

IBM Intelligent Operations Center



IBM Intelligent Operations Center Documentação do Produto

Versão 1 Release 5

IBM Intelligent Operations Center



IBM Intelligent Operations Center Documentação do Produto

Versão 1 Release 5

Nota

Antes de usar essas informações e o produto suportado, leia as informações em “Avisos” na página 359.

Esta edição aplica-se a IBM Intelligent Operations Center versão 1, release 5, modificação 0. Esta edição aplica-se a todos os releases e modificações subsequentes, até que seja indicado de outra forma em novas edições.

© Copyright IBM Corporation 2011, 2012.

Índice

Figuras vii

Capítulo 1. Visão Geral da Solução . . . 1

Público-Alvo	1
Recursos	2
Usuários e Benefícios	3
Componentes	5
Gerenciamento de Ocorrências	7
O Que Há de Novo na Versão 1.5	8
O Que Há de Novo para o Usuário	8
O Que Há de Novo para o Administrador	9

Capítulo 2. Instalando e Configurando 11

Preparando para Instalação	11
Serviços do Sistema do IBM Intelligent Operations Center	11
Requisitos de Hardware do IBM Intelligent Operations Center	12
Requisitos de Software Obrigatório	13
Navegadores Suportados	13
Pacotes de Mídia	14
Listas de Verificação de Instalação	14
Lista de Verificação - Instalação Usando o IBM Installation Manager	14
Lista de Verificação - Instalação Passo-a-Passo	15
Preparando os Servidores	17
Rede TCP/IP	20
Copiando o Pacote de Instalação para o servidor de instalação	23
Instalando O Java Runtime Environment	24
Instalando o IBM Intelligent Operations Center	
Utilizando o Installation Manager	25
Componentes de Instalação	28
Opções de Configuração	29
Reiniciando a Instalação Utilizando o Installation Manager	32
Passo-a-Passo da Instalação do IBM Intelligent Operations Center	32
Preparando o Pacote de Instalação	32
Verificando os Scripts de Instalação	33
Customizando as Propriedades de Instalação	33
Instalação de Arquivos de Topologia	34
Executando a Ferramenta de Pré-Verificação	41
Configurações de Segurança do Linux	42
O Comando installTopology	43
Opções de Instalação dos Componentes do IBM Intelligent Operations Center	44
Reiniciando a Instalação de Arquitetura do IBM Intelligent Operations Center Durante uma Instalação Passo-a-Passo	47
Instalando o Ferramenta de Controle de Plataforma	47
Instalando a Ferramenta de Verificação do Sistema	48

Instalando o aplicativo do IBM Intelligent Operations Center	49
Verificando a instalação	50
Configuração da Pós-Instalação do IBM Intelligent Operations Center	51
Configurando os Serviços de Colaboração para IPv6	51
Configurando Conexão Única para Serviços de Colaboração	52
Configurando o Tempo Limite da Sessão	53
Instalando e Configurando o serviços de modelo semântico	54
Configurando o Ferramenta de Controle de Plataforma	58
Criptografando a Senha Administrativa do Tivoli Service Request Manager	58
Configurando o Número Mínimo de Encadeamentos para o EventProcessor	59
Mudando o Tamanho do Conjunto de Encadeamentos Padrão e do Contêiner da Web	60
Instalando e Executando o Cyber Hygiene Passo a Passo	60
Mudanças no Sistema Operacional Linux	62
Revisando o Log do Cyber Hygiene	62
Reativando Logon de Raiz Remoto	63
Configurando Usuários que Requerem Acesso ssh	64
Instalando Ferramentas Fornecidas com a Solução	64
Excluindo Usuários de Amostra	65
Removendo os Serviços de Instalação do Sistema de Produção	66

Capítulo 3. Protegendo a Solução . . . 67

Funções e Acesso do Usuário	68
Usuários de Amostra	69
Grupos de Funções de Usuários e Permissões de Autorização	70
Grupo de Categorias de Usuários e Permissões de Dados	73
Incluindo um Usuário ou Grupo	74
Visualizando ou Modificando a Associação ao Grupo	76
Visualizando ou Editando um Perfil de Usuário	77
Excluindo um Usuário ou Grupo	77
Importando Usuários e Grupos	78
Resumo de Permissões do Usuário	79
Visão Geral do Cyber Hygiene	80
Segurança Cibernética	81
Listas de Verificação do Cyber Hygiene	82
Configuração Padrão do Cyber Hygiene	84
Ferramentas de Correção	88
Documentação do Cyber Hygiene	88

Capítulo 4. Integrando a Solução . . . 91

Exemplos de sistemas que podem ser integrados	91
Pontos de integração e protocolos	91

Eventos e KPIs	91
Integrando ao Common Alerting Protocol	93
Criando Eventos Utilizando o Serviço do	
Publicador	100
Criando e Publicando Eventos de Teste.	103
Publicador de Amostra	103
Script do Evento	107
Criando e Integrando KPIs	109
Monitorar Modelos e KPIs	110
Instâncias do Contexto de Monitoramento	111
Modelando KPIs	111
Definindo Hierarquias de KPI	114
Definindo Hierarquias do KPI com OWL	115
Comunicação de Evento de KPI Entre o IBM	
WebSphere Business Monitor e o IBM Intelligent	
Operations Center	116
Implementando Modelos de Monitor	119
Valores de Exibição de KPI	120
Armazenamento em Cache de KPIs	121
KPIs de Amostra	121
Configurando o Tivoli Service Request Manager	123
Utilizando a Interface com o Usuário do Tivoli	
Service Request Manager	124
Configurando Novos Usuários no Tivoli Service	
Request Manager	126
Procedimentos Padrão de Operação	127
Gerenciamento de recursos	132
procedimentos padrão de operação, fluxos de	
trabalho de Amostra e Recursos	138

Capítulo 5. Customizando a Solução 141

Customizando a Interface com o Usuário	141
Localizando a Interface com o Usuário	141
Lista de Portlets	141
Criando ou Customizando uma Página.	145
Customizando os portlets	145
Customizando a Ajuda do Portlet	165
Locais do Arquivo de Ajuda do Portlet.	166
Customizando KPIs	167
Principais Indicadores de Desempenho	168
Faça Backup Antes de Customizar KPIs	172
Customizando a Correlação de Evento	173
Correlação de Evento e o Aplicativo e Regra	173
Customizando Configurações de Correlação de	
Evento	174
Gerenciador de Mapa de Localização	176
Incluindo uma Classificação no Menu do Mapa	177
Incluindo um Mapa no Portlet.	177
Incluindo ou Alterando Áreas em um Mapa de	
Localização	177
Customizando o Portlet Gerenciador de Mapa	
de Localização	178
Especificando Dados de Configuração para Todo o	
Sistema	178
Atualizando a Tabela de Propriedades do	
Sistema	182
Configurando o IBM Cognos Business Intelligence	
para Criar Relatórios	183
Criando um Portlet Relatórios	183
Editando o Layout do Portlet de Relatórios	184
Customizando um Portlet para Exibir Relatórios	185

Localizando a URL do Relatório	185
Trabalhando com Modelo de Dados	185

Capítulo 6. Gerenciando a Solução 195

Sobre	195
Controlando os Serviços.	195
Iniciando os Serviços	195
Iniciando e Parando a Análise do Tivoli	
Netcool/OMNIBus	199
Parando os Serviços	199
Consultando o Status dos Serviços	202
Obtendo Ajuda para o Ferramenta de Controle	
de Plataforma	203
Consoles de Administração.	203
Gerenciando os Serviços.	206
Verificando os Componentes	210
Como Usar a Ferramenta Verificação do Sistema	210
Testes do Verificação do Sistema	211

