
21. Implemente o aplicativo de modelo de monitor.

## Conceitos relacionados

“KPIs aninhados”

Apesar de o IBM Business Monitor permite um KPI baseado no valor de outro KPI, ele não permite a definição de um relacionamento pai/filho entre KPIs. A definição de relacionamentos pai/filho deve ser feita no IBM Intelligent Operations Center.

“KPIs de Amostra” na página 73

KPIs de amostra são fornecidos com o IBM Intelligent Operations Center. Esses KPIs são projetados para fornecer orientação para implementação de diferentes tipos de KPIs usando o Kit de Ferramentas de Desenvolvimento do IBM Business Monitor. Modelos de monitor de amostra são fornecidos para proteção de água, transporte e pública.

“Comunicação de Ocorrência de KPI entre o IBM Business Monitor e o IBM Intelligent Operations Center” na página 67

O IBM Business Monitor pode enviar ocorrências de saída de um contexto de monitoramento ou de indicador chave de desempenho (KPI) ao IBM Intelligent Operations Center.

## Tarefas relacionadas

“Implementando Modelos de Monitor” na página 71

Após definir indicadores chaves de desempenho (KPIs) e seus modelos de monitor, os modelos de monitor precisam ser implementados no IBM Business Monitor em execução no servidor analítico do IBM Intelligent Operations Center.

## Referências relacionadas

“Instalando Ferramentas Fornecidas com a Solução” na página 21

Kits de ferramentas e ferramentas de desenvolvimento estão incluídas com o IBM Intelligent Operations Center. Eles são usados na customização do IBM Intelligent Operations Center.

## Informações relacionadas

 Centro de Informações do IBM Business Monitor

 Centro de Informações do Rational Application Developer

 XML Path Language (XPath) 2.0 (Segunda Edição)

## KPIs aninhados

Apesar de o IBM Business Monitor permite um KPI baseado no valor de outro KPI, ele não permite a definição de um relacionamento pai/filho entre KPIs. A definição de relacionamentos pai/filho deve ser feita no IBM Intelligent Operations Center.

Os KPIs de amostra do IBM Intelligent Operations Center definem uma série de KPIs Police Department.

```
Police Department ----- level 1
  Crime Response Time ----- level 2
    Crime Response Time Precinct One ----- level 3
    Crime Response Time Precinct Two ----- level 3
```

Nesse caso, Police Department tem um filho: Crime Response Time. Crime Response Time tem dois filhos: Crime Response Time Precinct One e Crime Response Time Precinct Two.

Os dois KPIs de nível 3 são definidos como KPIs de agregação. Ou seja, seus valores são calculados usando um valor métrico e uma função de agregação. Todo

os outros KPIs desse conjunto são KPIs de expressão com seus valores calculados dos valores dos outros KPIs. Por exemplo:

- Crime Response Time é baseado nos valores de Crime Response Time Precinct One e Crime Response Time Precinct Two.
- Police Department é baseado no valor de Crime Response Time.

#### Conceitos relacionados

“Definindo Relacionamentos Pai/Filho de KPI”

Os relacionamentos pai/filho de KPI são definidos em um documento Web Ontology Language (OWL) que é lido e processado pelo IBM Intelligent Operations Center.

## Definindo Relacionamentos Pai/Filho de KPI

Os relacionamentos pai/filho de KPI são definidos em um documento Web Ontology Language (OWL) que é lido e processado pelo IBM Intelligent Operations Center.

Por exemplo, as definições OWL para o KPI Police Department configuradas são:

```
<icop:KPIDefinition rdf:ID="Police_Department">
<icop:KPIBase.name>Police Department</icop:KPIBase.name>
<icop:KPIBase.id>Police_Department</icop:KPIBase.id>
<icop:KPIDefinition.isChildOf_ModelDefinition
  rdf:resource= "#icoc_sample_public_safety_monitor_model"/>
</icop:KPIDefinition >
```

```
<icop:KPIDefinition rdf:ID="Crime_Response_Time">
<icop:KPIBase.name>Crime Response Time</icop:KPIBase.name>
<icop:KPIBase.id>Crime_Response_Time</icop:KPIBase.id>
<icop:KPIDefinition.isChildOf_KPIDefinition rdf:resource= "#Police_Department"/>
</icop:KPIDefinition >
```

```
<icop:KPIDefinition rdf:ID="Crime_Response_Time_Precinct_One">
<icop:KPIBase.name>Crime Response Time Precinct One</icop:KPIBase.name>
<icop:KPIBase.id>Crime_Response_Time_Precinct_One</icop:KPIBase.id>
<icop:KPIDefinition.isChildOf_KPIDefinition rdf:resource= "#Crime_Response_Time"/>
</icop:KPIDefinition >
```

```
<icop:KPIDefinition rdf:ID="Crime_Response_Time_Precinct_Two">
<icop:KPIBase.name>Crime Response Time Precinct Two</icop:KPIBase.name>
<icop:KPIBase.id>Crime_Response_Time_Precinct_Two</icop:KPIBase.id>
<icop:KPIDefinition.isChildOf_KPIDefinition rdf:resource= "#Crime_Response_Time"/>
</icop:KPIDefinition >
```

#### Conceitos relacionados

“KPIs aninhados” na página 66

Apesar de o IBM Business Monitor permite um KPI baseado no valor de outro KPI, ele não permite a definição de um relacionamento pai/filho entre KPIs. A definição de relacionamentos pai/filho deve ser feita no IBM Intelligent Operations Center.

## Comunicação de Ocorrência de KPI entre o IBM Business Monitor e o IBM Intelligent Operations Center

O IBM Business Monitor pode enviar ocorrências de saída de um contexto de monitoramento ou de indicador chave de desempenho (KPI) ao IBM Intelligent Operations Center.

Ocorrências de saída do servidor do IBM Business Monitor são colocadas em uma fila de mensagens externas. O IBM Intelligent Operations Center usa esse mecanismo para receber atualizações de KPI de forma assíncrona.

## Conceitos relacionados

“Usando a Fila de Ocorrências de Entrada Definida para o IBM Intelligent Operations Center” na página 56  
Ocorrências CAP podem ser publicadas no IBM Intelligent Operations Center direcionando as mesmas à instância do WebSphere Message Broker incluída.

## Acionadores

Um acionador é um mecanismo que detecta uma ocorrência e pode causar processamento adicional em resposta a essa ocorrência.

As amostras de KPI fornecidas com o IBM Intelligent Operations Center definem dois tipos de acionadores. O primeiro acionador é disparado quando uma mensagem de alerta CAP, também conhecida como uma ocorrência de entrada, é recebida pelo servidor do IBM Business Monitor para um conjunto de KPIs definido. A mensagem de alerta CAP pode alterar ou não o KPI. O IBM Intelligent Operations Center determina se o KPI é alterado quando recebe a notificação de ocorrência do servidor do IBM Business Monitor.

Para ocorrências de saída, um acionador determina quando a ocorrência será enviada.

Os acionadores baseados em ocorrências podem ser usados para enviar notificações ao IBM Intelligent Operations Center quando entrada para um cálculo de KPI for alterada. No entanto, os acionadores de ocorrências não podem ser usados para abordar a situação quando um valor de KPI mudar após o vencimento de um período de tempo definido. Nas amostras do IBM Intelligent Operations Center, acionadores baseados em tempo são usados para enviar notificações ao IBM Intelligent Operations Center para esses KPIs com definições de período de tempo curto.

Por exemplo, o Severe Traffic Accidents KPI é definido para expirar a cada hora. Se o KPI tiver um valor igual a 3 às 10h e nenhuma mensagem de alerta CAP for recebida para esse KPI durante a próxima hora, então o período de tempo expira e o valor de KPI é reconfigurado para 0.

## Definindo Ocorrências de Entrada para o IBM Business Monitor

Nas amostras do IBM Intelligent Operations Center, as ocorrências de entrada são usadas para determinar quando um acionador é disparado. Ocorrências de entrada para um contexto KPI são definidas de maneira semelhante às aquelas para um contexto de monitoramento.

## Sobre Esta Tarefa

Ocorrências de entrada são definidas usando o Rational Application Developer ou o WebSphere Integration Developer com o IBM Business Monitor Developers Toolkit. Para obter mais informações sobre o uso dessas ferramentas, consulte os centros de informações para esses produtos.

Para definir uma ocorrência de entrada, faça o seguinte.

## Procedimento

1. Selecione o contexto KPI para a ocorrência de entrada.
2. Crie a ocorrência de entrada e especifique o nome e o ID da ocorrência.
3. Especifique o esquema CAP.
4. Especifique a condição do filtro.



5. Selecione o contexto KPI e crie uma nova ocorrência de entrada.
6. Crie um novo acionador para a ocorrência de entrada.
7. Certifique-se de que o acionador possa ser repetido de forma que o acionador seja disparado toda vez que a fonte acionadora seja atualizada e a condição acionadora seja.
8. Selecione a fonte acionadora.
9. Defina a condição acionadora. Quando a condição acionadora for atendida, o acionador será disparado.

## Exemplo

Os modelos de monitor de amostra do IBM Intelligent Operations Center são definidos de forma que um acionados dispare toda vez que uma mensagem de alerta CAP for recebida pelo servidor do IBM Business Monitor.

### Tarefas relacionadas

“Modelando KPIs” na página 63

Modele KPIs usando o Rational Application Developer ou o WebSphere Integration Developer com o IBM Business Monitor Developers Toolkit instalado. O Rational Application Developer e o IBM Business Monitor Developers Toolkit são incluídos como parte do IBM Intelligent Operations Center.

### Informações relacionadas

 Centro de Informações do IBM Business Monitor

 Centro de Informações do Rational Application Developer

## Definindo Ocorrências de Saída para o IBM Intelligent Operations Center

Ocorrências de saída definem as informações enviadas do IBM Business Monitor para o IBM Intelligent Operations Center quando um acionador dispara.

### Sobre Esta Tarefa

O IBM Intelligent Operations Center usa notificações de saída enviadas do servidor do IBM Business Monitor para determinar se o KPI foi alterado. Se o KPI tiver sido alterado, o IBM Intelligent Operations Center obtém os dados do KPI do servidor do IBM Business Monitor, atualiza as informações de cache do KPI e atualiza os dados do IBM Intelligent Operations Center.

Ocorrências de saída são definidas usando o Rational Application Developer ou o WebSphere Integration Developer com o IBM Business Monitor Developers Toolkit. Para obter mais informações sobre o uso dessas ferramentas, consulte os centros de informações para esses produtos.

Para definir uma ocorrência de saída, execute as seguintes etapas.

### Procedimento

1. Selecione o contexto KPI para a ocorrência de saída.
2. Crie a ocorrência de saída e especifique o nome e o ID da ocorrência.
3. Especifique o esquema de notificação. O esquema está localizado no arquivo `ioc-notification-v1.0.xsd`. O esquema está localizado no projeto `icoc_sample_monitor-models`.
4. Defina o conteúdo da ocorrência de saída. O conteúdo é baseado no esquema de notificação.

5. Sob **notificação**, para o valor de **sentfrom** insira Monitor.
6. Inclua os elementos de parâmetros no conteúdo da ocorrência, conforme definido nas subetapas a seguir:
  - a. Para o primeiro parâmetro, especifique 'modelID' para **parameterName** e o ID do modelo de monitor para **parameterValue**. Por exemplo, `icoc_sample_public_safety_monitor_model`.
  - b. Para cada KPI do conjunto de KPIs, inclua parâmetros para especificar o ID do KPI e o valor do KPI. O ID do KPI é especificado usando o elemento **parameterName** e o valor do KPI é especificado usando o elemento **parameterValue**. O ID do KPI deve ser associado a um KPI no conjunto de KPIs. Use a função `xs:string()` para especificar o valor do KPI como uma sequência. Por exemplo, **parameterName** pode ser 'Police\_Department' e **parameterValue** pode ser `xs:string(Police_Department)`.

## Exemplo

Segue um exemplo de uma notificação a ser enviada ao IBM Intelligent Operations Center:

```
<ns1:notification>
  <ns1:notificationType> Alert</ns1:notificationType>
  <ns1:sentFrom> Monitor</ns1:sentFrom>
  <ns1:headline> Police Department KPI Changed</ns1:headline>
  <ns1:description> Police Department KPI Changed</ns1:description>
  <ns1:kpiLink> Police Department</ns1:kpiLink>
  <ns1:category> Safety</ns1:category>
  <ns1:parameter>
    <ns1:parameterName> modelId</ns1:parameterName>
    <ns1:parameterValue>
      icoc_sample_public_safety_monitor_model</ns1:parameterValue>
    </ns1:parameter>
  <ns1:parameter>
    <ns1:parameterName> Police_Department</ns1:parameterName>
    <ns1:parameterValue> 0</ns1:parameterValue>
  </ns1:parameter>
  <ns1:parameter>
    <ns1:parameterName> Crime_Response_Time</ns1:parameterName>
    <ns1:parameterValue> 0</ns1:parameterValue>
  </ns1:parameter>
  <ns1:parameter>
    <ns1:parameterName> Crime_Response_Time_Precinct_One</ns1:parameterName>
    <ns1:parameterValue> PT3M30.000S</ns1:parameterValue>
  </ns1:parameter>
  <ns1:parameter>
    <ns1:parameterName> Crime_Response_Time_Precinct_Two</ns1:parameterName>
    <ns1:parameterValue> PT3M30.000S</ns1:parameterValue>
  </ns1:parameter>
</ns1:notification>
```

### Tarefas relacionadas

“Modelando KPIs” na página 63

Modele KPIs usando o Rational Application Developer ou o WebSphere Integration Developer com o IBM Business Monitor Developers Toolkit instalado. O Rational Application Developer e o IBM Business Monitor Developers Toolkit são incluídos como parte do IBM Intelligent Operations Center.

### Informações relacionadas

 Centro de Informações do IBM Business Monitor

 Centro de Informações do Rational Application Developer

## Implementando Modelos de Monitor

Após definir indicadores chaves de desempenho (KPIs) e seus modelos de monitor, os modelos de monitor precisam ser implementados no IBM Business Monitor em execução no servidor analítico do IBM Intelligent Operations Center.