Capítulo 7. Manutenção da Solução 259

Fazendo Backup de Dados	259
Ajustando o Desempenho	260
Ajustando o servidor de aplicativos	260
Ajustando o WebSphere Application Server	261
Gerenciando Arquivos de Log.	261
Atualizando o Token LTPA para Conexão Única	261
Dicas de Manutenção.	263

Capítulo 8. Usando a Interface da Solução. 265

Efetuando Logon	265
Efetuando Logoff	266
Visualizando ou Editando o Perfil do Usuário	266
Usando Páginas	267
Visualização Supervisor: Status	267
Visualização Supervisor: Operações	268
Visualização Operator: Operações	269
Supervisor: Relatórios	270
Operator: Relatórios	270
Visualização Mapa de Localização	270
Usando Portlets	271
Contatos	271
Detalhes	272
Gerenciando Eventos e Incidentes	274
Gerenciamento de recursos	275
Customizando o Portlet Detalhes.	275
Drill Down de Key Performance Indicator.	275
Mapa de Localização	276
Controles do Mapa	277
Selecionando Categorias de Evento para o Mapa	278
Customizando o Portlet do Mapa de Localização	279
Mapa	279
Usando os Controles de Mapa.	281
Selecionando as Categorias de Evento do Mapa	282
Selecionando as Capacidades de Recurso do	
Mapa	282
Reconfigurando o mapa	282
Incluindo um Evento	283
Customizando o Portlet Mapa.	284
Minhas Atividades	284

Notificações	286
Relatórios	288
Status	290
Capítulo 9. Resolução de Problemas e Suporte	293
Técnicas para Resolução de Problemas	293
Ativando Rastreios e Visualizando Arquivos de Log.	295
Arquivos de Log do Servidor de aplicativos	295
Arquivos de Log do Servidor de eventos	296
Executando a Ferramenta de Instalação Coleta de Informações	299
Resolução de Problemas dos Componentes	300
Instalando e Usando IBM Support Assistant Lite	303
IBM Intelligent Operations Center Mensagens	304
Usando Bases de Conhecimento e o Suporte IBM	322
Procurando Bases de Conhecimento	322
Obtendo Correções do Fix Central	323
Entrando em Contato com o Suporte IBM	324
Assinando Atualizações de Suporte	325
Trocando Informações com a IBM	326
Problemas Conhecidos e Soluções	328
Erros de Conexão ao Instalar o IBM Intelligent Operations Center	330
A Rede IPv6 Não é Iniciada	330
O Tivoli Service Request Manager não Inicia Não É Possível Criar Nova Página para Interface com o Usuário	331
Soluções Alternativas de Acessibilidade para Portlets	331
Solução Alternativa de Acessibilidade para Seleção de Datas no Portlet Relatórios	332
Novos Eventos Não São Exibidos no Portlet Detalhes	332
Mecanismo de Autenticação não Disponível	334
Servidor de Terceiros não Está Respondendo Nenhuma Atividade É Exibida no Portlet Minhas Atividades	335
Resolução de Problemas com Dados de Amostra Verificando o Status do Tivoli Service Request Manager	336
Verificando Permissões do Usuário	337
Verificando a Associação de um fluxo de trabalho com um procedimento padrão de operação	338
Verificando os Arquivos de Log	339
Dados de KPI Não São Exibidos nos Portlets Status ou Drill Down de Key Performance Indicator	339

Eventos Não São Atualizados nos Portlets Status ou Drill Down de Key Performance Indicator	340
--	-----

Capítulo 10. Referência 341

Produtos e Componentes Incluídos no IBM	
Intelligent Operations Center	341
Processos em Execução na Conta Raiz	342
Exceções do Cyber Hygiene	343
Permissões de Arquivo que Requerem Avaliação do Administrador do Sistema	344
Certificações de Segurança de Produtos e Componentes	345
Biblioteca em PDF.	346
Glossário	346
A	346
B	347
C	347
D	348
E	348
F	349
G	349
H	349
I	350
J.	350
K	351
L	351
M	352
N	352
O	352
P	352
R	353
S	353
T	354
U	354
V	355
W	355
X	356
Informações adicionais do produto	356
Aviso de Copyright e Marcas Registradas	358
Aviso de Copyright	358
Marcas Registradas	358

Avisos 359

Marcas Registradas	361
------------------------------	-----

Índice Remissivo 363

Figuras

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
- Apresentando informações relacionadas de uma maneira coerente

Os benefícios dessa solução são para:

- Ajustar os sistemas para alcançar resultados baseados nos insights ganhos
- 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 se baseia na suposição de que os usuários têm conhecimento prévio ou proficiência no uso de produtos do componente incluídos nessa solução. O centro de informações também se baseia na suposição de que os usuários têm um conhecimento básico do sistema operacional Linux Red Hat Enterprise. O treinamento para os produtos do componente ou sistema operacional está fora do escopo desse 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 Referência; consulte o link no final do tópico.

Conceitos relacionados:

“Informações adicionais do produto” na página 356

Os seguintes recursos adicionais estão disponíveis on-line.

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 instalados em hardware existente (local) 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 do 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 tem recursos de gerenciamento de evento, mapeamento integrado e monitoramento de recursos. A solução pode fornecer e controlar os procedimentos apropriados e o fluxo de trabalho para atividades na preparação para eventos e na resposta a eles. Ele também tem recursos de principal indicador de desempenho (KPI), relatório e colaboração para efetividade aprimorada. Esses recursos fornecem às autoridades a habilidade para integrar domínios para cooperação e tomada de decisão aprimoradas.

Gerenciamento de Eventos e de Incidentes

O IBM Intelligent Operations Center fornece um mecanismo de controle e relatório de eventos para possibilitar a identificação e o entendimento nos domínios subjacentes. É possível gerenciar ocorrências previstas, planejadas e atuais conforme se desenvolvem. Por exemplo, substituir canos que passam sob uma estrada é um evento ou ordem de serviço planejado que envolve ambas as operações, de água e tráfego. Clima severo que deve ocorrer nas próximas 24 horas é um evento previsto. Uma obstrução do tráfego é um evento atual afetado por ambos, os trabalhos na estrada e o clima.

Um integrated geographic information system (GIS) ou plano de localização mapeia os eventos visualmente para você possa medir o impacto de eventos por meio de mapeamento interativo e análise de cenário.

Gerenciamento de Recurso, Resposta e Atividade

O IBM Intelligent Operations Center fornece um sistema para armazenar procedimentos e fluxos de trabalho apropriados baseados em atividades associadas com eventos. É possível controlar o progresso de fluxos de trabalho e monitorar ou atualizar o status de atividades designadas para você.

Informações sobre um intervalo de recursos disponíveis podem ser destacadas em um mapa. As informações são fáceis de acessar quando e onde você precisar delas.

Monitoramento de Status

O IBM Intelligent Operations Center fornece uma ferramenta para a criação e exibição de 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.

Produzindo Relatórios

O IBM Intelligent Operations Center tem um recurso de relatório integrado para que você possa configurar e executar relatórios com os eventos e KPIs fornecidos pela solução. É possível usar esse recurso para coletar e apresentar as informações mais úteis para você em uma base regular e atualizada. Esse recurso oferece todas as vantagens de resumos e apresentação gráfica customizados.

Usuários e Benefícios

O IBM Intelligent Operations Center foi projetado para equipe envolvida com o controle operacional em organizações, departamentos do governo, autoridades locais ou municipais: 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">• Obtenha um resumo de eventos e incidentes de nível executivo por meio de mapas, painéis, alertas• Determinar as medidas do sucesso organizacional com Key Performance Indicators (KPIs)• Identifique e controle problemas por meio de relatórios• Direcione propriedade e a implementação de política baseado em dados fornecidos

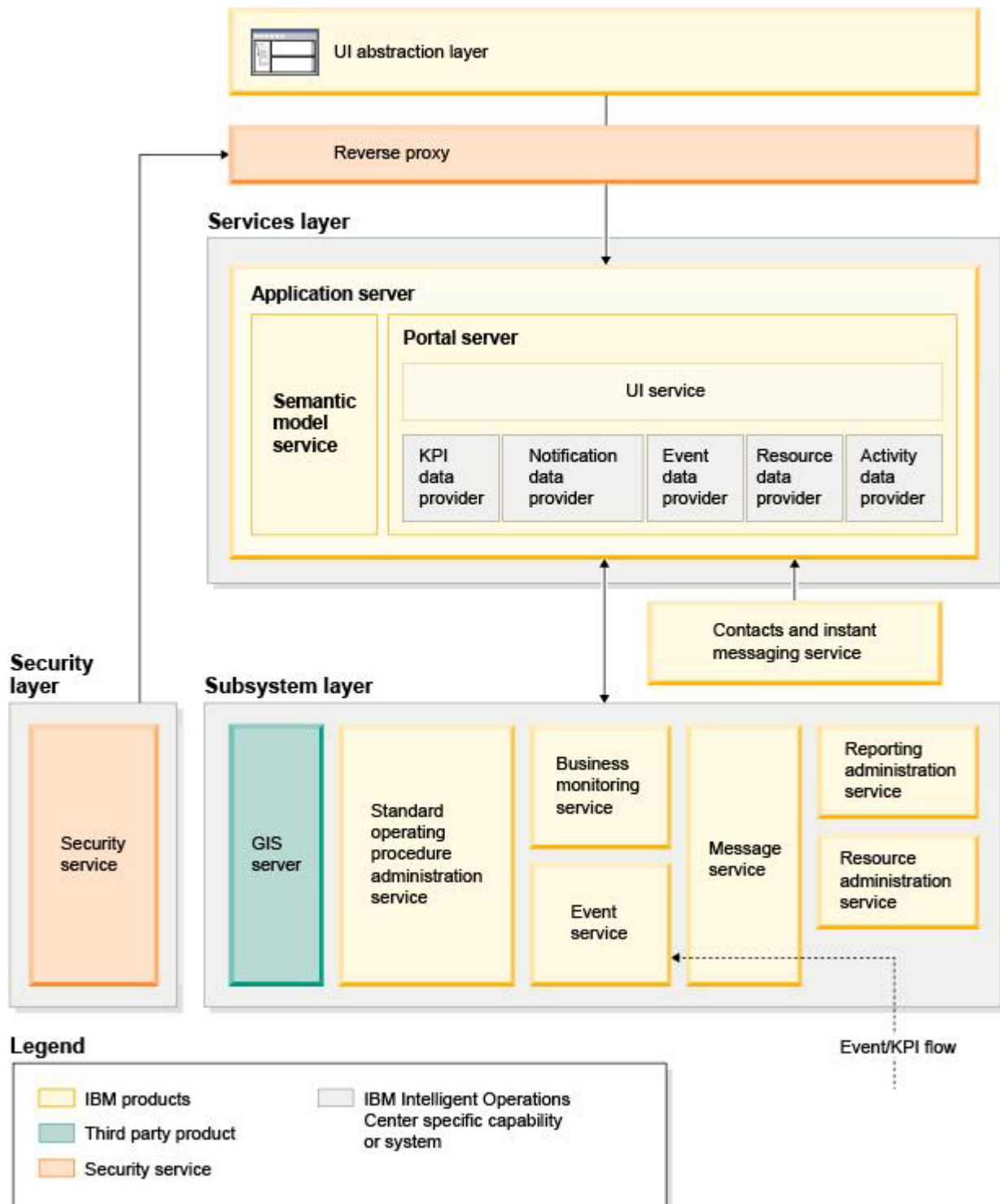
Tabela 1. Usuários e Benefícios do IBM Intelligent Operations Center (continuação)

Se você é um...	Este software pode ajudá-lo a...
Supervisor	<ul style="list-style-type: none"> • Identificar e executar ações em conflitos e problemas mostrados em mapas, painéis e alertas • Gerenciar ocorrências por meio da inclusão de novos eventos, edição de eventos existentes, cancelamento de eventos e escalção de eventos para incidentes • Forneça informações sobre recursos e os gerencie • Armazene e gerencie a execução de procedimentos e fluxos de trabalho associados com eventos • Monitore KPIs • Comunicar-se fácil e rapidamente a respeito de assuntos importantes • Projete relatórios úteis
Operador	<ul style="list-style-type: none"> • Crie, edite e monitore o status de eventos e incidentes a serem exibidos em listas • Receba e atualize status de atividades designadas • Verifique os recursos disponíveis • Execute relatórios regulares e atualizados • Notifique, atualize e emita alertas para colegas, gerentes ou executivos apropriados • Comunique-se rapidamente e facilmente em emergências e outras situações que requeiram uma resposta
Administrador de Usuários	<ul style="list-style-type: none"> • Inclua novos usuários e designe-os para grupos com a autenticação apropriada • Garanta a segurança de dados por meio de grupos de autorização baseados em função e categoria com permissões apropriadas • Configurar permissões adequadas à área de conhecimento e aos dados necessários
Administrador do sistema	<ul style="list-style-type: none"> • Customize páginas e portlets para que se ajustem à sua organização • Customize de acordo com os requisitos de gerenciamento os eventos e KPIs exibidos • Crie e publique eventos de teste • Configure relatórios e distribuição

Componentes

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

O diagrama a seguir mostra uma visualização de alto nível 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 variedade de dados que podem ser fornecidos de sistemas operacionais subjacentes, os dados são normalizados de acordo com um modelo de referência semântica padrão, que fornece um diretório comum para mapeamento de relacionamentos. Esse modelo facilita a análise do efeito e a resposta para os eventos sem a necessidade de diversas conversões de informações. O modelo de semântica fornece acesso às informações de KPI e 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 interação possibilita a comunicação bidirecional de mensagens em vários formatos, padrões abertos onde possível. Ao usar ferramentas padrão de mercado para transformar a partir das origens para o modelo semântico de referência, os sistemas operacionais subjacentes não precisam ser mudados. 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:

- 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 geographic information system (GIS), diagrama de mapa de localização ou plano para eventos de mapeamento, incidentes e recursos visualmente e espacialmente
- Criação e monitoramento de principais indicadores de desempenho (KPIs), que são atualizados como mudanças de dados por meio de conexões para sistemas de domínio subjacente
- Criação e monitoramento de procedimentos padrão de operação (SOPs) com fluxo de trabalho e atividades em associação com eventos
- Alertas entrando do campo, incluindo aqueles que requerem respostas emergenciais ou padrão
- Recursos de colaboração, por meio de um recurso de mensagem instantânea com o IBM Lotus Sametime
- Criação e distribuição ou relatórios regulares e atualizados baseados em dados de evento ou de KPI
- Um modelo de segurança baseado em função

Para obter informações adicionais sobre os serviços do sistemas IBM Intelligent Operations Center, consulte o link no final do tópico.

Conceitos relacionados:

“Serviços do Sistema do IBM Intelligent Operations Center” na página 11
Os servidores do IBM Intelligent Operations Center fornecem uma série de serviços.

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 dados do evento possibilita ao IBM Intelligent Operations Center assimilar dados de diversos sistemas para prever e reagir constantemente a eventos e tendências significantes.

Mensagens do evento são itens de dados autocontidos que contêm informações básicas, mas completas, às quais os destinatários podem responder. Mensagens do evento são colocadas em filas pelo IBM Intelligent Operations Center e processadas pelo serviço de manipulação de eventos.