### Sobre Esta Tarefa

Para implementar um modelo de monitor que será usado pelo IBM Business Monitor, projetos Java Enterprise Edition (JEE) devem ser gerados a partir dos modelos definidos. Quando os projetos JEE forem gerados, o aplicativo de modelo pode ser exportado como um arquivo EAR. O arquivo EAR pode então ser implementado no IBM Business Monitor em execução no servidor analítico do IBM Intelligent Operations Center.

### Procedimento

1. No Rational Application Developer ou no WebSphere Integration Developer com o IBM Business Monitor Developers Toolkit instalado, clique com o botão direito do mouse no modelo de monitor que requer geração de projeto na guia **Enterprise Explorer**. Por exemplo, `icoc_sample_public_safety_monitor_model`.
2. Clique em **Gerar Projetos JEE de Monitor**. Os projetos a seguir serão criados: `modelApplication`, `modelLogic` e `modelModerator`.
3. Exporte o aplicativo de modelo de monitor clicando com o botão direito do mouse no projeto `modelApplication` e clicando em **Exportar > EAR**.
4. Teste os KPIs antes de implementar o arquivo EAR no IBM Business Monitor.
5. Implemente o arquivo EAR no servidor do IBM Business Monitor usando as instruções no centro de informações do IBM Business Monitor.

### Informações relacionadas

 Centro de Informações do IBM Business Monitor

 Centro de Informações do Rational Application Developer

## Valores de Exibição de KPI

Os pacotes configuráveis de recursos do IBM Intelligent Operations Center pode ser usado para fornecer valores de exibição alternativos dos valores fornecidos pelos modelos do IBM Business Monitor.

Os nomes de exibição de KPI e nomes de intervalos são definidos nos modelos de amostra do IBM Business Monitor fornecidos com o IBM Intelligent Operations Center. Exemplos de nomes de exibição de KPI são:

- Água
- Qualidade da Água

Exemplos de nomes de intervalos são:

- valor de status aceitável
- valor de status de cuidado
- valor de status de agir

Cada artefato, por exemplo, KPI e intervalo, definido no IBM Business Monitor tem um ID associado ao nome de exibição. IDs não podem conter espaços, enquanto que os valores de exibição podem. Os IDs são usados como chaves para consultar valores em um pacote configurável de recursos. O IBM Intelligent Operations Center usa esses IDs para selecionar valores de exibição de KPI. Se nenhum valor for especificado no pacote configurável de recursos para o ID, o valor especificado na definição do IBM Business Monitor é usado.

Os valores de exibição de KPI são localizados pelo IBM Business Monitor usando os códigos ISO de idioma e país do servidor do IBM Business Monitor. Por exemplo, um valor de porcentagem de KPI seria exibido no formato 12.61% quando o código do idioma for en\_US e 12,61% quando o código do idioma for fr\_FR. As definições do pacote configurável de recursos não são usadas para esses valores.

O pacote configurável de recursos de propriedades padrão do IBM Intelligent Operations Center é `com.ibm.iss.icoc.rest.monitor.resources.Messages.properties`. O pacote configurável pode ser localizado em `icoc_rest_monitor_resources_utils`.

Este é um exemplo de pacote configurável de recursos:

```
kpi.NO.VALUE=No data to determine the KPI value
kpi.RANGE.UNDETERMINED=undetermined
Flood_Control=Flood Control
Water_Levels=Water Levels
Flow_Discharge_City_River=Flow Discharge City River
Water_Level_City_Lake=Water Level City Lake
```

Nesse exemplo, os valores de `kpi.NO.VALUE` e de `kpi.RANGE.UNDETERMINED` são usados pelo IBM Intelligent Operations Center quando os KPIs do IBM Business Monitor retornam um valor nulo. Por exemplo, o KPI Water Lake City Lake é definido com um período de tempo diário repetitivo baseado no último período integral. Se nenhuma ocorrência CAP for recebida para esse KPI em um domingo e o KPI for solicitado na segunda-feira, nulo é retornado, já que nenhum dado está disponível do dia anterior. O valor de exibição está configurado para "No data to determine the KPI value" e o nome de exibição do intervalo está configurado para "undetermined".

As outras entradas, `Flood_Control`, `Water_Levels`, `Flow_Discharge_City_River` e `Water_Level_City_Lake`, definem os valores de exibição para os IDs de KPIs definidos no modelo de monitor de amostra `icoc sample water monitor model` fornecido pelo IBM Intelligent Operations Center. Essas entradas podem especificar texto alternativo dos valores especificados no monitor do IBM Business Monitor. Por exemplo, o pacote configurável de recursos pode ser usado para fornecer valores traduzidos em vez de alterar o modelo em si.

### Conceitos relacionados

“KPIs de Amostra”

KPIs de amostra são fornecidos com o IBM Intelligent Operations Center. Esses KPIs são projetados para fornecer orientação para implementação de diferentes tipos de KPIs usando o Kit de Ferramentas de Desenvolvimento do IBM Business Monitor. Modelos de monitor de amostra são fornecidos para proteção de água, transporte e pública.

## Armazenamento em Cache de KPIs

As definições de configuração do IBM Intelligent Operations Center afetam quando as configurações de KPI são recuperadas do IBM Business Monitor.

Por padrão, o IBM Intelligent Operations Center carrega KPIs em um cache e atualiza o cache a cada duas horas.

Para a maioria dos KPIs, esse tempo de atualização é suficiente para fornecer KPIs atualizados ao IBM Intelligent Operations Center. Se houver KPIs definidos com períodos de tempo mais curtos do que duas horas ou se houver KPIs que são frequentemente atualizados, o intervalo de atualização de cache padrão pode ser insuficiente.

### Conceitos relacionados

“Especificando Dados de Configuração para Todo o Sistema” na página 81

A tabela IBM Intelligent Operations Center SYSPROP armazena os dados de configuração do IBM Intelligent Operations Center.

---

## KPIs de Amostra

KPIs de amostra são fornecidos com o IBM Intelligent Operations Center. Esses KPIs são projetados para fornecer orientação para implementação de diferentes tipos de KPIs usando o Kit de Ferramentas de Desenvolvimento do IBM Business Monitor. Modelos de monitor de amostra são fornecidos para proteção de água, transporte e pública.

Os KPIs com nível mais baixo são definidos como KPIs de agregação. KPIs de agregação são calculados a partir de valores contidos em mensagens de alerta CAP recebidas e uma função de agregação, como média, máximo, mínimo, soma, número de ocorrências ou desvio padrão. Seus valores são expressos em medidas quantificáveis. A ajuda instantânea é utilizada para exibir os valores reais de KPI. Valores de KPI de nível inferior são localizados no formato apropriado com base no código do idioma do servidor do IBM Business Monitor. Os KPIs superiores são mapeados para valores baseados na maneira com que o mapeamento é definido no KPI de amostra.

O valor do KPI de amostra superior é um número que equivale à cor e ao nível de resposta recomendado (0 é aceitável, 1 é monitoramento e 2 é ação). O valor do KPI inferior é uma duração, um decimal, uma porcentagem ou uma moeda, dependendo do KPI representado. Por exemplo:

- 15% é o valor real de um KPI que representa a porcentagem dos voos atrasados em um determinado aeroporto durante um período de tempo.
- 5 minutos, 7 segundos é o valor real de um KPI que representa o tempo de resposta policial médio para um determinado local durante um período de tempo.

Os arquivos de origem para os modelos de monitor de amostra do IBM Intelligent Operations Center são fornecidos em um archive que pode ser importado para o Rational Application Developer ou o WebSphere Integration Developer com o IBM Business Monitor Toolkit instalado. O archive pode ser modificado para alterar, incluir ou excluir definições de KPI. As definições podem ser geradas novamente e reimplementadas no IBM Intelligent Operations Center.

Os modelos de amostra fornecidos com o IBM Intelligent Operations Center são:

- modelo de monitor de segurança pública de amostra icoc
- modelo de monitor de transporte de amostra icoc
- modelo de monitor de água de amostra icoc

Estes modelos contém as seguintes amostras de KPI:

- Água
  - Controle de Enchentes
    - Níveis das Águas
      - Fluxo de Escoamento do Rio da Cidade
      - Nível das Águas do Lago da Cidade
  - Gerenciamento das Águas
    - Planejamento Estratégico
      - Alagamento
      - Fornecimento de Água versus Demanda
  - Qualidade da Água
    - Indicadores Físicos
      - Turvação
      - pH
- Transporte
  - Aeroportos
    - Voos Atrasados
      - Voos Atrasados do Aeroporto Um
      - Voos Atrasados do Aeroporto Dois
  - Estradas e Trânsito
    - Ocorrências em Estradas
      - Acidentes Graves de Trânsito
  - Gerenciamento de Transporte
    - Receita
      - Pedágios de Pontes e Túneis
      - Receita de Instalações de Estacionamento
- Segurança Pública
  - Corpo de Bombeiros
    - Ferimentos Sofridos pelos Bombeiros
      - Ferimentos Sofridos pelos Bombeiros no Quartel de Bombeiros Um
      - Ferimentos Sofridos pelos Bombeiros no Quartel de Bombeiros Dois
  - Departamento de Polícia
    - Tempo de Resposta Policial
      - Tempo de Resposta Policial do Distrito Policial Um
      - Tempo de Resposta Policial do Distrito Policial Dois

- Gerenciamento de Segurança Pública
  - Orçamento de Segurança Pública
    - Orçamento do Departamento de Serviço de Emergência Médica
    - Orçamento do Corpo de Bombeiros
    - Orçamento do Departamento de Polícia

#### **Conceitos relacionados**

“Status” na página 96

Use o portlet Status para visualizar o status dos Key Performance Indicator (KPIs) de uma única organização ou de várias organizações.

“Drill Down de Key Performance Indicator” na página 97

Use o portlet Drill Down de Key Performance Indicator para consultar informações adicionais sobre um KPI, o status e os valores de seus KPIs subjacentes e o seu tempo de cálculo.

“Customizando KPIs” na página 60

Indicadores chaves de desempenho (KPIs) podem ser criados e modificados usando o IBM Business Monitor e o IBM Business Monitor Development Toolkit.

#### **Tarefas relacionadas**

“Implementando Modelos de Monitor” na página 71

Após definir indicadores chaves de desempenho (KPIs) e seus modelos de monitor, os modelos de monitor precisam ser implementados no IBM Business Monitor em execução no servidor analítico do IBM Intelligent Operations Center.





---

## Capítulo 5. Customizando a Solução

A customização da solução para se adequar à sua operação específica inclui as tarefas cobertas nesta seção com relação à interface com o usuário e a tabela de propriedades de sistema. A customização tem uma relação muito próxima com a integração da solução e os links apropriados são incluídos nos tópicos sobre ocorrência e indicador chave de desempenho (KPI) desta seção.

---

### Customizando a Interface com o Usuário

É possível customizar elementos da interface com o usuário do IBM Intelligent Operations Center para se adequarem à sua operação

Assim como customizar o layout e a aparência de portlets, também é possível criar novas páginas. Para obter informações adicionais, consulte a documentação do produto WebSphere Portal.

#### Informações relacionadas

 [Documentação do Produto IBM WebSphere Portal](#)

### Localizando a Interface com o Usuário

As configurações do navegador determinam as configurações de idioma, data e hora da interface com o usuário do IBM Intelligent Operations Center. Um administrador pode customizar os formatos de data e hora.

No IBM Intelligent Operations Center, as configurações do seu navegador determinam o idioma do texto. Quando o idioma não estiver disponível no IBM Intelligent Operations Center, será utilizado o idioma mais próximo; por exemplo, francês do Canadá reverte para francês que por sua vez reverte para inglês, idioma que sempre estará disponível. Suas configurações de navegador também determinam o fuso horário de todas as datas e horários exibidos. Valores de data e hora no IBM Intelligent Operations Center são ajustados automaticamente de acordo com o fuso horário do navegador.

Todas as datas e horários são apresentados em seu fuso horário no formato especificado na tabela do banco de dados SYSPROP. As propriedades do sistema armazenam as sequências de formato de data e hora. Para alterar o valor no banco de dados editando a propriedade, siga o link no final do tópico.

#### Conceitos relacionados

“Especificando Dados de Configuração para Todo o Sistema” na página 81  
A tabela IBM Intelligent Operations Center SYSPROP armazena os dados de configuração do IBM Intelligent Operations Center.

### Lista de Portlets

O IBM Intelligent Operations Center é uma solução baseada em portlet que usa a tecnologia de portal para fornecer ferramentas e exibir informações. Todos os portlets incluídos no IBM Intelligent Operations Center são listados.

Os portlets incluídos no IBM Intelligent Operations Center são descritos na tabela a seguir. A tabela também indica em quais visualizações cada portlet está disponível.

Tabela 18. Portlets no IBM Intelligent Operations Center

Portlet	Descrição	Visualizações do Usuário
“Status” na página 96	O portlet Status fornece um resumo em nível executivo do status dos KPIs das várias organizações às quais você possui permissão de visualização. Use este portlet para visualizar mudanças atualizadas no status do KPI para que seja possível planejar e tomar uma ação, se necessário.	Executivo
“Drill Down de Key Performance Indicator” na página 97	Ao visualizar uma categoria de KPI no portlet Status que precisa de atenção, selecione-a. Todos os KPIs da categoria selecionada são, em seguida, exibidos no portlet Drill Down de Key Performance Indicator. É possível usar essa lista para inspecionar os KPIs subjacentes até obter os detalhes do KPI que causaram a mudança de status.	Executivo
“Coordenador - Alertas” na página 98	O portlet Coordenador - Alertas fornece uma lista dinâmica e interativa de alertas que resultam da mudança de KPIs e de eventos correlatos. A função desse portlet é advertir sobre mudanças no KPI ou status do evento. A lista contém detalhes chave para cada um dos alertas.	Executivo, Operações
“Contatos do Sametime” na página 100	O portlet Contatos do Sametime fornece uma lista de contatos organizada por grupo. Ela pode ser customizada com base nas pessoas com as quais você precisa se comunicar. É possível conversar com pessoas e modificar status, contatos ou grupos on-line.	Executivo, Operações

Tabela 18. Portlets no IBM Intelligent Operations Center (continuação)

Portlet	Descrição	Visualizações do Usuário
“Mapa” na página 101	<p>No portlet Mapa:</p> <p>Um mapa da região geográfica fornece informações sobre o local do evento.</p> <p>Um formulário de entrada seleciona quais categorias de ocorrências são mostradas no mapa e na lista do portlet Ocorrências.</p>	Operações
“Ocorrências” na página 105	O portlet Ocorrências fornece uma lista de eventos. A lista contém detalhes chave para cada um dos eventos. É possível exibir uma descrição mais detalhada de um evento passando o mouse sobre a linha na lista.	Operações
Publicador de Amostras	O portlet Publicador de Amostras é uma ferramenta de teste automatizada destinada a um administrador que gerencia ou verifica a solução. Funciona como um aplicativo cliente para testar a publicação de mensagens CAP no IBM Intelligent Operations Center. O portlet Publicador de Amostras pode eliminar o requisito para criar manualmente um aplicativo cliente de teste.	Administração
Resumo das permissões do usuário	O portlet Resumo das permissões do usuário é fornecido como uma ferramenta de teste. É possível inserir um ID de usuário para exibir detalhes das permissões do IBM Intelligent Operations Center para o usuário.	Administração
Intelligent Operations Center - Sobre	O portlet Sobre exibe os detalhes da versão do IBM Intelligent Operations Center que você instalou.	Administração

## Customizando o Layout da Página

É possível customizar a aparência e o layout dos portlets incluídos no IBM Intelligent Operations Center.

## Sobre Esta Tarefa

Use a interface com o usuário do WebSphere Portal para customizar portlets:

### Procedimento

1. Para abrir o WebSphere Portal, clique na guia **Administração**.
2. No WebSphere Portal, clique em **Interface com o Usuário do Portal**.
3. Na Interface com o Usuário do Portal, clique na opção obrigatória:
  - Para registrar temas e diferentes aparências, configurar o tema padrão e a aparência padrão para cada tema, clique em **Temas e Aparências**.
  - Para customizar os principais elementos do site nos temas, incluindo banner, navegação, fontes e cores, clique em **Customizador de Temas**.
4. Faça as modificações necessárias. Para obter informações adicionais sobre como usar o WebSphere Portal para customizar portlets, consulte o link na parte inferior do tópico para a documentação do produto WebSphere Portal.

### Informações relacionadas

 [Documentação do Produto IBM WebSphere Portal](#)

## Configurando o Mapa

Um administrador pode configurar a visualização de mapas para todos os usuários. Você poderá configurar o ponto central e nível de zoom do mapa. O ponto central pode ser ajustado para coordenadas específicas de latitude e longitude. Também é possível selecionar o mapa que os outros usuários verão. Selecione seu servidor do Esri GIS instalado ou um serviço GIS publicamente disponível, por exemplo, ArcGIS.com.

## Sobre Esta Tarefa

Para implementar suas alterações na configuração dos mapas, siga o procedimento a seguir. Configurações de amostra mostrando como o mapa pode ser configurado são fornecidas no link no final do tópico.

Passa o mouse sobre um ícone para visualizar a ajuda instantânea que indica o propósito do ícone.

### Procedimento

1. Efetue login em <http://portalServer/wps/myportal> como um usuário administrativo.
2. Na barra de navegação na parte superior da página, clique em **Administração**.
3. No menu da barra lateral, clique em **Gerenciamento de Portlets > Portlets**.
4. Localize o portlet Mapa e clique em **Configurar Portlet** (ícone de chave).
5. Modifique a configuração conforme necessário.
6. Clique em **OK** para salvar a configuração modificada.

### Conceitos relacionados

“Mapa” na página 101

Use o portlet Mapa para ver onde as ocorrências estão localizadas em um mapa e para controlar quais categorias de ocorrências são mostradas.

### Configuração do Mapa de Amostra

As configurações de amostra para o mapa base, o ponto central do mapa e o nível de zoom do mapa fornecem um exemplo de como o mapa pode ser configurado. Configurações válidas são fornecidas conforme aplicável.

Esta tabela fornece um exemplo de como é possível configurar as definições do mapa. Também especifica configurações válidas. Etapas detalhadas para a tarefa de configuração do mapa são explicadas no link no final do tópico.

Tabela 19. Valores Aceitos e Exemplos de Definições de Configuração

Configuração	Valores aceitos	Configuração de preferência	Valor de exemplo
O ponto central do mapa com valores para latitude e longitude respectivamente	Coordenadas válidas de latitude e longitude	com.ibm.iss.map.centerLat	-11.3
		com.ibm.iss.map.centerLon	-50
O nível de zoom para o mapa com um valor de nível de zoom	A faixa válida de níveis de zoom é determinada pelo mapa base. Em geral, a faixa é de 1 para cima. O valor 1 é o nível de zoom mais baixo, que é o zoom máximo. O mapa base padrão fornecido com o IBM Intelligent Operations Center, ArcGIS, mostra detalhes geográficos até o nível de zoom 12.	com.ibm.iss.map.zoom	4
O mapa base com valores para o tipo de mapa e a URL do mapa, respectivamente.	O tipo de mapa válido é ARC_GIS_REST.	com.ibm.iss.map.baseMap.type	ARC_GIS_REST
		com.ibm.iss.map.baseMap.Url	http://services.arcgisonline.com/ArcGIS/rest/services/World_Street_Map/MapServer/tile/{z}/{y}/{x}

---

## Especificando Dados de Configuração para Todo o Sistema

A tabela IBM Intelligent Operations Center SYSPROP armazena os dados de configuração do IBM Intelligent Operations Center.

As propriedades a seguir são propriedades que abrangem todo o sistema, utilizadas pelo IBM Intelligent Operations Center.

Tabela 20. Valores de SYSPROP para Todo o Sistema, Usados pelo IBM Intelligent Operations Center

Região	Assunto	Nome	Tipo	Valor
Sistema	*	DateFormat	Sequência	O formato usado quando o IBM Intelligent Operations Center exibe a data. O padrão é yyyy-MM-dd. Qualquer padrão válido de data Java <code>java.text.SimpleDateFormat</code> pode ser especificado.
Sistema	*	DateTimeFormat	Sequência	O formato utilizado quando o IBM Intelligent Operations Center exibe a data e hora. O padrão é yyyy-MM-dd HH:mm:ss. Qualquer padrão Java <code>java.text.SimpleDateFormat</code> válido de data e hora pode ser especificado.
Sistema	*	ModelManagerServerEJBPort	Sequência	Porta EJB utilizada pelo IBM Model Manager.
Sistema	*	ModelManagerServerHostname	Sequência	Nome de host ou endereço IP usado pelo IBM Model Manager.
Sistema	*	MonitorServerHostname	Sequência	Nome de host ou endereço IP utilizado pelo IBM Business Monitor.
Sistema	*	MonitorServerWebPort	Sequência	A porta da Web utilizada pelo Gateway de Serviços REST do IBM Business Monitor.
Sistema	*	PortalServerHostname	Sequência	Nome de host ou endereço IP usado pelo WebSphere Portal Server.
Sistema	*	PortalServerWebPort	Sequência	Porta da Web usado pelo WebSphere Portal Server.
Sistema	*	RegExpEmail	Sistema	Expressão regular usada para validar um endereço de e-mail. O padrão é <code>\b[a-zA-Z0-9._%]+@[a-zA-Z0-9.-]+\.[a-zA-Z]{2,6}\b</code> .
Sistema	*	RegExpTelephone	Sistema	Expressão regular usada para validar um número de telefone. O padrão é <code>[\w]+</code>
Sistema	*	SecurityUserPrefix	Sequência	O prefixo do ID do usuário utilizado para mapear o usuário ao nome distinto de LDAP. O padrão é <code>uid</code> .
Sistema	*	SecurityUserSuffix	Sequência	Sufixo de ID do usuário usado ao mapear o usuário a um nome de local distinto.
Sistema	*	TimeFormat	Sequência	Formato usado quando o IBM Intelligent Operations Center exibe a hora. O padrão é HH:mm:ss. Qualquer padrão de hora válido Java <code>java.text.SimpleDateFormat</code> pode ser especificado.
Sistema	*	TSRMServerHostname	Sequência	Nome de host do Tivoli Service Request Manager.
Sistema	*	TSRMServerWebPort	Sequência	Porta da web utilizada pelo Tivoli Service Request Manager.
Sistema	*	TSRMServerWorkflowUri	Sequência	URI do fluxo de trabalho usado pelo Tivoli Service Request Manager. O padrão é <code>/maximo/ui/?event=loadapp&amp;value=sr&amp;&amp;additionalevent=useqbe&amp;additionaleventvalue=TICKETID={0}</code> . O valor de incidente CAP é substituído por <code>{0}</code> .

As informações a seguir podem ser alteradas para configurar o método de processamento de KPIs.

Tabela 21. Valores de SYSPROP Que Afetam o Processamento de KPI

Região	Assunto	Nome	Tipo	Valor
KPI	*	CacheKpis	Booleano	<p>Especifica se KPIs recuperadas do IBM Business Monitor devem ou não ser armazenadas em cache.</p> <p>Se false, KPIs sempre serão recuperadas de IBM Business Monitor quando o IBM Intelligent Operations Center solicitar informações da KPI.</p> <p>Se true, KPIs são armazenadas em cache para reuso. Com que frequência o cache é atualizado é especificado por KpiCacheRefreshInterval.</p> <p>O padrão é true.</p>
KPI	*	KpiCacheRefreshInterval	Integer	<p>Especifica a frequência de atualização do cache de KPI. O intervalo é especificado em minutos.</p> <p>KpiCacheRefreshInterval será ignorado se CacheKpis for especificado como false.</p>
KPI	*	KpiSentToGroup	Sequência	<p>Especifica os grupos que recebem notificações de KPI. Separe os nomes de grupo com ponto-e-vírgula (;). O padrão é CityWideExecutive;CityWideSupervisor.</p>
KPI	*	PreLoadKpis	Booleano	<p>Especifica se as KPIs são recuperadas a partir de IBM Business Monitor quando o IBM Intelligent Operations Center for iniciado.</p> <p>Se false, KPIs são recuperadas a partir do IBM Business Monitor apenas quando o IBM Intelligent Operations Center informações da KPI.</p> <p>Se true, todos os KPIs são recuperados do IBM Business Monitor quando o IBM Intelligent Operations Center for iniciado. KPIs são armazenadas em cache para reuso. Com que frequência o cache é atualizado é especificado por KpiCacheRefreshInterval.</p> <p><b>Nota:</b> Se PreLoadKpis for true, supõe-se que CacheKpis seja true, não importa o valor especificado.</p> <p>O padrão é true.</p>

É possível alterar os valores de SYSPROP a seguir para configurar correlação de ocorrência. Os valores de correlação e ocorrências determinam se o IBM Intelligent Operations Center identifica se diversas ocorrências afetarão uma à outra devido ao horário ou proximidade.

Tabela 22. Valores de SYSPROP que Afetam Correlação de Ocorrências

Região	Assunto	Nome	Tipo	Valor
Impacto	Correlação	Distância	Flutuação	A distância entre ocorrências que podem afetar umas às outras. O padrão é 5. A unidade de distância é especificado por UnitOfDistance.
Impacto	Correlação	TimeWindow	Flutuação	Valor de tempo entre ocorrências que podem afetar umas às outras. O valor é definido em horas. O padrão é 2.
Impacto	Correlação	UnitOfDistance	Sequência	Unidade de distância utilizada com o valor Distance. Valores válidos são mile e kilometer.

**Importante:** Se qualquer um dos valores de SYSPROP do Impacto for alterado, o servidor do Tivoli Netcool/Impact no servidor de gerenciamento e evento deve ser reiniciado para tornar essas mudanças efetivas.

#### **Conceitos relacionados**

“Política para a Correlação de Ocorrências” na página 47

A política de correlação de ocorrência determina se o IBM Intelligent Operations Center identifica ocorrências que afetam umas às outras devido a seu horário ou proximidade.

## **Atualizando a Tabela SYSPROP**

Para alterar dados de configuração do IBM Intelligent Operations Center em todo o sistema, atualize a tabela SYSPROP.

### **Sobre Esta Tarefa**

**Importante:** O procedimento a seguir recarrega o banco de dados do IBM Intelligent Operations Center e exclui todos os dados existentes do IBM Intelligent Operations Center. Dados excluídos incluem todos as ocorrências e alertas Protocolo de Alerta Comum (CAP) existentes. Para atualizar uma propriedade para todo o sistema sem perder dados existentes na solução, atualize a tabela SYSPROP manualmente.

### **Procedimento**

1. No servidor de banco de dados, edite o arquivo a seguir:  
`/opt/IBM/iss/ioc/db/IOC_PopulateSysPropTables.sql`
2. Faça as alterações necessárias.
3. Salve o arquivo.
4. Execute o comando a seguir:  
`/opt/IBM/iss/ioc/db/createIOCDB_db2.sh`

---

## **Criando KPIs para Uso com o IBM Intelligent Operations Center**

Indicadores Chaves de Desempenho (KPIs) são tratados por ocorrências dentro do IBM Intelligent Operations Center. Eles são usados para direcionar dados estatísticos que podem ser usados para analisar tendências ou para indicar áreas problemáticas.

O IBM Intelligent Operations Center fornece um conjunto de KPIs e ocorrências de amostra que podem ser usados para atualizar status de KPI. Cada instalação do IBM Intelligent Operations Center deve definir os KPIs necessários para seu ambiente. Para obter informações adicionais, consulte o link no final do tópico.



### **Conceitos relacionados**

“Customizando KPIs” na página 60

Indicadores chaves de desempenho (KPIs) podem ser criados e modificados usando o IBM Business Monitor e o IBM Business Monitor Development Toolkit.

---

## **Configurando o IBM Intelligent Operations Center para Receber Ocorrências**

Mensagens de filas de ocorrências externas são recebidas pelo IBM Intelligent Operations Center em uma fila de entrada. As mensagens devem seguir o Common Alerting Protocol.

Para configurar comunicação de ocorrência no IBM Intelligent Operations Center, você deve:

- Definir a fila para mensagens de ocorrências que estão sendo enviadas ao IBM Intelligent Operations Center.
- Estruturar as mensagens de ocorrências enviadas à fila de acordo com CAP.