Eventos vêm no IBM Intelligent Operations Center em diferentes formulários baseados na natureza das operações e domínios no hub de operações central. Alguns exemplos dos formulários de evento são: acionadores, limites, eventos complexos e eventos gerados 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 sejam resumidos e transferidos somente para o IBM Intelligent Operations Center caso precisem 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 exemplos 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.

O Que Há de Novo na Versão 1.5

O IBM Intelligent Operations Center 1.5 introduz novos recursos úteis para o administrador e o usuário.


O Que Há de Novo para o Usuário

Com o IBM Intelligent Operations Center 1.5, é possível gerenciar recursos e atividades associados com um evento.

Gerencie Recursos e Interaja com Mapas de Localização

Nos portlets novos Mapa de Localização e aprimorados Mapa, é possível:

- Avaliar os recursos disponíveis nas proximidades de um evento baseado em um mapa geográfico.
- Trabalhe com um novo tipo de mapa, um mapa de localização, com áreas interativas definidas. Por exemplo, um mapa de localização pode se basear em plano de rotas para um sistema de transporte.
- Visualize mais de um evento armazenado em cluster no mesmo local em um mapa.

 Para saber mais sobre o novo portlet Mapa de Localização e os portlets Mapa e Detalhes aprimorados, consulte os links no final do tópico.

Controle o Status das Atividades Associadas com Eventos

No novo portlet Minhas Atividades, é possível:

- Visualizar para o seu grupo as tarefas abertas associadas com um procedimento e um evento.
- Visualizar o status de tarefas designadas para você.
- Mudar o status de tarefas designadas para você.

 Para saber mais sobre o portlet Minhas Atividades, consulte o link no final do tópico.

Produza Relatórios

No novo portlet Relatórios, é possível:

- Visualizar até seis relatórios de eventos como gráficos.
- Criar relatórios customizados baseado em critérios e dados de seleção, incluindo relatórios para eventos por data ou intervalo de datas.
- Copiar uma URL de relatório e fazer com que o relatório seja exibido em um quadro à direita do portlet.

 Para saber mais sobre o portlet Relatórios, consulte o link no final do tópico.

Conceitos relacionados:

“Mapa de Localização” na página 276

Utilize o portlet do Mapa de Localização para ver os eventos marcados em um mapa de localização. Um mapa de localização no IBM Intelligent Operations Center é um mapa ou plano com áreas pré-definidas para interação, por exemplo, áreas de assentos em um grande estádio esportivo.

“Mapa” na página 279

Use o portlet Mapa para ver eventos e recursos em um mapa.

“Detalhes” na página 272

Use o portlet Detalhes para visualizar, monitorar e gerenciar eventos no IBM Intelligent Operations Center.

“Minhas Atividades” na página 284

O portlet Minhas Atividades exibe uma lista dinâmica de atividades pertencentes ao grupo do qual o usuário que está conectado à interface é membro.

“Relatórios” na página 288

Use o portlet Relatórios para visualizar um relatório de eventos como um gráfico. O portlet fornece opções para agrupar eventos e é possível escolher eventos por uma data ou intervalo de data específico. Estes relatórios ajudam a planejar respostas a eventos atuais e futuros.


O Que Há de Novo para o Administrador

Com a versão 1.5, é possível customizar seus portlets e layouts de página. Também é possível configurar procedimentos padrão de operação e fluxos de trabalho.

Customizar portlets

Com as novas opções de configuração de portlet, é possível configurar para cada portlet:


- Propriedades que são específicas a portlets individuais, por exemplo, configurar o ponto central e o nível de zoom para um mapa
- Propriedades que são genéricas nos portlets, por exemplo, configurar a altura do portlet

 Para saber mais sobre como customizar portlets, consulte o link no final do tópico.

Gerencie Eventos com Procedimentos Padrão de Operação e Fluxos de Trabalho

É possível definir procedimentos e atividades associados com eventos:

- Definir o procedimentos padrão de operação baseado em um plano de tarefas.
- Criar o fluxos de trabalho.
- Definir parâmetros para a seleção de um procedimento padrão de operação com base nos parâmetros de um evento.

 Para saber mais sobre como associar atividades associadas a eventos, consulte o link procedimento padrão de operação no final do tópico.


Script e Publicação de Eventos

É possível usar o novo portletScript do Evento para criar uma lista de eventos sequencial para ser publicada em intervalos de tempo pré-definidos.

 Para saber mais sobre como criar scripts e publicar eventos, consulte o link no final do tópico.

Verifique o Status de Serviço


É possível usar a nova ferramenta Verificação do Sistema para verificar o status operacional dos serviços do IBM Intelligent Operations Center.

 Para saber mais sobre a ferramenta Verificação do Sistema, consulte o link no final do tópico.

Suporte Protocolos

O IBM Intelligent Operations Center agora suporta eventos com protocolos diferentes do Protocolo de Alerta Comum. É possível:

- Estender tipos numerados para eventos Protocolo de Alerta Comum e non-Common Alerting Protocol.
- Customizar os menus pop-up no portlet Detalhes.
- Aceitar eventos de diversos domínios para exibição em portlets.

 Para saber mais sobre pontos de integração e protocolos, consulte o link no final do tópico.

Conceitos relacionados:

“Procedimentos Padrão de Operação” na página 127

É possível definir o procedimento padrão de operação e atividades para gerenciar eventos que chegam ao IBM Intelligent Operations Center. Use o portlet Procedimentos Padrão de Operação para acessar os aplicativos procedimento padrão de operação, matriz de seleção de procedimento padrão de operação e designer de fluxo de trabalho no Tivoli Service Request Manager.

“Script do Evento” na página 107

Use o portlet Script do Evento para gravar um script para criar uma lista sequencial de eventos a serem publicados em intervalos de tempo predefinidos.

“Verificando os Componentes” na página 210

A ferramenta Verificação do Sistema testa componentes dentro do IBM Intelligent Operations Center para determinar se eles estão acessíveis e operacionais.

“Pontos de integração e protocolos” na página 91

Outros sistemas podem ser integrados com a solução por meio dos serviços e políticas do IBM Intelligent Operations Center. Dados podem ser recebidos no formato Common Alerting Protocol (CAP); outros protocolos também são suportados.

Tarefas relacionadas:

“Customizando os portlets” na página 145

Como administrador, é possível alterar as configurações de portlet para customizar um portlet.

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, entenda a configuração do sistema do IBM Intelligent Operations Center e certifique-se de que os pré-requisitos são atendidos para o ambiente.

Serviços do Sistema do IBM Intelligent Operations Center

Os servidores do IBM Intelligent Operations Center fornecem uma série de serviços.

Serviços de Analítica

Fornecer análise de dados e serviços de apresentação.

Servidor de aplicativos

Fornecer serviços do Java Enterprise Edition que dão suporte ao produto.

Segurança

Fornecer serviços que determinam se um usuário está autorizado a utilizar o sistema e definir seus privilégios dentro do sistema.

Serviços de Autorização

Fornecer serviços que determinam os serviços a que um usuário está autorizado a usar.

Monitoramento de negócios

Fornecer agregação, análise e apresentação do processo de negócios e informações sobre atividade em tempo real.

Servidor de Mensagem Instantânea

Fornecer capacidades de colaboração em tempo real para usuários e aplicativos.

Serviços de Configuração

Gerencia a configuração do produto, incluindo inventário e gerenciamento de mudanças.

Banco de Dados

Fornecer o gerenciador do banco de dados para dados do aplicativo e do sistema.

Diretório

Fornecer o mapeamento entre nomes e valores. Os serviços de dados são utilizados como repositório para nomes de usuários e senhas.

Manipulação de eventos

Coleta, agrega, apresenta e manipula eventos do sistema.

Serviços do Sistema de Mensagens

Fornecer serviços de mensagens e de fluxo de trabalho para o produto.