Para obter informações adicionais, consulte os links na parte inferior do tópico.

### **Conceitos relacionados**

“Usando a Fila de Ocorrências de Entrada Definida para o IBM Intelligent Operations Center” na página 56

Ocorrências CAP podem ser publicadas no IBM Intelligent Operations Center direcionando as mesmas à instância do WebSphere Message Broker incluída.

“Integrando ao Common Alerting Protocol” na página 48

O Protocolo de Alerta Comum (CAP) é usado para trocar informações de ocorrências entre o IBM Intelligent Operations Center e sistemas externos.



---

## Capítulo 6. Gerenciando a Solução

Os tópicos nesta sessão descrevem como executar tarefas administrativas para o IBM Intelligent Operations Center.

---

### Controlando os Servidores

Os servidores do IBM Intelligent Operations Center podem ser controlados e colocados em fila através de um comando no servidor de gerenciamento e evento.

#### Iniciando os Servidores

Um script está disponível para iniciar os servidores do IBM Intelligent Operations Center.

#### Procedimento

Execute o comando a seguir no servidor de gerenciamento e evento para iniciar todos os servidores IBM Intelligent Operations Center.

```
/opt/IBM/ISP/mgmt/scripts/IOCControl.sh start all password
```

em que *senha* é a senha do administrador IBM Intelligent Operations Center definida quando o IBM Intelligent Operations Center foi implementado. Para iniciar apenas um servidor, execute o comando a seguir.

```
/opt/IBM/ISP/mgmt/scripts/IOCControl.sh start server_ID password
```

em que *ID\_servidor* é um ID listado em **Opções de Destino** na ajuda **IOCControl** e *senha* é a senha do administrador IBM Intelligent Operations Center definida quando o IBM Intelligent Operations Center foi implementado.

**Importante:** Se estiver iniciando servidores individualmente, o TDS deve ser iniciado antes de quaisquer outros servidores serem iniciados.

#### Resultados

Os servidores IBM Intelligent Operations Center solicitados serão iniciados.

#### O que Fazer Depois

Após os servidores do IBM Intelligent Operations Center serem iniciados, inicie a análise do Tivoli Netcool/OMNIBus.

### Tarefas relacionadas

“Iniciando a Análise do Tivoli Netcool/OMNIBus”

Inicie a análise do Tivoli Netcool/OMNIBus após todos os servidores do IBM Intelligent Operations Center terem sido iniciados.

“Parando os Servidores”

Um script está disponível para parar os servidores IBM Intelligent Operations Center.

“Consultando o Status dos Servidores” na página 89

Um script está disponível para determinar o status dos servidores do IBM Intelligent Operations Center.

“Obtendo Ajuda para o Comando IOCControl” na página 89

Informações sobre as opções de ação e destino para o comando **IOCControl** estão disponíveis.

## Iniciando a Análise do Tivoli Netcool/OMNIBus

Inicie a análise do Tivoli Netcool/OMNIBus após todos os servidores do IBM Intelligent Operations Center terem sido iniciados.

### Sobre Esta Tarefa

No servidor de gerenciamento e evento, execute os comandos a seguir.

#### Procedimento

1. Execute

```
mv /opt/IBM/netcool/omnibus/log/ioc_xml.log /opt/IBM/netcool/omnibus/log/old_ioc_xml.log
```

2. Execute

```
/opt/IBM/netcool/omnibus/probes/ncp_xml -name ioc_xml -propsfile /opt/IBM/netcool/omnibus/probes/linux2x86/ioc_xml.props &
```

## Parando os Servidores

Um script está disponível para parar os servidores IBM Intelligent Operations Center.

#### Procedimento

Execute o comando a seguir no servidor de gerenciamento e evento para iniciar todos os servidores IBM Intelligent Operations Center.

```
/opt/IBM/ISP/mgmt/scripts/IOCControl.sh stop all password
```

em que *senha* é a senha do administrador IBM Intelligent Operations Center definida quando o IBM Intelligent Operations Center foi implementado.

Para interromper apenas um servidor, execute o comando a seguir.

```
/opt/IBM/ISP/mgmt/scripts/IOCControl.sh stop server_ID password
```

em que *ID\_servidor* é um ID listado em **Opções de Destino** na ajuda **IOCControl** e *senha* é a senha do administrador IBM Intelligent Operations Center definida quando o IBM Intelligent Operations Center foi implementado.

#### Resultados

Os servidores IBM Intelligent Operations Center solicitados serão interrompidos.

### Tarefas relacionadas

“Iniciando os Servidores” na página 87

Um script está disponível para iniciar os servidores do IBM Intelligent Operations Center.

“Consultando o Status dos Servidores”

Um script está disponível para determinar o status dos servidores do IBM Intelligent Operations Center.

“Obtendo Ajuda para o Comando IOControl”

Informações sobre as opções de ação e destino para o comando **IOControl** estão disponíveis.

## Consultando o Status dos Servidores

Um script está disponível para determinar o status dos servidores do IBM Intelligent Operations Center.

### Procedimento

No servidor de gerenciamento e evento, execute o seguinte comando para consultar o status de todos os servidores do IBM Intelligent Operations Center.

```
/opt/IBM/ISP/mgmt/scripts/IOControl.sh status all password
```

em que *senha* é a senha do administrador IBM Intelligent Operations Center definida quando o IBM Intelligent Operations Center foi implementado.

Para verificar apenas um servidor, execute o comando a seguir.

```
/opt/IBM/ISP/mgmt/scripts/IOControl.sh status server_ID password
```

em que *ID\_servidor* é um ID listado em **Opções de Destino** na ajuda **IOControl** e *senha* é a senha do administrador IBM Intelligent Operations Center definida quando o IBM Intelligent Operations Center foi implementado.

### Resultados

Servidores que foram iniciados serão exibidos como **[on]**. Servidores que não foram iniciados serão exibidos como **[off]**.

### Tarefas relacionadas

“Iniciando os Servidores” na página 87

Um script está disponível para iniciar os servidores do IBM Intelligent Operations Center.

“Parando os Servidores” na página 88

Um script está disponível para parar os servidores IBM Intelligent Operations Center.

“Obtendo Ajuda para o Comando IOControl”

Informações sobre as opções de ação e destino para o comando **IOControl** estão disponíveis.

## Obtendo Ajuda para o Comando IOControl

Informações sobre as opções de ação e destino para o comando **IOControl** estão disponíveis.

### Procedimento

No servidor de gerenciamento e evento execute um dos comandos a seguir para o comando **IOControl**.

```
/opt/IBM/ISP/mgmt/scripts/IOControl.sh help
```

ou

```
/opt/IBM/ISP/mgmt/scripts/IOControl.sh
```

## Resultados

As opções para o comando **IOControl** serão exibidas.

### Tarefas relacionadas

“Iniciando os Servidores” na página 87

Um script está disponível para iniciar os servidores do IBM Intelligent Operations Center.

“Parando os Servidores” na página 88

Um script está disponível para parar os servidores IBM Intelligent Operations Center.

“Consultando o Status dos Servidores” na página 89

Um script está disponível para determinar o status dos servidores do IBM Intelligent Operations Center.

---

## Manutenção da Solução

Execute as tarefas descritas nesta seção para manter sua solução executando de forma ideal.

### Ajustando o Desempenho

As seções a seguir descrevem como ajustar o servidor de portal e o WebSphere Application Server.

#### Ajustando o Servidor de Portal Sobre Esta Tarefa

Utilize as diretrizes a seguir, baseadas nos resultados dos testes de desempenho, para configurar o tamanho do heap da Java Virtual Machine.

#### Procedimento

1. Configure os tamanhos máximo e mínimo do heap para o mesmo valor.
2. Configure o tamanho do heap para um valor compatível com a memória física e que seja acima de 2 GB.

#### O que Fazer Depois

Para obter informações, consulte o Portal Server 7 Performance Tuning Guide.

#### Ajustando o WebSphere Application Server

Para obter informações sobre o ajuste do desempenho do WebSphere Application Server Versão 7, consulte o Centro de Informações do WebSphere Application Server, Network Deployment, Versão 7.0.

### Dicas de Manutenção

Dicas adicionais para manter a solução são documentadas na forma de notas técnicas individuais no IBM Support Portal.

O link a seguir ativa uma consulta customizada da base de conhecimento Suporte de produção: [Visualizar Todas as Dicas de Manutenção para o IBM Intelligent Operations Center](#).





---

## Capítulo 7. Usando a Interface da Solução

O IBM Intelligent Operations Center é uma solução baseada na Web usando tecnologia de portal. Pode ser acessada com qualquer um dos navegadores da Web suportados.

Para obter detalhes sobre quais navegadores são suportados, consulte os requisitos detalhados do sistema.

---

### Efetuando Logon

Efetue logon para acessar a interface com o usuário do IBM Intelligent Operations Center.

#### Antes de Iniciar

Entre em contato com o administrador local para obter o seu ID e senha do usuário. O administrador é responsável por garantir que você possua o nível de acesso de segurança adequado para sua função na organização. O administrador fornecerá também uma URL para o IBM Intelligent Operations Center.

#### Procedimento

1. Insira a URL da Web no campo de endereço do navegador.
2. Na página inicial do servidor, insira o ID do usuário e senha.
3. Clique em **Efetuar login**.

#### Resultados

A página inicial do IBM Intelligent Operations Center é exibida no navegador da Web. Estão disponíveis apenas as páginas, recursos e dados a que você possui permissão de acesso. Entre em contato com o administrador se precisar de acesso adicional.

#### Tarefas relacionadas

“Efetuando Logoff”

Efetue logoff para sair da interface com o usuário IBM Intelligent Operations Center e finalizar a sessão do servidor. Por padrão, o link **Efetuar Logout** está localizado no canto superior direito do IBM Intelligent Operations Center.

---

### Efetuando Logoff

Efetue logoff para sair da interface com o usuário IBM Intelligent Operations Center e finalizar a sessão do servidor. Por padrão, o link **Efetuar Logout** está localizado no canto superior direito do IBM Intelligent Operations Center.

### Tarefas relacionadas

“Efetuando Logon” na página 93

Efetue logon para acessar a interface com o usuário do IBM Intelligent Operations Center.

---

## Visualizando ou Editando o Perfil do Usuário

É possível visualizar ou alterar as informações no perfil do usuário para o IBM Intelligent Operations Center.

### Sobre Esta Tarefa

O perfil contém as informações previamente inseridas por você ou por seu administrador. É possível atualizar o perfil editando as informações nos campos de atributo. Por exemplo, é possível alterar a senha existente para uma nova senha.

*Tabela 23. Atributos do Perfil do Usuário do IBM Intelligent Operations Center*

Atributo	Descrição	O usuário pode editar?
ID do usuário*	Um ID é designado para cada novo usuário pelo administrador para propósitos de identificação.	Não
Senha*	Uma senha é designada pelo administrador para segurança. A senha deve ser exclusiva e possuir de 5 a 60 caracteres de comprimento. Senhas válidas devem conter apenas os caracteres a-z, A-Z, ponto ".", traço "-" e sublinhado "_".	Sim
Nome	Um nome pode ser inserido pelo administrador ou pelo usuário.	Sim
Sobrenome*	Um sobrenome, ou nome de família, é inserido pelo administrador.	Sim
Correio	Um endereço de e-mail pode ser inserido pelo administrador ou pelo usuário.	Sim

**Nota:** Os atributos marcados com um asterisco são necessários para a criação bem sucedida de um novo usuário, aqueles que não estão marcados com um asterisco são opcionais.

### Procedimento

1. No lado direito da barra de navegação na parte superior, selecione **Editar Meu Perfil**. Os atributos do perfil são exibidos.
2. Para alterar a senha:
  - a. Insira a senha atual (o texto da senha não é exibido).
  - b. No campo **Nova Senha** e nos campos **Confirmar Senha**, insira a nova senha.
3. Insira ou edite as informações em qualquer um dos campos restantes.
4. Para submeter as mudanças, clique em **OK**.

### Resultados

O perfil do usuário está atualizado com as mudanças.

## Visualização Executivo

Use a visualização Executivo para obter uma visualização consolidada dos Key Performance Indicator (KPIs) e alertas associados aos KPIs. A visualização Executivo permite que usuários com responsabilidade entre organizações monitorem, gerenciem e respondam a mudanças de status com relação às áreas-chaves de desempenho e bem-estar organizacional.

A visualização Executivo é uma página da Web interativa. Ela contém os portlets a seguir, que é possível considerar como sendo seções independentes da página que cooperam umas com as outras para fornecer informações e interação abrangentes no nível executivo:

Tabela 24. Portlets da Visualização Executivo

Portlet	Descrição
“Status” na página 96	O portlet Status fornece um resumo em nível executivo do status dos KPIs das várias organizações às quais você possui permissão de visualização. Use este portlet para visualizar mudanças atualizadas no status do KPI para que seja possível planejar e tomar uma ação, se necessário.
“Drill Down de Key Performance Indicator” na página 97	Ao visualizar uma categoria de KPI no portlet Status que precisa de atenção, selecione-a. Todos os KPIs da categoria selecionada são, em seguida, exibidos no portlet Drill Down de Key Performance Indicator. É possível usar essa lista para inspecionar os KPIs subjacentes até obter os detalhes do KPI que causaram a mudança de status.
“Coordenador - Alertas” na página 98	O portlet Coordenador - Alertas fornece uma lista dinâmica e interativa de alertas que resultam da mudança de KPIs e de eventos correlatos. A função desse portlet é advertir sobre mudanças no KPI ou status do evento. A lista contém detalhes-chave para cada um dos alertas. Por exemplo, quando um KPI muda o status de amarelo para vermelho, um alerta é enviado para o portlet Coordenador - Alertas.
“Contatos do Sametime” na página 100	O portlet Contatos do Sametime fornece uma lista de contatos organizada por grupo. Ela pode ser customizada com base nas pessoas com as quais você precisa se comunicar. É possível conversar com pessoas e modificar status, contatos ou grupos on-line.

Para obter ajuda no uso de cada portlet, clique no canto superior direito do portlet e selecione **Ajuda** a partir do menu exibido.

Para redimensionar um portlet, clique no canto superior direito do portlet e selecione opções a partir do menu que é exibido, conforme segue:

- Para expandir o portlet para preencher a página, selecione **Maximizar**.