Monitorando Serviços e Agentes

Fornecer atividade de monitoramento no produto.

Portal

Fornecer serviços que dão suporte à interação do usuário com o produto.

Modelo semântico

Fornecer serviços permitindo que os aplicativos modelem objetos e relacionamentos reais.

Conceitos relacionados:

“Componentes” na página 5

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

Requisitos de Hardware do IBM Intelligent Operations Center

Cinco servidores que atendem aos requisitos mínimos são necessários para instalar o IBM Intelligent Operations Center.

Os servidores devem ser x86 de 64 bits.

Os servidores de requisitos mínimos utilizados pelo IBM Intelligent Operations Center são mostrados em Tabela 2. O espaço mínimo em disco recomendado não inclui espaço para reinicialização e partições de troca.

Tabela 2. Requisitos de Hardware Mínimos

Recurso	Servidor de aplicativos	Servidor de eventos	servidor de dados	Servidor de Gerenciamento	Servidor de instalação
CPUs	4	4	4	4	2
Memória	24 GB	16 GB	16 GB	24 GB	4 GB
Adaptadores de rede	1	1	1	1	1
Espaço em Disco	113 GB	108 GB	108 GB	108 GB	108 GB
Espaço em disco adicional necessário durante a instalação	90 GB	90 GB	90 GB	90 GB	90 GB

Os requisitos mínimos para os diretórios em cada servidor, exceto o espaço necessário para a inicialização e para as partições de troca, são mostrados no Tabela 3.

Tabela 3. Requisitos Mínimos de Espaço para Cada Diretório

Diretório	Espaço Mínimo	Observações
/	8 GB	
/opt	35 GB ou 40 GB	São necessários 40 GB para o servidor de aplicativos, e 35 GB para todos os outros servidores
/usr	8 GB	
/home	5 GB	
/tmp	10 GB	
/chroot	1 GB	
/datahome	25 GB	
/loghome	8 GB	
/installMedia	90 GB	Esse diretório pode ser excluído após a instalação.
/var	8 GB	

Tarefas relacionadas:

“Preparando os Servidores” na página 17

Antes de instalar o IBM Intelligent Operations Center, valide se os requisitos de configuração do servidor foram satisfeitos. A ferramenta de pré-verificação verificará se muitas desses requisitos foram implementados.

Informações relacionadas:



Requisitos do sistema

Requisitos de Software Obrigatório

Antes de instalar o IBM Intelligent Operations Center, os servidores devem ter o software apropriado instalado.

O IBM Intelligent Operations Center requer que o Red Hat Enterprise Linux (RHEL) 5 Server x86-64 Atualização 5 ou mais recente seja instalado em todos os servidores. O Red Hat Enterprise Linux Versão 6 não é suportado.

Tarefas relacionadas:

“Preparando os Servidores” na página 17

Antes de instalar o IBM Intelligent Operations Center, valide se os requisitos de configuração do servidor foram satisfeitos. A ferramenta de pré-verificação verificará se muitas desses requisitos foram implementados.

Informações relacionadas:



Requisitos do sistema

Navegadores Suportados

A interfaces de soluções do IBM Intelligent Operations Center suporta uma série de navegadores. Alguns navegadores podem ser utilizados com limitações.

O IBM Intelligent Operations Center foi testado e é suportado nos seguintes navegadores:

- Microsoft Internet Explorer 8.x (apenas 32 bits)
- Microsoft Internet Explorer 9.x (apenas 32 bits)
- Mozilla Firefox 10 ESR

Visualização de Compatibilidade do Internet Explorer

O IBM Intelligent Operations Center não dá suporte à Visualização de Compatibilidade 8 do Internet Explorer ou Internet Explorer 9.

Nota: A Visualização de Compatibilidade pode ser ativada temporariamente, se você encontrar um problema ao criar uma nova página para a interface com o usuário, consulte o link no final do tópico para obter detalhes.

Desempenho do Internet Explorer 8.x

Os usuários podem observar um desempenho lento utilizando o Internet Explorer 8.x.

Para evitar este problema, utilize o Internet Explorer 9.x ou o Firefox 10 ESR.

Resolução Mínima da Tela

O IBM Intelligent Operations Center foi projetado para execução em uma resolução de tela mínima de 1280 x 800.

Tarefas relacionadas:

“Não É Possível Criar Nova Página para Interface com o Usuário” na página 331
Resolva um problema que ocorre durante a criação de uma nova página se você estiver trabalhando com o Microsoft Internet Explorer 9.

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.

Informações relacionadas:



Passport Advantage



Faça o download dos arquivos de imagem do IBM Intelligent Operations Center Versão 1.5

Listas de Verificação de Instalação

As listas de verificação da instalação estão disponíveis para as duas opções diferentes de instalação para o IBM Intelligent Operations Center. Estas listas de verificação fornecem uma visão geral das etapas de instalação e podem ser usadas para rastrear o processo de instalação.

Lista de Verificação - Instalação Usando o IBM Installation Manager

Utilize esta lista de verificação para controlar as etapas de instalação, ao instalar o IBM Intelligent Operations Center utilizando o IBM Installation Manager.

Sobre Esta Tarefa

Uma versão para impressão dessa lista de verificação está disponível usando o link relacionado no final desse tópico.

Procedimento

- ___ 1. Certifique-se de ter o hardware necessário.
- ___ 2. Certifique-se de que o software necessário esteja instalado no hardware.
- ___ 3. Prepare os servidores.
- ___ 4. Copie o pacote de instalação no servidor de instalação.
- ___ 5. Instale o Java Runtime Environment.
- ___ 6. Instale o IBM Installation Manager.
- ___ 7. Reinicie o IBM Installation Manager e instale o pacote **Configurar Topologia**.
- ___ 8. Reinicie o IBM Installation Manager e instale o pacote **Preparar Servidores de Destino**. Se esta etapa for concluída com sucesso, ignore a etapa do 9.
- ___ 9. Reinicie o IBM Installation Manager e instale o pacote **Ignorar Erros de Verificação do Sistema**. Ao executar o IBM Installation Manager após a resolução dos erros de verificação do sistema ou após determinar a continuidade da instalação, selecione **Preparar Servidores de Destino** e **Ignorar Erros de Verificação do Sistema** na segunda execução.
- ___ 10. Reinicie IBM Installation Manager e instale o pacote **Preparar Ambiente**.
- ___ 11. Reinicie IBM Installation Manager e instale o pacote **Instalar e Configurar Plataforma - Parte 1**.

Dica: Não selecione Parte 1 e Parte 2 ao mesmo tempo. Estas etapas levarão o maior tempo para ser executado. Se ambos forem executados juntos e houver uma falha, ambos precisarão ser executados novamente, mesmo que um tenha sido bem sucedido.