- Para ocultar o conteúdo do portlet, além da sua barra de título, selecione **Minimizar**.
- Para restaurar um portlet minimizado ou maximizado para a sua visualização padrão, selecione **Restaurar**.

## Status

Use o portlet Status para visualizar o status dos Key Performance Indicator (KPIs) de uma única organização ou de várias organizações.

### O que é o portlet Status?

O portlet Status fornece um resumo em nível executivo do status dos KPIs das várias organizações às quais você possui permissão de visualização. Use este portlet para visualizar mudanças atualizadas no status do KPI para que seja possível planejar e tomar uma ação, se necessário.

### O que este portlet exibe?

Cada linha contém informações de KPI sobre uma organização que está nomeada na primeira coluna da tabela. Cada organização e as categorias de KPI associadas a ela são representadas por células coloridas. A cor do plano de fundo de um KPI reflete seu status.

O código da cor do plano de fundo fornecido com os KPIs de amostra do IBM Intelligent Operations Center é configurado conforme segue:

- O verde indica que está tudo certo, com base nos parâmetros aceitáveis para esse KPI
- Amarelo indica cuidado ou monitoramento necessário.
- Vermelho indica que a ação é recomendada.
- Cinza indica que existem dados insuficientes disponíveis para calcular o status do KPI.

O status indeterminado indica que não há valor de KPI disponível para o período de tempo definido. Essa situação ocorre quando o IBM Intelligent Operations Center não recebeu quaisquer mensagens para um dado KPI no período de tempo especificado. Por exemplo, o nível de água para uma fonte é calculado diariamente. Se nenhuma mensagem de nível de água para aquela fonte de água for recebida em um determinado dia, não haverá dados para determinar o valor de KPI.

Quando um KPI subjacente é alterado, a mudança é refletida no portlet Status. Por exemplo, um dos KPIs de amostra que determina o status do KPI de Qualidade da Água altera o status de aceitável para cuidado. A mudança é refletida no portlet com uma mudança na cor do plano de fundo da célula Qualidade da Água de verde para amarelo. Além disso, o portlet Coordenador - Alertas indica que um KPI foi alterado.

Quando a solução recebe uma mensagem relacionada ao cálculo de um KPI, ocorre uma mudança instantânea de cor. Esta é uma vantagem quando o KPI é um que está suscetível a receber mudanças em tempo real, como atrasos em aeroporto ou acidentes de trânsito. Isso não é relevante para KPIs históricos, como controle de enchentes, em que são tomadas medidas regulares diariamente e é improvável que haja uma mudança repentina afetando o status nesse ínterim.

Para exibir todos os KPIs subjacentes e os seus detalhes no portlet Drill Down de Key Performance Indicator, clique em uma célula colorida da tabela presente no portlet Status.

Para obter mais informações sobre o uso da interface da solução, clique em **Ajuda** no canto superior direito da página do navegador.

Para obter mais informações sobre a administração e customização da solução, acesse IBM Intelligent Operations Center .

## Drill Down de Key Performance Indicator

Use o portlet Drill Down de Key Performance Indicator para consultar informações adicionais sobre um KPI, o status e os valores de seus KPIs subjacentes e o seu tempo de cálculo.

### O que é o Portlet Drill Down de Key Performance Indicator?

Ao visualizar uma categoria de KPI no portlet Status que precisa de atenção, selecione-a. Todos os KPIs da categoria selecionada são, em seguida, exibidos no portlet Drill Down de Key Performance Indicator. É possível usar essa lista para inspecionar os KPIs subjacentes até obter os detalhes do KPI que causaram a mudança de status.

### O que este portlet exibe?

O portlet Drill Down de Key Performance Indicator mostra todos os KPIs subjacentes associados à organização ou à categoria de KPI selecionada no portlet Status. Os KPIs são exibidos na forma de uma lista aninhada que pode ser expandida ou reduzida. O status de cada KPI subjacente é representado pela cor, da mesma maneira que a cor é usada para os KPIs exibidos no portlet Status. Os KPIs subjacentes controlam a cor do KPI pai. Para exibir o valor real do KPI, passe o cursor do mouse sobre o KPI. Por exemplo, o valor real para os Acidentes Graves de Trânsito é 10, uma base para o KPI de Gerenciamento de Transporte.

### Trabalhando com a Lista de KPIs

É possível executar as tarefas presentes na lista a seguir a partir da barra de ação na parte superior do portlet. Para visualizar a ação associada a um ícone, posicione o mouse sobre o ícone.

- Para atualizar o conteúdo da lista, clique em **Atualizar** .
- Para selecionar todos os KPIs presentes na lista, clique em **Selecionar Tudo**.
- Para cancelar seleção de todos os KPIs presentes na lista, clique em **Cancelar Seleção de Tudo**.
- Para reduzir uma lista expandida, clique em **Reduzir Tudo**.
- Para classificar a lista em ordem alfabética, clique no nome da coluna que será classificada.
- Para reverter uma lista classificada em uma não classificada, clique em **Limpar Classificação**.
- Para selecionar quais colunas serão exibidas, clique em **Configurar Opções** e selecione as caixas de seleção.
- Para selecionar quais linhas serão exibidas, insira texto no campo **Filtro Rápido** para filtrar as linhas de acordo com o texto definido. O botão à esquerda do campo permite limpar o filtro.

Para obter mais informações sobre o uso da interface da solução, clique em **Ajuda** no canto superior direito da página do navegador.

## KPIs de Amostra

Administrador

Um conjunto de KPIs de amostra é fornecido com o IBM Intelligent Operations Center. Esses KPIs são projetados para fornecer orientação para o planejamento e a implementação de diferentes tipos de KPIs para se adequarem à sua organização. Os exemplos são fornecidos nas áreas de água, transporte e segurança pública.

Para obter mais informações sobre esse assunto, acesse o IBM Intelligent Operations Center e procure KPIs de amostra. Consulte também o centro de informações para obter mais informações sobre a administração e customização da solução.

## Coordenador - Alertas

Use o portlet Coordenador - Alertas para visualizar as mensagens de alerta e os seus detalhes.

### O que é o Portlet Coordenador - Alertas?

O portlet Coordenador - Alertas é uma janela interativa contendo uma lista de todos os alertas atuais relevantes para você. São visualizados apenas os alertas que foram enviados aos seus grupos de usuários. Alertas são notificações recebidas quando:

- Diversos eventos estão acontecendo nas mesmas adjacências e em horários semelhantes, logo, podem estar em conflito ou pode ser necessária coordenação
- Uma mudança de valor de Key Performance Indicator (KPI) predefinido ocorre onde essa mudança tiver sido definida como um acionador de alerta pelo administrador

É possível também usar o portlet Coordenador - Alertas para exibir mais detalhes de um alerta.

### O que este portlet exibe?

O portlet Coordenador - Alertas fornece uma lista dinâmica e interativa de alertas que resultam da mudança de KPIs e de eventos correlatos. A função desse portlet é advertir sobre mudanças no KPI ou status do evento. A lista contém detalhes chave para cada um dos alertas.

Para mostrar uma descrição mais detalhada de um alerta, passe o cursor do mouse sobre a linha. Para consultar todas as informações associadas àquele alerta em uma janela pop-up, clique com o botão direito do mouse na linha e selecione **Propriedades**.

Inicialmente, quando uma página de portal é aberta, o portlet Coordenador - Alertas exibe todos os alertas atuais. Remova qualquer alerta a partir do portlet clicando com o botão direito do mouse na linha e selecionando **Fechar alerta**. É possível fechar diversos alertas dessa maneira ao selecionar diversas linhas. Apenas feche um alerta após tê-lo tratado adequadamente, pois ao ser fechado, o alerta será removido para todos os destinatários.

Clique no botão no canto superior direito da janela pop-up para cancelá-lo e retornar à lista.

## Propriedades do Alerta

A janela pop-up dos detalhes do alerta exibe as seguintes propriedades:

Tabela 25. Propriedades do Alerta

Propriedade	Conteúdo
Título	Breve descrição do alerta
Categoria	Classificação de alto nível do evento ou KPI
Emissor	Origem do alerta
Enviado aos Grupos	Grupos para os quais o alerta foi enviado
Enviado	Data e hora em que o alerta foi enviado
Descrição	Descrição adicional do alerta
Refere-se a Alertas	Identificador de ocorrência, se o alerta foi causado pelas ocorrências correlatas
Refere-se a KPIs	Nome do KPI, se o alerta foi causado por uma mudança de valor de KPI

## Trabalhando com a Lista

A partir da barra de ação na parte superior da lista, é possível executar as tarefas a seguir.

- Para atualizar o conteúdo da lista, clique em **Atualizar**.
- Para exportar o conteúdo da lista, selecione uma **Opção de Exportação** para a lista:
  - Exportar como HTML
  - Exportar tudo para CSV
- Para imprimir o conteúdo da lista, selecione **Opções de Impressão** para a lista:
  - Imprimir tudo
  - Imprimir selecionado
  - Imprimir visualização
- Para selecionar quais colunas serão mostradas, clique em **Configurar Opções** e selecione as caixas de seleção.
- Para selecionar quais linhas serão mostradas, clique em **Filtro Avançado** para filtrar linhas de acordo com as regras definidas. As regras podem ser inseridas pela coluna, condição e palavra-chave. Como alternativa, insira uma palavra-chave no campo de filtro rápido. A barra de filtro localizada na parte superior da lista indica se foi aplicado um filtro e o número de linhas mostradas com relação ao total.
- Para limpar o filtro, clique em **Limpar Filtro**. Como alternativa, clique no botão à esquerda do campo de filtro rápido.

Um contador na barra de ação no final da lista indica o número de itens exibidos e o número total de itens. O número de itens que podem ser exibidos é limitado a 25. Se houver mais linhas do que pode ser exibido de uma vez, é possível avançar ou retroceder páginas clicando nos botões na barra de ação no final da lista.

Para obter mais informações sobre o uso da interface da solução, clique em **Ajuda** no canto superior direito da página do navegador.

Para obter mais informações sobre a administração e customização da solução, acesse IBM Intelligent Operations Center .

## Contatos do Sametime

O portlet Contatos do Sametime autoriza o uso do sistema de mensagens instantâneas do IBM Lotus Sametime no IBM Intelligent Operations Center.

### O que é o Portlet Contatos do Sametime?

O portlet Contatos do Sametime fornece uma lista de contatos organizada por grupo. Ela pode ser customizada com base nas pessoas com as quais você precisa se comunicar. É possível conversar com pessoas e modificar status, contatos ou grupos on-line.

### O que este portlet exibe?

A lista que aparece em Contatos do Sametime quando você efetua logon pela primeira vez depende da maneira como a organização configurou grupos no IBM Intelligent Operations Center.

Use os menus suspensos na parte superior do portlet para trabalhar com a lista.

- Use o menu **Pessoas** para incluir contatos ou modificar grupos.
- Use o menu **Opções** para modificar a mensagem de status ou visualizar apenas as pessoas que estão on-line.

Para obter ajuda mais detalhada sobre como usar o portlet Contatos do Sametime, clique no menu de exibição suspenso no canto direito da parte superior do portlet e selecione **Ajuda**.

---

## Visualização Operações

Use a visualização Operações para manter o reconhecimento das ocorrências. É direcionada para operadores, gerentes ou outros eventos atuais de monitoramento e eventos futuros do planejamento.

A visualização Operações é uma página da Web interativa. Ela contém os portlets a seguir, que é possível considerar como sendo seções independentes da página que cooperam umas com as outras para fornecer informações e interação abrangentes no nível de operações:

*Tabela 26. Portlets da Visualização Operações*

Portlet	Descrição
"Mapa" na página 101	Um mapa da região geográfica fornece informações sobre o local do evento.  Um formulário de entrada seleciona quais categorias de ocorrências são mostradas no mapa e na lista do portlet Ocorrências.
"Ocorrências" na página 105	O portlet Ocorrências fornece uma lista de eventos. A lista contém detalhes chave para cada um dos eventos. É possível exibir uma descrição mais detalhada de um evento passando o mouse sobre a linha na lista.



Tabela 26. Portlets da Visualização Operações (continuação)

Portlet	Descrição
“Coordenador - Alertas” na página 98	<p>O portlet Coordenador - Alertas fornece uma lista dinâmica e interativa de alertas que resultam da mudança de KPIs e de eventos correlatos. A função desse portlet é advertir sobre mudanças no KPI ou status do evento. A lista contém detalhes chave para cada um dos alertas.</p> <p>Por exemplo, quando dois eventos graves ocorrem juntos no mesmo local e horário, é enviado um alerta para o portlet Coordenador - Alertas.</p>
“Contatos do Sametime” na página 100	O portlet Contatos do Sametime fornece uma lista de contatos organizada por grupo. Ela pode ser customizada com base nas pessoas com as quais você precisa se comunicar. É possível conversar com pessoas e modificar status, contatos ou grupos on-line.

Para obter ajuda no uso de cada portlet, clique no canto superior direito do portlet e selecione **Ajuda** a partir do menu exibido.

Para redimensionar um portlet, clique no canto superior direito do portlet e selecione opções a partir do menu que é exibido, conforme segue:

- Para expandir o portlet para preencher a página, selecione **Maximizar**.
- Para ocultar o conteúdo do portlet, além da sua barra de título, selecione **Minimizar**.
- Para restaurar um portlet minimizado ou maximizado para a sua visualização padrão, selecione **Restaurar**.

## Mapa

Use o portlet Mapa para ver onde as ocorrências estão localizadas em um mapa e para controlar quais categorias de ocorrências são mostradas.

### O que é o Portlet Mapa?

O portlet Mapa é o ponto de início para interação com a página Operações. O portlet fornece uma representação visual dos eventos em um mapa que permite a identificação de padrões do local, conflitos e outros problemas. Também pode ser usado para atualizar o conteúdo do portlet Ocorrências. É possível selecionar no portlet Mapa a categoria do evento que você deseja exibir no mapa e a lista de portlets de Eventos.

### O que este portlet exhibe?

O portlet Mapa possui duas interfaces interativas conforme mostrado na seguinte tabela:

Tabela 27. Exibição do Portlet Mapa

Elemento da interface	Descrição
Mapa	Um mapa da região geográfica fornece informações sobre o local do evento.
Filtro	Um formulário de entrada seleciona quais categorias de ocorrências são mostradas no mapa e na lista do portlet Ocorrências.

Inicialmente, quando a página Operações é aberta, o portlet Mapa mostra todos os eventos que são relevantes. O mapa usa os valores de latitude e longitude especificados no registro de eventos para mostrar a localização do evento no formulário de um ícone ou uma estrutura de tópicos de polígono da área.

**Nota:** Se um evento não possuir coordenadas, ele será exibido apenas na lista de portlets Ocorrências e não aparecerá no portlet Mapa.

## Como o Mapa é Atualizado?

O mapa o mantém atualizado ao incluir novas ocorrências no mapa conforme são inseridas no sistema, sujeitas a quaisquer filtros que você tenha configurado para limitar as categorias mostradas. É possível exibir uma descrição do evento clicando no marcador do evento no mapa.

Para visualizar o formulário de filtro, clique em **Selecionar o conteúdo no mapa e lista de eventos**. As categorias de evento exibidas no mapa e no portlet Ocorrências podem ser alteradas com base na seleção de formulário de filtro que é feita. O mapa continua abaixo do filtro. É possível se concentrar na categoria do evento que se deseja analisar, utilizando o filtro para ocultar as categorias de evento que não são necessárias. O mapa responde para qualquer nova seleção de categoria enviada a partir do formulário de filtro. Quando uma solicitação é enviada, a janela do mapa é atualizada e apenas os locais de eventos da categoria selecionada são plotados no mapa. Altere a categoria de eventos exibida marcando ou desmarcando uma caixa de seleção no formulário de filtro. Para fechar o formulário de filtro, clique em **Fechar seleção de conteúdo**. Se você sair da página e retornar, todas as categorias serão reconfiguradas para selecionadas.

É possível se concentrar nos eventos individuais que deseja analisar marcando as caixas de seleção no portlet Ocorrências. Esses eventos são destacados no mapa.

## Marcadores do Mapa

O mapa representa o local de um evento com um dos seguintes tipos de marcador:

*Tabela 28. Marcadores do Mapa*

Tipo de Marcador	Descrição
Ícone	Identifique a localização de um evento no mapa com um ícone exclusivo para cada categoria
Polígono	Uma estrutura de tópicos no mapa da área associada a um evento

**Nota:** O ícone e o nome da categoria estão incluídos nos detalhes sobre a ocorrência na lista de portlets de Ocorrências. Quando uma ocorrência é escalada para um incidente no portlet de Ocorrências, o ícone exibido no mapa é alterado de um ícone específico da categoria para um triângulo vermelho com um ponto de exclamação.

## Usando os Controles de Mapa

É possível se movimentar pelo mapa, em duas dimensões, usando o mouse ou o teclado.

## Os controles do mapa estão localizados no canto superior esquerdo do mapa

Os controles do mapa estão localizados no canto superior esquerdo do mapa. Eles são compostos de:

1. Setas de panoramização (para cima, para baixo, à esquerda, à direita)
2. Aumentar zoom
3. Visualização Global (maximiza a diminuição do zoom)
4. Diminuir zoom

## Controles de Panoramização para se Movimentar pelo Mapa

Para se movimentar pelo mapa, é possível:

- Clicar e arrastar o mapa usando o mouse
- Pressionar a seta de panoramização para cima ou a tecla de seta para cima no teclado para se deslocar para o norte
- Pressionar a seta de panoramização para baixo ou a tecla de seta para baixo no teclado para se deslocar para o sul
- Pressionar a seta de panoramização para a direita ou a tecla de seta para direita no teclado para se deslocar para o leste
- Pressionar a seta de panoramização para a esquerda ou a tecla de seta para esquerda no teclado para se deslocar para o oeste

## Controles de Zoom para Obter uma Visualização Mais ou Menos Detalhada

Para aumentar e diminuir o zoom do mapa, é possível:

- Clicar no ícone + do mapa para aumentar o zoom ou no ícone - do mapa para diminuir o zoom da parte central do mapa
- Clicar duas vezes com o mouse no centro do mapa e aumentar o zoom no local selecionado
- Clicar no ícone **Visualização global** para maximizar a diminuição do zoom para mostrar a visualização global
- Pressionar a tecla + no teclado para aumentar zoom
- Pressionar a tecla - no teclado para diminuir zoom
- Pressionar Shift ao usar o mouse para desenhar um retângulo ao redor da área na qual será aumentado o zoom

## Incluindo um Evento

É possível criar um evento, incluindo-o no mapa do portlet Mapa e na lista de portlets Ocorrências ao mesmo tempo. O mapa e a lista fornecem duas maneiras de olhar para o mesmo conteúdo.

### Sobre Esta Tarefa

Use o diálogo **Incluir Evento** para especificar propriedades de evento, conforme definido na tabela a seguir:

**Nota:**

Tabela 29. Propriedades de Evento

Propriedade	Conteúdo
Remetente *	Origem ou ID do usuário
Nome do contato	Pessoa com quem entrar em contato para obter informações adicionais
Número de telefone para contato	Número de telefone da pessoa de contato
Endereço de e-mail de contato	Endereço de e-mail da pessoa de contato
Tipo de evento*	Classificação de evento abaixo do nível de categoria
Status do evento*	Instruções de manipulação de eventos
Escopo do evento*	Público alvo desejado para a mensagem
Restrição	Informações adicionais necessárias quando o escopo é 'Restrito'
Título*	Breve descrição do evento
Categoria*	Classificação de evento de alto nível
Gravidade*	Intensidade do impacto do evento
Certeza*	Confiança na predição do evento
Urgência*	Intervalo de tempo para ação em resposta ao evento
Tipo de mensagem	Natureza da mensagem
Descrição	Descrição adicional do evento
Endereço da Web	Endereço da Web para obter informações adicionais sobre o evento
Data / hora de envio*	Data e hora em que a mensagem foi enviada
Data / hora efetiva	Data e hora em que a mensagem está efetiva
Data / hora de início	Data e hora em que o evento está previsto para começar
Data / hora de expiração	Data e hora em que o evento está previsto para terminar
Descrição da área	Descrição da área afetada
Latitude / Longitude	Coordenadas da localização do evento

## Procedimento

1. Clique com o botão direito em uma localização no mapa e clique em **Criar um nova ocorrência** para ativar o diálogo **Incluir Ocorrência**. Algumas propriedades da ocorrência são preenchidas automaticamente.
2. Especifique as propriedades de evento restantes, usando os campos no diálogo. As propriedades marcadas com um asterisco são necessárias para a criação bem sucedida de um novo evento, aquelas que não estão marcadas com um asterisco são opcionais.
3. Clique em **OK** para salvar o evento ou em **Cancelar** para parar a inclusão do evento.

## Resultados

Um ícone que representa a categoria do novo evento é exibido na localização solicitada no mapa e os seus principais detalhes, na lista de portlets Ocorrências.

**Nota:** Não é possível criar um evento para uma localização na qual já é exibido um ícone ou um polígono. Para criar um evento para uma localização já

ocupada por um evento no mapa, oculte a categoria de evento usando o filtro e clique novamente com o botão direito do mouse na localização.

Para obter mais informações sobre o uso da interface da solução, clique em **Ajuda** no canto superior direito da página do navegador.

## Configurando o Mapa

Administrador

Um administrador pode alterar configurações de mapa para todos os usuários. O administrador pode alterar o ponto central e o nível de zoom para a exibição do mapa. O administrador também pode selecionar o mapa base que o usuário vê, por exemplo, ArcGIS.

Para obter mais informações sobre este assunto, acesse o IBM Intelligent Operations Center e procure por configurando o mapa. Consulte também o centro de informações para obter mais informações sobre a administração e customização da solução.

## Ocorrências

Use o portlet Ocorrências para visualizar, monitorar e gerenciar eventos no IBM Intelligent Operations Center.

### O que é o Portlet Ocorrências?

O portlet Ocorrências é uma janela interativa no IBM Intelligent Operations Center. Todos os eventos os quais o usuário está autorizado a visualizar estão visíveis na lista e no mapa do portlet Mapa. A lista de eventos pode ser filtrada para exibir um subconjunto de eventos.

### O que este portlet exibe?

O portlet Ocorrências fornece uma lista de eventos. A lista contém detalhes chave para cada um dos eventos. É possível exibir uma descrição mais detalhada de um evento passando o mouse sobre a linha na lista.

Inicialmente, quando o IBM Intelligent Operations Center é aberto, o portlet Ocorrências mostra todos os eventos que são relevantes. A lista de eventos é automaticamente atualizada ao detectar um novo evento ou uma mudança em um evento. As categorias de ocorrências mostradas na lista Ocorrências e no mapa no portlet Mapa são as mesmas.

Remova eventos do mapa e da lista desmarcando as caixas de seleção presentes no formulário de entrada no portlet Mapa. Filtre o conteúdo da lista de eventos usando as opções de filtro na barra de ação na parte superior do portlet Ocorrências. Essas opções de filtro afetam apenas a lista e não o mapa.

## Propriedades de Evento

A tabela a seguir define as propriedades que descrevem um evento:

Tabela 30. Propriedades de Evento

Propriedade	Conteúdo
Remetente *	Origem ou ID do usuário

Tabela 30. Propriedades de Evento (continuação)

Propriedade	Conteúdo
Nome do contato	Pessoa com quem entrar em contato para obter informações adicionais
Número de telefone para contato	Número de telefone da pessoa de contato
Endereço de e-mail de contato	Endereço de e-mail da pessoa de contato
Tipo de evento*	Classificação de evento abaixo do nível de categoria
Status do evento*	Instruções de manipulação de eventos
Escopo do evento*	Público alvo desejado para a mensagem
Restrição	Informações adicionais necessárias quando o escopo é 'Restrito'
Título*	Breve descrição do evento
Categoria*	Classificação de evento de alto nível
Gravidade*	Intensidade do impacto do evento
Certeza*	Confiança na predição do evento
Urgência*	Intervalo de tempo para ação em resposta ao evento
Tipo de mensagem	Natureza da mensagem
Descrição	Descrição adicional do evento
Endereço da Web	Endereço da Web para obter informações adicionais sobre o evento
Data / hora de envio*	Data e hora em que a mensagem foi enviada
Data / hora efetiva	Data e hora em que a mensagem está efetiva
Data / hora de início	Data e hora em que o evento está previsto para começar
Data / hora de expiração	Data e hora em que o evento está previsto para terminar
Descrição da área	Descrição da área afetada
Latitude / Longitude	Coordenadas da localização do evento

**Nota:** As propriedades marcadas com um asterisco são necessárias para a criação bem sucedida de um novo evento, aquelas que não estão marcadas com um asterisco são opcionais.

## Trabalhando com a Lista

A partir da barra de ação na parte superior da lista, é possível executar as tarefas a seguir.

- Para atualizar o conteúdo da lista, clique em **Atualizar**.
- Para exportar o conteúdo da lista, selecione uma **Opção de Exportação** para a lista:
  - Exportar como HTML
  - Exportar tudo para CSV
- Para imprimir o conteúdo da lista, selecione **Opções de Impressão** para a lista:
  - Imprimir tudo
  - Imprimir selecionado
  - Imprimir visualização

- Para selecionar quais colunas serão mostradas, clique em **Configurar Opções** e selecione as caixas de seleção.
- Para selecionar quais linhas serão mostradas, clique em **Filtro Avançado** para filtrar linhas de acordo com as regras definidas. As regras podem ser inseridas pela coluna, condição e palavra-chave. Como alternativa, insira uma palavra-chave no campo de filtro rápido. A barra de filtro localizada na parte superior da lista indica se foi aplicado um filtro e o número de linhas mostradas com relação ao total.
- Para limpar o filtro, clique em **Limpar Filtro**. Como alternativa, clique no botão à esquerda do campo de filtro rápido.

Um contador na barra de ação no final da lista indica o número de itens exibidos e o número total de itens. O número de itens que podem ser exibidos é limitado a 25. Se houver mais linhas do que pode ser exibido de uma vez, é possível avançar ou retroceder páginas clicando nos botões na barra de ação no final da lista.

## Gerenciando Eventos Existentes

É possível visualizar ou editar detalhes de um evento, alterar o status de um evento ou cancelar um evento na lista.

### Procedimento

1. Clique com o botão direito do mouse em uma linha na lista de eventos e selecione uma opção a partir do menu:
  - Para atualizar as informações sobre um evento, selecione **Atualizar Evento** para exibir o diálogo. Isso resulta em uma mudança no tipo de mensagem para atualizar.
  - Para alterar o status do evento para incidente, selecione **Escalar para Incidente**. Isso resulta em uma mudança nas propriedades do tipo de código e de mensagem e em um ícone diferente no mapa. Quando o evento é um incidente com um fluxo de trabalho associado, é possível selecionar o fluxo de trabalho.
  - Para cancelar um evento, selecione **Cancelar Evento**. O evento é removido da lista e do mapa.
  - A opção é apenas disponível.
  - Para visualizar as informações sobre um evento, selecione **Propriedades** para exibir a janela pop-up.
2. Clique em **OK** ou **Cancelar**.

## Incluindo um Evento

É possível criar um evento, incluindo-o na lista de portlets Ocorrências. Quando são fornecidos detalhes sobre a localização, o evento é incluído no mapa do portlet Mapa ao mesmo tempo. Também há uma opção para criar um evento a partir do portlet Mapa. Clique com o botão direito em um local no mapa para obter as coordenadas concluídas automaticamente.

### Procedimento

1. Clique em **Incluir Evento** para exibir o diálogo. Muitas das propriedades de evento são concluídas automaticamente. O tipo de mensagem é configurado como alerta. A data e hora de envio podem ser alteradas.
2. Especifique as propriedades de evento restantes usando campos no diálogo.
3. Clique em **OK** para salvar o evento ou em **Cancelar** para parar a inclusão do evento.

## Resultados

Os principais detalhes para o evento são incluídos na lista de portlets Ocorrências, e o ícone para o novo evento aparece no mapa se as coordenadas tiverem sido inseridas.

Para obter mais informações sobre o uso da interface da solução, clique em **Ajuda** no canto superior direito da página do navegador.