- Importante:** Não encerre os servidores entre as fases de instalação. O encerramento dos servidores entre fases não foi testado e pode gerar em resultados imprevisíveis.
- ___ 12. Reinicie IBM Installation Manager e instale o pacote **Instalar e Configurar Plataforma- Parte 2**.
 - ___ 13. Reinicie IBM Installation Manager e instale o pacote **Instalar Ferramenta de Controle da Plataforma**.
 - ___ 14. Reinicie IBM Installation Manager e instale o pacote **Instalar Ferramenta de Verificação do Sistema**.
 - ___ 15. Reinicie todos os servidores IBM Intelligent Operations Center.
 - a. Encerre todos os servidores IBM Intelligent Operations Center usando o Ferramenta de Controle de Plataforma.
 - b. Encerre e reinicie todos os servidores a partir do sistema operacional.
 - c. Inicie todos os servidores IBM Intelligent Operations Center usando o Ferramenta de Controle de Plataforma.
 - ___ 16. Reinicie IBM Installation Manager e instale o pacote **Instalar Aplicativo**. Isso instalará o aplicativo IBM Intelligent Operations Center.
 - ___ 17. Configure a arquitetura do IBM Intelligent Operations Center.
 - ___ a. Configure os serviços de colaboração se estiver usando o IPv6.
 - ___ b. Configure a conexão única para serviços de colaboração.
 - ___ c. Instale e configure o serviços de modelo semântico.
 - ___ d. Configure o Ferramenta de Controle de Plataforma.
 - ___ e. Criptografe a Tivoli Service Request Manager senha administrativa.
 - ___ f. Configure o número mínimo de encadeamentos para o EventProcessor.
 - ___ g. Mude o tamanho do conjunto de encadeamentos Padrão e Contêiner da Web.
 - ___ 18. Instale todos os outros aplicativos.
 - ___ 19. Reinicie IBM Installation Manager, instale e execute o pacote **Cyber Hygiene**. O Cyber Hygiene fornece segurança adicional para sistema IBM Intelligent Operations Center.
- Nota:** O Cyber Hygiene é instalado e executado na mesma etapa.
- ___ 20. Configure usuários que requerem acesso e senhas ssh.

Resultados

A arquitetura do IBM Intelligent Operations Center e o aplicativo do IBM Intelligent Operations Center estão instalados e prontos para uso.

O que Fazer Depois

Um ferramenta para reunir informações é fornecida para coletar logs de instalação para ajudar a diagnosticar problemas de instalação.

Conceitos relacionados:

“Visão Geral do Cyber Hygiene” na página 80

O recurso Cyber Hygiene do IBM Intelligent Operations Center é designado para fornecer serviços que corrigem exposições de segurança potenciais no sistema instalado.

Informações relacionadas:



Versão para impressão dessa lista de verificação

Lista de Verificação - Instalação Passo-a-Passo

Utilize esta lista de verificação para controlar as etapas de instalação ao instalar o IBM Intelligent Operations Center, utilizando scripts e comandos.

Sobre Esta Tarefa

Uma versão para impressão dessa lista de verificação está disponível usando o link relacionado no final desse tópico.

Procedimento

- ___ 1. Certifique-se de ter o hardware necessário.
- ___ 2. Certifique-se de que o software requerido esteja instalado no hardware.
- ___ 3. Prepare os servidores.
- ___ 4. Instale o Java Runtime Environment.
- ___ 5. Copie o pacote de instalação no servidor.
- ___ 6. Descompacte e prepare o pacote de instalação.
- ___ 7. Defina as propriedades de instalação.
- ___ 8. Defina a topologia para a instalação editando o arquivo de propriedades de topologia.
- ___ 9. Gere a senha de topologia que será usada para criptografar os arquivos-chave.
- ___ 10. Gere o arquivo de topologia.
- ___ 11. Execute a ferramenta de Pré-Verificação para verificar se o ambiente está pronto para instalar o IBM Intelligent Operations Center.
- ___ 12. Defina as configurações de segurança Linux utilizando a ferramenta fornecida ou executando uma série de comandos.
- ___ 13. Instale a arquitetura do IBM Intelligent Operations Center. Isso pode ser feito em uma ou em três fases. Se for executada em um ambiente virtualizado, a instalação de várias fases permitirá criar uma captura instantânea entre as fases da instalação.
 - Instalar o IBM Intelligent Operations Center em uma fase. A instalação levará até 14 horas.
 - Instalar o IBM Intelligent Operations Center em três fases. As três fases são:
 - a. Copiar os arquivos de instalação do servidor de instalação para os servidores de destino. Esta fase leva aproximadamente 2 horas.
 - b. Instalar a primeira fase da topologia. Esta fase leva aproximadamente 9 horas.
 - c. Instalar a segunda fase da topologia. Esta fase leva aproximadamente 3 horas.

Importante: Não encerre os servidores entre as fases de instalação. O encerramento dos servidores entre fases não foi testado e pode gerar em resultados imprevisíveis.

- ___ 14. Instale o Ferramenta de Controle de Plataforma.
- ___ 15. Instale a ferramenta do Verificação do Sistema.
- ___ 16. Verifique se a arquitetura do IBM Intelligent Operations Center está corretamente instalada.
- ___ 17. Configure a arquitetura do IBM Intelligent Operations Center.
 - ___ a. Configure os serviços de colaboração se estiver usando o IPv6.
 - ___ b. Configure a conexão única para serviços de colaboração.
 - ___ c. Instale e configure o serviços de modelo semântico.
 - ___ d. Criptografe a senha do administrador do Tivoli Service Request Manager.
 - ___ e. Configure o número mínimo de encadeamentos para o EventProcessor.
 - ___ f. Mude o tamanho do conjunto de encadeamentos Padrão e Contêiner da Web.
- ___ 18. Instale o aplicativo do IBM Intelligent Operations Center.
- ___ 19. Instale todos os outros aplicativos.
- ___ 20. Instale e execute o Cyber Hygiene. O Cyber Hygiene fornece segurança adicional para o sistema IBM Intelligent Operations Center.

Nota: O Cyber Hygiene é instalado e executado na mesma etapa.

__ 21. Configurar usuários que requerem acesso e senhas ssh.

Resultados

A arquitetura do IBM Intelligent Operations Center e o aplicativo do IBM Intelligent Operations Center estão instalados e prontos para uso.

O que Fazer Depois

Um ferramenta para reunir informações é fornecida para coletar logs de instalação para ajudar a diagnosticar problemas de instalação.

Conceitos relacionados:

“Visão Geral do Cyber Hygiene” na página 80

O recurso Cyber Hygiene do IBM Intelligent Operations Center é designado para fornecer serviços que corrigem exposições de segurança potenciais no sistema instalado.

Informações relacionadas:



Versão para impressão dessa lista de verificação

Preparando os Servidores

Antes de instalar o IBM Intelligent Operations Center, valide se os requisitos de configuração do servidor foram satisfeitos. A ferramenta de pré-verificação verificará se muitas desses requisitos foram implementados.

Sobre Esta Tarefa

Se estiver executando em um ambiente virtual, usar um modelo para essas etapas pode ajudar a reduzir o tempo de configuração.

Procedimento

1. Certifique-se de que os servidores atendam aos requisitos de hardware e software.
2. Configurar a rede TCP/IP.
 - a. Defina um nome completo e um nome abreviado do host, utilizando um servidor DNS ou por definição no arquivo `/etc/hosts`.
 - b. Verificar a configuração TCP/IP. Os servidores serão configurados corretamente, se os testes a seguir forem concluídos com sucesso.
 - 1) O comando `hostname -s` retorna o nome abreviado do host definido para o servidor.
 - 2) O comando `hostname -f` retorna o nome completo de domínio e do host para o servidor.
 - 3) Os resultados de um comando `ping`, ou do comando `ping6` para ambientes IPV6, com o nome abreviado do host para cada servidor indica que o servidor está acessível.
 - 4) Os resultados de um comando `ping`, ou do comando `ping6` para ambientes IPV6, com o nome completo para cada servidor indica que o servidor está acessível.
 - c. Ative o endereçamento do loopback local para cada servidor no arquivo `/etc/hosts`.
 - d. Verificar o endereçamento do loopback local. Os servidores serão configurados corretamente, se os testes a seguir forem concluídos com sucesso.
 - 1) O comando `ping -n localhost` retorna o endereço 127.0.0.1.
 - 2) O comando `ping -n localhost.localdomain` retorna o endereço 127.0.0.1.
 - 3) O comando `ping6 -n localhost6` em um ambiente IPV6 retorna o endereço `::1`.
 - 4) O comando `ping6 -n localhost6.localdomain6` em um ambiente IPV6 retorna o endereço `::1`.