Para obter mais informações sobre a administração e customização da solução, acesse IBM Intelligent Operations Center .

## Coordenador - Alertas

Use o portlet Coordenador - Alertas para visualizar as mensagens de alerta e os seus detalhes.

### O que é o Portlet Coordenador - Alertas?

O portlet Coordenador - Alertas é uma janela interativa contendo uma lista de todos os alertas atuais relevantes para você. São visualizados apenas os alertas que foram enviados aos seus grupos de usuários. Alertas são notificações recebidas quando:

- Diversos eventos estão acontecendo nas mesmas adjacências e em horários semelhantes, logo, podem estar em conflito ou pode ser necessária coordenação
- Uma mudança de valor de Key Performance Indicator (KPI) predefinido ocorre onde essa mudança tiver sido definida como um acionador de alerta pelo administrador

É possível também usar o portlet Coordenador - Alertas para exibir mais detalhes de um alerta.

### O que este portlet exibe?

O portlet Coordenador - Alertas fornece uma lista dinâmica e interativa de alertas que resultam da mudança de KPIs e de eventos correlatos. A função desse portlet é advertir sobre mudanças no KPI ou status do evento. A lista contém detalhes chave para cada um dos alertas.

Para mostrar uma descrição mais detalhada de um alerta, passe o cursor do mouse sobre a linha. Para consultar todas as informações associadas àquele alerta em uma janela pop-up, clique com o botão direito do mouse na linha e selecione **Propriedades**.

Inicialmente, quando uma página de portal é aberta, o portlet Coordenador - Alertas exibe todos os alertas atuais. Remova qualquer alerta a partir do portlet clicando com o botão direito do mouse na linha e selecionando **Fechar alerta**. É possível fechar diversos alertas dessa maneira ao selecionar diversas linhas. Apenas feche um alerta após tê-lo tratado adequadamente, pois ao ser fechado, o alerta será removido para todos os destinatários.

Clique no botão no canto superior direito da janela pop-up para cancelá-lo e retornar à lista.



## Propriedades do Alerta

A janela pop-up dos detalhes do alerta exibe as seguintes propriedades:

Tabela 31. Propriedades do Alerta

Propriedade	Conteúdo
Título	Breve descrição do alerta
Categoria	Classificação de alto nível do evento ou KPI
Emissor	Origem do alerta
Enviado aos Grupos	Grupos para os quais o alerta foi enviado
Enviado	Data e hora em que o alerta foi enviado
Descrição	Descrição adicional do alerta
Refere-se a Alertas	Identificador de ocorrência, se o alerta foi causado pelas ocorrências correlatas
Refere-se a KPIs	Nome do KPI, se o alerta foi causado por uma mudança de valor de KPI

## Trabalhando com a Lista

A partir da barra de ação na parte superior da lista, é possível executar as tarefas a seguir.

- Para atualizar o conteúdo da lista, clique em **Atualizar**.
- Para exportar o conteúdo da lista, selecione uma **Opção de Exportação** para a lista:
  - Exportar como HTML
  - Exportar tudo para CSV
- Para imprimir o conteúdo da lista, selecione **Opções de Impressão** para a lista:
  - Imprimir tudo
  - Imprimir selecionado
  - Imprimir visualização
- Para selecionar quais colunas serão mostradas, clique em **Configurar Opções** e selecione as caixas de seleção.
- Para selecionar quais linhas serão mostradas, clique em **Filtro Avançado** para filtrar linhas de acordo com as regras definidas. As regras podem ser inseridas pela coluna, condição e palavra-chave. Como alternativa, insira uma palavra-chave no campo de filtro rápido. A barra de filtro localizada na parte superior da lista indica se foi aplicado um filtro e o número de linhas mostradas com relação ao total.
- Para limpar o filtro, clique em **Limpar Filtro**. Como alternativa, clique no botão à esquerda do campo de filtro rápido.

Um contador na barra de ação no final da lista indica o número de itens exibidos e o número total de itens. O número de itens que podem ser exibidos é limitado a 25. Se houver mais linhas do que pode ser exibido de uma vez, é possível avançar ou retroceder páginas clicando nos botões na barra de ação no final da lista.

Para obter mais informações sobre o uso da interface da solução, clique em **Ajuda** no canto superior direito da página do navegador.

Para obter mais informações sobre a administração e customização da solução, acesse IBM Intelligent Operations Center .

## Contatos do Sametime

O portlet Contatos do Sametime autoriza o uso do sistema de mensagens instantâneas do IBM Lotus Sametime no IBM Intelligent Operations Center.

### O que é o Portlet Contatos do Sametime?

O portlet Contatos do Sametime fornece uma lista de contatos organizada por grupo. Ela pode ser customizada com base nas pessoas com as quais você precisa se comunicar. É possível conversar com pessoas e modificar status, contatos ou grupos on-line.

### O que este portlet exibe?

A lista que aparece em Contatos do Sametime quando você efetua logon pela primeira vez depende da maneira como a organização configurou grupos no IBM Intelligent Operations Center.

Use os menus suspensos na parte superior do portlet para trabalhar com a lista.

- Use o menu **Pessoas** para incluir contatos ou modificar grupos.
- Use o menu **Opções** para modificar a mensagem de status ou visualizar apenas as pessoas que estão on-line.

Para obter ajuda mais detalhada sobre como usar o portlet Contatos do Sametime, clique no menu de exibição suspenso no canto direito da parte superior do portlet e selecione **Ajuda**.

---

## Capítulo 8. Resolução de Problemas e Suporte

Para isolar e resolver problemas com o software IBM, é possível usar informações de resolução de problemas e de suporte, que contêm instruções sobre utilização de recursos de determinação do problema que são fornecidos com os produtos IBM.

---

### Resolvendo um Problema

As informações a seguir apresentam uma abordagem sistemática para resolução de problemas. O objetivo da resolução de problemas é determinar o motivo de algo não funcionar conforme esperado e como resolver o problema.

A primeira etapa no processo de resolução de problemas é descrever o problema por completo. A descrição do problema irá ajudá-lo e também ao representante de suporte técnico IBM a saber por onde começar a localizar a causa do problema. Esta etapa inclui responder as seguintes perguntas:

- Quais São os Sintomas do Problema?
- Onde Ocorre o Problema?
- Quando o Problema Ocorre?
- Sob Quais Condições o Problema Ocorre?
- É Possível Reproduzir o Problema?

As respostas a essas perguntas geralmente resultam em uma boa descrição do problema, que por sua vez pode levá-lo à uma resolução de problema.

#### Quais São os Sintomas do Problema?

Ao começar a descrever um problema, a pergunta mais óbvia é “Qual é o problema?” Esta pergunta pode parecer mais simples; no entanto, é possível dividi-la em várias perguntas mais objetivas que apresentam um panorama mais descritivo para o problema. Essas perguntas podem incluir:

- Quem ou o que está relatando o problema?
- Quais são os códigos de erros e mensagens?
- Como ocorre a falha do sistema? Por exemplo, é um loop, interrupção, paralisação, queda no desempenho ou resultado incorreto?

#### Onde Ocorre o Problema?

Determinar a origem do problema nem sempre é fácil, mas é uma das etapas mais importantes na resolução de um problema. Várias camadas de tecnologia podem existir entre o relatório e os componentes com falha. Redes, discos e unidades são apenas alguns dos componentes que devem ser considerados ao investigar problemas.

As perguntas a seguir podem ajudá-lo a se concentrar no local de origem do problema para isolar a camada do problema:

- O problema é específico a uma plataforma ou sistema operacional ou é comum a diversas plataformas ou sistemas operacionais?
- O ambiente e configuração atuais são suportados?

O fato de uma camada relatar o problema não significa que o problema tem origem nessa camada. Parte da ação de identificar a origem de um problema é compreender o ambiente em que ele existe. Não tenha pressa em descrever o ambiente com problema por inteiro, incluindo o sistema operacional e versão, todos os produtos de software e versões correspondentes e informações de hardware. Confirme que o ambiente está em execução em uma configuração suportada; muitos problemas têm origem em níveis incompatíveis de software que não devem ser executados juntos ou que não foram completamente testados para execução em conjunto.

## **Quando o Problema Ocorre?**

Desenvolva uma linha de tempo detalhada que o leve até a falha, especialmente nos casos que são ocorrências únicas. A maneira mais fácil de desenvolver uma linha de tempo é começar pelo fim: Comece pelo momento em que o erro foi reportado (sendo o mais preciso possível, incluindo milissegundos) e continue pelos logs e informações disponíveis. Geralmente, basta chegar no primeiro evento suspeito encontrado em um log de diagnóstico.

Para desenvolver uma linha de tempo detalhada de eventos, responda estas perguntas:

- O problema ocorre apenas em determinada hora do dia ou da noite?
- Em qual frequência o problema ocorre?
- Qual foi sequência de eventos até o momento em que o problema foi relatado?
- O problema ocorre após uma alteração de ambiente, como upgrade ou instalação de software ou hardware?

Responder a esse tipo de perguntas pode oferecer uma boa perspectiva de como investigar o problema.

## **Sob Quais Condições o Problema Ocorre?**

Saber quais sistemas e aplicativos estavam em execução no momento em que o problema ocorreu é uma parte importante da resolução do problema. Essas perguntas sobre o seu ambiente podem ajudá-lo a identificar a causa-raiz do problema:

- O problema sempre ocorre quando a mesma tarefa é executada?
- Uma determinada sequência de eventos precisa ser seguida para que o problema ocorra?
- Algum outro aplicativo sofre falhas no mesmo momento?

Responder a esse tipo de pergunta pode ajudá-lo a explicar o ambiente em que o problema ocorre e correlacionar quaisquer dependências. Lembre-se que o fato de diversos problemas ocorrerem ao mesmo tempo não significa que os problemas estejam necessariamente relacionados.

## **É Possível Reproduzir o Problema?**

A partir de uma perspectiva de resolução de problemas, o problema ideal é aquele que pode ser reproduzido. Geralmente, quando um problema pode ser reproduzido, você tem à sua disposição um conjunto maior de ferramentas ou procedimentos para ajudá-lo na investigação. Consequentemente, problemas que podem ser reproduzidos muitas vezes são mais fáceis de serem depurados e resolvidos. No entanto, problemas que podem ser reproduzidos possuem uma

desvantagem: Se o problema tiver um impacto comercial significativo, você provavelmente não desejará que ele ocorra novamente. Se possível, recrie o problema em um ambiente de teste ou desenvolvimento, onde existe maior flexibilidade e controle durante a investigação.

- É possível recriar o problema em um sistema de teste?
- O mesmo tipo de problema está sendo encontrado por diversos usuários ou aplicativos?
- O problema pode ser recriado por meio da execução de um único comando, um conjunto de comandos ou um aplicativo específico?

#### **Informações Relacionadas**

“Procurando Bases de Conhecimento”

É possível localizar soluções para problemas, frequentemente, pesquisando as bases de conhecimento da IBM. É possível otimizar resultados utilizando os recursos, ferramentas de suporte e métodos de procura disponíveis.

---

## **Procurando Bases de Conhecimento**

É possível localizar soluções para problemas, frequentemente, pesquisando as bases de conhecimento da IBM. É possível otimizar resultados utilizando os recursos, ferramentas de suporte e métodos de procura disponíveis.

### **Sobre Esta Tarefa**

Você poderá encontrar informações úteis procurando por IBM Intelligent Operations Center no centro de informações; no entanto, algumas vezes será necessário procurar além do centro de informações para encontrar as respostas necessárias e resolver seus problemas.

### **Procedimento**

Para procurar as informações necessárias nas bases de conhecimento, utilize uma ou mais das abordagens a seguir:

- Localize o conteúdo necessário utilizando o IBM Support Portal.  
O IBM Support Portal é uma visualização única e centralizada com todas as ferramentas e informações de suporte técnico para todos os sistemas, produtos de software e serviços IBM. O IBM Support Portal permite acessar o portfólio de suporte eletrônico da IBM a partir de um único lugar. É possível ajustar as páginas para concentrar as informações e recursos necessários para prevenção e resolução mais rápida de problemas. Familiarize-se com o IBM Support Portal visualizando os vídeos de demonstração ([https://www.ibm.com/blogs/SPNA/entry/the\\_ibm\\_support\\_portal\\_videos](https://www.ibm.com/blogs/SPNA/entry/the_ibm_support_portal_videos)) sobre esta ferramenta. Esses vídeos apresentam o IBM Support Portal, exploram a resolução de problemas e outros recursos e demonstram como ajustar a página ao mover, incluir e excluir portlets.
- Procure conteúdo sobre o IBM Intelligent Operations Center usando um dos recursos técnicos adicionais a seguir:
  - Notas Técnicas e APARs (Relatórios de Problemas) do IBM Intelligent Operations Center
  - Página de Portal de Suporte do IBM Intelligent Operations Center
  - Página de Fóruns e Comunidades do IBM Intelligent Operations Center
- Procure conteúdo usando a procura por cabeçalhos principais IBM. É possível usar a procura do cabeçalho principal IBM digitando sua sequência de procura no campo Procura na parte superior de qualquer página [ibm.com](http://ibm.com).

- Procure conteúdo usando qualquer mecanismo de procura externo, como Google, Yahoo ou Bing. Se você usar um mecanismo de procura externo, seus resultados provavelmente incluirão informações que estão fora do domínio ibm.com. Entretanto, algumas vezes é possível localizar informações úteis na resolução de problemas sobre os produtos IBM em grupos de notícias, fóruns e blogs que não estão na página ibm.com.

**Dica:** Inclua “IBM” e o nome do produto em sua procura se estiver procurando informações sobre um produto IBM.

---

## Entrando em Contato com o Suporte IBM

O Suporte IBM fornece assistência para correção de defeitos no produto, responder perguntas frequentes e realizar redescoberta.

### Antes de Iniciar

Após tentar encontrar sua resposta ou solução por meio de outras opções de ajuda como notas técnicas, entre em contato com o Suporte IBM. Antes de entrar em contato com o Suporte IBM, sua empresa deve ter uma assinatura de software IBM e contrato de suporte ativos; além disso, você deve estar autorizado a enviar problemas para a IBM. Para obter informações sobre os tipos de suporte disponíveis, consulte o tópico Support portfolio no *Software Support Handbook*.