- e. Certifique-se de que as portas requeridas pelo IBM Intelligent Operations Center estejam disponíveis. As portas requeridas para cada servidor são mostradas no Tabela 4.

Tabela 4. Portas Necessárias para Utilização do Produto

Servidor	Portas Requeridas para Utilização do Produto
Aplicativo	80, 82, 389, 390, 443, 2814, 5060, 5061, 5062, 5063, 5064, 5065, 5066, 5067, 5068, 5069, 5070, 5071, 5072, 5073, 5558, 5559, 5560, 5561, 5562, 5563, 5564, 5578, 5579, 5580, 5581, 5582, 5583, 5584, 7234, 7276, 7278, 7279, 7280, 7281, 7283, 7284, 7286, 7287, 7288, 7289, 7290, 7291, 7292, 8008, 8880, 8882, 8883, 8885, 8887, 8889, 8890, 9044, 9045, 9046, 9047, 9048, 9049, 9050, 9060, 9061, 9062, 9063, 9064, 9065, 9066, 9067, 9080, 9081, 9082, 9083, 9084, 9085, 9086, 9101, 9102, 9103, 9104, 9105, 9106, 9107, 9354, 9356, 9357, 9359, 9361, 9363, 9364, 9404, 9405, 9406, 9407, 9408, 9409, 9410, 9411, 9412, 9413, 9414, 9415, 9416, 9417, 9418, 9419, 9420, 9421, 9422, 9423, 9424, 9443, 9444, 9445, 9446, 9447, 9448, 9449, 9633, 9634, 9635, 9636, 9638, 9640, 9641, 9810, 9811, 9812, 9813, 9814, 9815, 10000, 10001, 10002, 10003, 10004, 10005, 10006, 10007, 10008, 10009, 10010, 10011, 10012, 10013, 10014, 10015, 10016, 10017, 10025, 10026, 10027, 10028, 10029, 10030, 10031, 10032, 10033, 10034, 10035, 10036, 10037, 10038, 10039, 10040, 10041, 10042, 31000, 31001, 31002, 31003, 31004, 31005, 31006, 31007, 31008, 31009, 31010, 31011, 31012, 31013, 31014, 31015, 31016
Evento	80 82, 84, 389, 390, 1414, 8008, 9060, 9080, 20000, 31000, 31001, 31002, 31003, 31004, 31005, 31006, 31007, 31008, 31009, 31010, 31011, 31012, 31013, 31014, 31015, 31016
Data	389, 390, 50000, 50001, 50002, 50003, 50004, 50005, 50006, 50007, 50008
Gerenciamento	80, 82, 389, 390, 1098, 1099, 1527, 1918, 5060, 5061, 5062, 5063, 5064, 5065, 5066, 5067, 5068, 5069, 5070, 5071, 5072, 5073, 5558, 5559, 5560, 5561, 5562, 5563, 5564, 5578, 5579, 5580, 5581, 5582, 5583, 5584, 7135, 7136, 7137, 7276, 7278, 7279, 7280, 7282, 7284, 7286, 7287, 7288, 7289, 7290, 7291, 7292, 7293, 8008, 8880, 8882, 8884, 8886, 8888, 8890, 8892, 9043, 9044, 9045, 9046, 9047, 9048, 9049, 9050, 9061, 9062, 9063, 9064, 9065, 9066, 9067, 9080, 9081, 9082, 9083, 9084, 9085, 9086, 9101, 9102, 9103, 9104, 9105, 9106, 9107, 9354, 9356, 9358, 9360, 9362, 9364, 9366, 9404, 9405, 9406, 9407, 9408, 9409, 9410, 9411, 9412, 9413, 9414, 9415, 9416, 9417, 9418, 9419, 9420, 9421, 9422, 9423, 9424, 9443, 9444, 9445, 9446, 9447, 9448, 9448, 9449, 9633, 9634, 9635, 9637, 9639, 9641, 9643, 9810, 9811, 9812, 9813, 9814, 9815, 9816, 13100, 13101, 13104, 41001, 50001

- f. Certifique-se de que o máximo de descritores de arquivos abertos definidos pelo parâmetro **nofile** no arquivo `/etc/security/limits.conf` esteja configurado para 20480 para os seguintes servidores:

- Servidor de aplicativos
- Servidor de eventos
- servidor de dados
- Servidor de Gerenciamento

Isso é feito incluindo as seguintes linhas no arquivo `/etc/security/limits.conf`:

```
* soft nofile 20480
* hard nofile 20480
```

Isso irá configurar o limite flexível (padrão) do número de arquivos abertos para todos os usuários como 20480, e também configurará o limite máximo para todos os usuários como 20480. Talvez você queira aumentar o limite máximo se outros aplicativos precisarem de mais de 20480 arquivos.

- g. Inclua ou atualize o parâmetro **net.ipv4.tcp_fin_timeout** no arquivo `/etc/sysctl.conf` para 30 para os seguintes servidores:

- Servidor de aplicativos
- Servidor de eventos
- servidor de dados
- Servidor de Gerenciamento

3. Desativar todos os firewalls do Linux.

4. Desative o SELinux (Security Enforcing Linux) editando o arquivo `/etc/selinux/config` e alterando o SELINUX para desativado. Depois de alterar a configuração, reinicialize o servidor.

5. Assegure que todos os servidores tenham a mesma hora e data configurados conforme indicado pelo sistema operacional Linux. Pode ser utilizado um serviço de sincronização de horário.
6. Ative o serviço `sshd` em cada servidor executando o comando `/etc/init.d/sshd start`. O serviço precisa ser ativada para efetuar login raiz com autenticação de senha. A porta 22 do TCP/IP deve ser configurada no sistema operacional como uma porta de acesso ssh disponível para uso durante o processo de instalação. O número da porta TCP/IP para o acesso SSH do Ferramenta de Controle de Plataforma é especificado no arquivos de propriedades de topologia. Somente o Ferramenta de Controle de Plataforma utiliza a porta configurada.
7. Instale os pacotes Linux no Tabela 5 em cada servidor utilizando o comando `yum install package_name`. Esses pacotes estão disponíveis no Red Hat.

Tabela 5. Pacotes Obrigatórios e Opcionais Linux para os Servidores de Destino do IBM Intelligent Operations Center

Pacote	Servidor de aplicativos	servidor de dados	Servidor de eventos	Servidor de Gerenciamento
compat-libstdc++-33-3*	obrigatório	obrigatório	obrigatório	obrigatório
libXp-1.0.0-8*	obrigatório	opcional	obrigatório	obrigatório
libXmu-1*	obrigatório	opcional	obrigatório	obrigatório
libXtst-1*	obrigatório	opcional	obrigatório	obrigatório
pam-0*	obrigatório	opcional	opcional	opcional
rpm-build-4*	obrigatório	opcional	opcional	obrigatório
libaio-0*	obrigatório	obrigatório	opcional	obrigatório
libstdc++-4*	obrigatório	obrigatório	obrigatório	obrigatório
libXft-2*	obrigatório	opcional	opcional	obrigatório
compat-db-4*	obrigatório	opcional	opcional	obrigatório
elfutils-libs-0*	obrigatório	opcional	opcional	obrigatório
elfutils-0*	obrigatório	opcional	opcional	obrigatório
libgcc-4*	obrigatório	opcional	obrigatório	opcional
compat-glibc-2*	obrigatório	opcional	obrigatório	opcional
openmotif22-2*	obrigatório	opcional	obrigatório	opcional
audit-libs-1*	obrigatório	opcional	opcional	opcional
glibc-2*	obrigatório	opcional	opcional	opcional
glibc-common-2*	obrigatório	opcional	opcional	opcional
glibc-headers-2*	opcional	obrigatório	opcional	obrigatório
glibc-devel-2*	opcional	obrigatório	opcional	obrigatório
compat-gcc*	opcional	obrigatório	opcional	obrigatório
libXft-2*	opcional	opcional	obrigatório	opcional
libXpm-3*	opcional	opcional	obrigatório	opcional
xorg-x11-xauth*	opcional	opcional	obrigatório	opcional
ksh-*	opcional	opcional	opcional	obrigatório

Os comandos a seguir podem ser usados para instalar os pacotes obrigatórios em cada servidor. Se o pacote já estiver instalado, ele não será reinstalado.