### Procedimento

Conclua as etapas a seguir para entrar em contato com o Suporte IBM para resolver um problema:

1. Defina o problema, reúna informações de histórico e determine a gravidade do problema. Para obter informações adicionais, consulte o tópico Getting IBM support no *Software Support Handbook*.
2. Reúna informações de diagnóstico.
3. Envie o problema para o Suporte IBM através de uma das maneiras a seguir:
  - On-line por meio do Página de Portal de Suporte do IBM Intelligent Operations Center: É possível abrir, atualizar e visualizar todas as suas Solicitações de Serviços a partir do portlet Solicitações de Serviço na página Solicitação de Serviço.
  - Por telefone: para obter o número de telefone para contato em sua região, consulte a página da Web Directory of worldwide contacts.

### Resultados

Caso o problema enviado seja a respeito de um defeito de software ou de uma documentação ausente ou com informações incorretas, o Suporte IBM criará um Authorized Program Analysis Report (APAR). O APAR descreve o problema em detalhes. Sempre que possível, o Suporte IBM oferece uma solução que pode ser implementada até que o APAR seja resolvido e uma correção seja entregue. A IBM publica APARs resolvidos no Web site de Suporte IBM diariamente, para que outros usuários que tenham o mesmo problema possam beneficiar da mesma solução.

### O que Fazer Depois

Esteja preparado para trabalhar com o representante de suporte técnico IBM utilizando o IBM Assist On-Site, um plug-in de assistência remota que pode ser

transferido por download para o seu computador. O representante de suporte técnico IBM pode usar a ferramenta IBM Assist On-Site para visualizar sua área de trabalho e compartilhar o controle de seu mouse e teclado. Esta ferramenta pode reduzir o tempo necessário para identificar o problema, coletar os dados necessários e resolver o problema. Para obter informações adicionais, consulte IBM Assist On-Site.

---

## Trocando Informações com a IBM

Para diagnosticar ou identificar um problema, pode ser necessário fornecer dados e informações sobre o seu sistema ao Suporte IBM. Em outros casos, o Suporte IBM pode fornecer ferramentas ou utilitários a serem usados na determinação de problemas.

### Enviando Informações ao Suporte IBM

Para reduzir o tempo de resolução do problema, é possível enviar informações de rastreamento e diagnóstico ao Suporte IBM.

#### Procedimento

Para enviar informações de diagnóstico para o Suporte IBM:

1. Abra um Problem Management Record (PMR) usando a ferramenta Service Request.
2. Colete manualmente os dados de diagnóstico necessários. Os dados de diagnóstico ajudam a reduzir o tempo necessário para resolver seu PMR.
3. Compacte os arquivos usando formato ZIP ou TAR.
4. Transfira os arquivos para a IBM. Você poderá utilizar um dos seguintes métodos para transferir os arquivos para a IBM:
  - Ferramenta Service Request
  - Métodos tradicionais de upload de dados: FTP, HTTP
  - Métodos seguros de upload de dados: FTPS, SFTP, HTTPS
  - E-mail

Todos esses métodos de troca de dados são explicados no Web site IBM Support.

### Recebendo Informações do Suporte IBM

Ocasionalmente, um representante de suporte técnico da IBM pode solicitar que você faça o download de ferramentas de diagnóstico ou outros arquivos. É possível usar FTP para fazer o download desses arquivos.

#### Antes de Iniciar

Assegure que seu representante de suporte técnico IBM tenha fornecido o servidor preferencial para download dos arquivos e o diretório e nome de arquivo exatos a serem acessados.

#### Procedimento

Para fazer o download dos arquivos do Suporte IBM:

1. Utilize o FTP para conectar-se ao site fornecido pelo representante de suporte técnico IBM e efetue login anônimo. Utilize seu endereço de e-mail como senha.
2. Acesse o diretório apropriado:

- a. Acesse o diretório /fromibm.  
`cd fromibm`
- b. Mude para o diretório fornecido pelo representante de suporte técnico IBM.  
`cd nameofdirectory`
3. Ative o modo binário para sua sessão.  
`binary`
4. Use o comando **get** para fazer download do arquivo especificado por seu representante de suporte técnico IBM.  
`get nomearquivo.extensão`
5. Encerre sua sessão FTP.  
`quit`

---

## Assinando Atualizações de Suporte

É possível assinar para obter atualizações para manter-se informado sobre os produtos IBM que você usa.

### Sobre Esta Tarefa

Ao assinar o recebimento de atualizações, você receberá importantes informações técnicas e atualizações para recursos e ferramentas específicos do Suporte IBM. É possível assinar atualizações usando uma de duas abordagens:

#### Alimentações RSS

A alimentação RSS a seguir está disponível para o IBM Intelligent Operations Center: *IBM Intelligent Operations Center for Smarter Cities*.

Para obter informações gerais sobre RSS, incluindo etapas para iniciar e uma lista de páginas da Web da IBM ativadas para RSS, visite o site Alimentações RSS de Suporte de Software IBM.

#### Minhas Notificações

Com as Minhas Notificações, é possível assinar atualizações do Suporte para qualquer produto IBM. (As Minhas Notificações substituem o Meu Suporte, que é uma ferramenta semelhante que você pode ter usado no passado). Com as Minhas Notificações, é possível especificar se deseja receber anúncios por e-mail diariamente ou semanalmente. É possível especificar que tipo de informações deseja receber (tais como publicações, dicas, atualizações de produtos (também conhecidas como alertas), downloads e drivers). As Minhas Notificações permitem que você customize e categorize os produtos sobre os quais deseja ser informado e os métodos de entrega que melhor se adaptam a suas necessidades.

### Procedimento

Para assinar as atualizações do Suporte:

1. Para assinar a alimentação RSS do *IBM Intelligent Operations Center for Smarter Cities*, use as subetapas a seguir:
  - a. Abra o link Alimentação RSS do IBM Intelligent Operations Center for Smarter Cities.
  - b. Na janela Assinar com Live Bookmark, selecione uma pasta na qual deseja salvar o marcador de alimentação RSS e clique em **Assinar**.







Para obter informações adicionais sobre como assinar alimentações RSS, consulte o link Alimentações RSS de Suporte de Software IBM na seção Informações Relacionadas no final do tópico.

2. Para assinar as Minhas Notificações, acesse o IBM Support Portal e clique em **Minhas Notificações** no portlet **Notificações**.
3. Efetue sign in usando seu ID e senha da IBM e clique em **Enviar**.
4. Identifique sobre o que e como deseja receber atualizações.
  - a. Clique na guia **Assinar**.
  - b. Selecione IBM Intelligent Operations Center e clique em **Continuar**.
  - c. Selecione suas preferências de como receber atualizações: por e-mail, on-line em uma pasta designada ou como um feed RSS ou Atom.
  - d. Selecione os tipos de atualizações de documentação que deseja receber, por exemplo, novas informações sobre downloads do produto e comentários do grupo de discussão.
  - e. Clique em **Enviar**.

## Resultados

Até modificar suas preferências de alimentações RSS e de Minhas Notificações, você recebe notificações de atualizações solicitadas. É possível modificar suas preferências quando necessário (por exemplo, se você parar de usar um produto e começar a usar outro produto).

### Informações Relacionadas

-  Alimentações RSS de Suporte de Software IBM
-  Assine as atualizações de conteúdo de suporte Minhas Notificações
-  Minhas notificações para o suporte técnico IBM
-  Minhas notificações para a visão geral do suporte técnico IBM

---

## Dicas de Resolução de Problemas

Esta seção contém uma lista de problemas que ocorrem comumente e algumas dicas de resolução de problemas para cada item.

### Trabalhar com o Portlet Sametime Causa o Recarregamento de outros Portlets

No portlet Sametime, se estiver trabalhando com contatos, clicar no menu Pessoas ou Opções faz com que todos os outros portlets sejam recarregados. Para evitar distração pela atividade dos outros portlets, maximize o portlet Sametime enquanto estiver trabalhando com ele. Enquanto o portlet Sametime é maximizado, os outros portlets ainda são recarregados, mas a atividade está oculta da visualização.



---

## Capítulo 9. Referências

Esses tópicos contêm informações de referência adicionais para ajudá-lo.

---

### Biblioteca em PDF

Este tópico fornece links para o conteúdo do centro de informações em formato PDF.

O conteúdo do centro de informações está disponível no seguinte PDF para a impressão conveniente:

- Centro de Informações do IBM Intelligent Operations Center

---

### Informações Adicionais

Os seguintes recursos adicionais estão disponíveis on-line.

#### WebSphere Portal

- Página de suporte do produto WebSphere Portal: [http://www.ibm.com/support/entry/portal/Overview/Software/WebSphere/WebSphere\\_Portal](http://www.ibm.com/support/entry/portal/Overview/Software/WebSphere/WebSphere_Portal)
- Biblioteca de informações do WebSphere Portal: <http://www.ibm.com/software/genservers/portal/library/>
- Wiki do WebSphere Portal: <http://www.lotus.com/ldd/portalwiki.nsf>

#### WebSphere Application Server

- Página de suporte do produto WebSphere Application Server: <http://www.ibm.com/software/webservers/appserv/was/support/>
- Biblioteca de informações do WebSphere Application Server: <http://www.ibm.com/software/webservers/appserv/was/library/index.html>
- Centro de Informações do WebSphere Application Server 7.0.x: <http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp>

#### Centros de Informações

- Centro de informações do WebSphere Application Server 7.0.x: <http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp>
- Centro de informações do Tivoli Service Request Manager: [http://publib.boulder.ibm.com/infocenter/tivihelp/v32r1/index.jsp?topic=com.ibm.srm.doc/srm\\_welcome.htm](http://publib.boulder.ibm.com/infocenter/tivihelp/v32r1/index.jsp?topic=com.ibm.srm.doc/srm_welcome.htm)
- Centro de informações do Lotus Notes: <http://publib.boulder.ibm.com/infocenter/domhelp/v8r0/index.jsp>
- Centro de informações do WebSphere Message Broker: <http://publib.boulder.ibm.com/infocenter/wmbhelp/v7r0m0/index.jsp>
- Centro de informações do IBM Business Monitor: <http://publib.boulder.ibm.com/infocenter/dmndhelp/v7r0mx/index.jsp?topic=com.ibm.btools.help.monitor.doc/home/home.html>
- Centro de informações do Rational Application Developer: [http://publib.boulder.ibm.com/infocenter/radhelp/v7r5/index.jsp?topic=com.ibm.rad.legal.doc/helpindex\\_rad.html](http://publib.boulder.ibm.com/infocenter/radhelp/v7r5/index.jsp?topic=com.ibm.rad.legal.doc/helpindex_rad.html)

## Redbooks

- Domínio Redbooks: <http://publib-b.boulder.ibm.com/Redbooks.nsf>

## Outros Recursos da Web

- Treinamento e certificação do Tivoli: <http://www.ibm.com/software/tivoli/education/>
- OASIS Protocolo de Alerta Comum Versão 1.2 <http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2-os.html>
- Web site do Red Hat: <http://www.redhat.com/>

---

## Aviso de Copyright e Marcas Registradas

### Aviso de Copyright

© Copyright IBM Corporation 2011. Todos os direitos reservados. Pode ser utilizado somente mediante um Contrato de Licença de Software da IBM. Nenhuma parte desta publicação poderá ser reproduzida, transmitida, transcrita, armazenada em um sistema de recuperação ou convertida em qualquer linguagem de computador em hipótese alguma, seja por meio eletrônico, mecânico, magnético, ótico, químico, manual ou de outra maneira, sem permissão expressa, por escrito, da IBM Corporation. A IBM Corporation concede ao Cliente permissão limitada para fazer cópia impressa ou outras reproduções de qualquer documentação lida por máquina para utilização própria, contanto que cada reprodução contenha o aviso de direitos autorais da IBM Corporation. Não será concedido nenhum outro direito autoral sem permissão prévia, por escrito, da IBM Corporation. O documento não é destinado para uso de produção e é fornecido “no estado em que se encontra” sem garantia de nenhum tipo. **Todas as garantias são, deste modo, renunciadas, incluindo as garantias de comercialização e adequação a um determinado propósito.**

Direitos Restritos para Usuários do Governo dos Estados Unidos -- Uso, duplicação ou divulgação restritos pelo documento GSA ADP Schedule Contract com a IBM Corporation.

### Marcas Registradas

IBM, WebSphere, DB2, Rational, Tivoli, ibm.com, Passport Advantage, Sametime e Redbooks são marcas registradas da IBM Corporation nos Estados Unidos e/ou em outros países.

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

Pentium é uma marca registrada da Intel Corporation ou suas subsidiárias nos Estados Unidos e/ou em outros países

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

Adobe, Acrobat, Portable Document Format (PDF), e PostScript são marcas ou marcas registradas da Adobe Systems Incorporated nos Estados Unidos e/ou em outros países.

Oracle, Javascript e Java são marcas registradas da Oracle e/ou suas afiliadas.

ArcGIS, EDN, StreetMap, @esri.com e www.esri.com são marcas, marcas registradas ou marcas de serviço da Esri nos Estados Unidos, na Comunidade Européia ou outras jurisdições específicas.

Outros nomes podem ser marcas registradas de seus respectivos proprietários. Outros nomes de empresas, produtos e serviços podem ser marcas registradas ou marcas de serviço de terceiros.



---

## Comentários do Leitor

**IBM Intelligent Operations Center**  
**Centro de Informações do IBM Intelligent Operations Center**  
**Versão 1.0**

Neste formulário, faça-nos saber sua opinião sobre este manual. Utilize-o se encontrar algum erro, ou se quiser externar qualquer opinião a respeito (tal como organização, assunto, aparência...) ou fazer sugestões para melhorá-lo.

Para pedir publicações extras, fazer perguntas ou tecer comentários sobre as funções de produtos ou sistemas IBM, fale com o seu representante IBM.

Quando você 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 você.

Não se esqueça de preencher seu nome e seu endereço abaixo, se deseja resposta.

Comentários:

---

Nome

---

Endereço

---

Companhia ou Empresa

---

Telefone

IBM Corporation  
Information Development  
Department DLUA  
P.O. Box 12195  
Research Triangle Park, NC