Servidor de aplicativos

```
yum install compat-libstdc++-33-3* libXp-1.0.0-8* libXmu-1* libXtst-1* pam-0*
```

```
rpm-build-4* libaio-0* libstdc++-4* libXft-2* compat-db-4* elfutils-libs-0*
elfutils-0* libgcc-4* compat-glibc-2* openmotif22-2* audit-libs-1* glibc-2*
glibc-common-2*
```

servidor de dados

```
yum install compat-libstdc++-33-3* libaio-0* libstdc++-4* glibc-headers-2*
glibc-devel-2* compat-gcc*
```

Servidor de eventos

```
yum install compat-libstdc++-33-3* libXp-1.0.0-8* libXmu-1* libXtst-1* libstdc++-4*
libgcc-4* compat-glibc-2* openmotif22-2* libXft-2* libXpm-3* xorg-x11-xauth*
```

Servidor de Gerenciamento

```
yum install compat-libstdc++-33-3* libXp-1.0.0-8* libXmu-1* libXtst-1* rpm-build-4*
libaio-0* libstdc++-4* libXft-2* compat-db-4* elfutils-libs-0* elfutils-0*
glibc-headers-2* glibc-devel-2* compat-gcc* ksh-*
```

8. Certifique-se de que Java 1.6 não esteja instalado em nenhum dos servidores:

- Servidor de instalação
- Servidor de aplicativos
- Servidor de eventos
- servidor de dados
- Servidor de Gerenciamento

Conceitos relacionados:

“Requisitos de Software Obrigatório” na página 13

Antes de instalar o IBM Intelligent Operations Center, os servidores devem ter o software apropriado instalado.

“Requisitos de Hardware do IBM Intelligent Operations Center” na página 12

Cinco servidores que atendem aos requisitos mínimos são necessários para instalar o IBM Intelligent Operations Center.

Tarefas relacionadas:

“Instalando o IBM Intelligent Operations Center Utilizando o Installation Manager” na página 25

O IBM Intelligent Operations Center pode ser instalado usando o instalador gráfico fornecido.

Informações relacionadas:

 <http://www.redhat.com/>

Rede TCP/IP

Antes de instalar o IBM Intelligent Operations Center, a rede TCP/IP entre os servidores deve ser configurada corretamente.

Todos os servidores, incluindo o servidor de instalação, usados pelo IBM Intelligent Operations Center devem ser configurados com um nome de host abreviado e um nome de host completo. Os nomes do host devem resolver em cada servidor para o endereço IP correto. A configuração pode ser feita utilizando um servidor DNS ou incluindo definições no arquivo `/etc/hosts`.

O nome completo do host para cada servidor deve ter pelo menos três componentes. Por exemplo: `myhost.mydomain.com`, onde o domínio de nível superior é um domínio de nível superior de Internet padrão.

Importante: Nomes abreviados do host e nomes completos do host devem ser especificados com letras maiúsculas ou minúsculas corretas. Por exemplo, `MyCompany.MyDomain.com` não pode ser especificado como `mycompany.mydomain.com`.

A rede do IPv6 é suportada pelo IBM Intelligent Operations Center, mas o IPv4 também deve ser instalado e configurado. Os endereços IPv4 não precisam ser designados para os servidores, mas o endereço de loopback IPv4 (127.0.0.1) deve ser ativado e o nome do host local deve resolver para 127.0.0.1.

As mudanças na configuração são mostradas no Tabela 6. Essas são as diretrizes para a configuração da rede TCP/IP no IBM Intelligent Operations Center servidor de instalação e nos servidores de destino, ao editar os arquivos de configuração de rede do Linux. As notas de configuração do Tabela 6 são apenas diretrizes. Qualquer configuração de rede em conformidade com os requisitos descritos anteriormente deverá funcionar.

Tabela 6. Diretrizes de Configuração do TCP/IP

Seqüência de	Observações
/etc/hosts	<p>O arquivo hosts resolve nomes de TCP/IP para endereços IP. Se a configuração não tiver um servidor DNS, todos os servidores e seus endereços IP, o nomes abreviados e os nomes completos do host deverão ser definidos neste arquivo. Os endereços de loopback local e os nomes do host também serão definidos neste arquivo.</p> <p>Se um servidor DNS estiver sendo usado, os hosts resolvidos pelo DNS não precisarão ser incluídos neste arquivo.</p> <p>Importante: Ao utilizar o IPv4, o endereço de loopback local 127.0.0.1 deve ser mapeado para os nomes do host local e localhost.localdomain.</p> <p>A seguir, um arquivo de amostra /etc/hoststutilizando endereços IPv4.</p> <pre># local loopback definitions -- do not remove # or alter these! 127.0.0.1 localhost.localdomain localhost # use the following if IPv6 is enabled in your # network definitions ::1 localhost6.localdomain localhost6 # installation server 192.168.0.205 IOC15Install.IOC15.com IOC15Install # target runtime servers 192.168.0.211 IOC15App.IOC15.com IOC15App 192.168.0.212 IOC15Event.IOC15.com IOC15Event 192.168.0.213 IOC15DB.IOC15.com IOC15DB 192.168.0.214 IOC15Mgmt.IOC15.com IOC15Mgmt</pre> <p>Utilize a nota de endereço IPv6 para designar endereços estáticos IPv6.</p> <p>Ambos os endereços, IPv6 e IPv4, podem ser definidos no mesmo servidor.</p>

Tabela 6. Diretrizes de Configuração do TCP/IP (continuação)

Seqüência de	Observações
/etc/sysconfig/network-scripts/ifcfg- <i>adapter_name</i>	<p>O arquivo <i>ifcfg-adapter_name</i> define as configurações de rede básicas para o adaptador de rede especificado. O nome designado do Linux para o adaptador de rede é especificado por <i>adapter_name</i>. O valor típico para o <i>adapter_name</i> é <i>eth0</i>, mas pode ser diferente para o ambiente.</p> <p>Para a rede IPv4 os seguintes parâmetros devem ser definidos.</p> <p>IPADDR Especifique o endereço IP do IPv4 do servidor que está sendo configurado.</p> <p>NETMASK Especifique a máscara de rede IPv4 do servidor que está sendo configurado.</p> <p>GATEWAY Especifique o endereço IP de rede padrão IPv4 do servidor que está sendo configurado.</p> <p>BOOTPROTO Se o endereçamento IP estático estiver sendo usado, especifique nenhum.</p> <p>NM_CONTROLLED Especifique não para desativar o serviço de Gerenciamento de Redes a partir da modificação do arquivo <i>ifcfg-adapter_name</i>.</p> <p>ONBOOT Especifique sim para iniciar automaticamente o adaptador.</p> <p>IPV6INIT Especifique sim se o adaptador utilizar a rede IPv6.</p> <p>IPV6ADDR Especifique o endereço IP IPv6 do servidor se o IPV6INIT=yes for especificado.</p> <p>IPV6_DEFAULTGW Especifique o endereço IP do gateway da rede padrão do IPv6 se o IPV6INIT=yes for especificado.</p>
/etc/sysconfig/network	<p>O arquivo <i>rede</i> especifica parâmetros gerais de rede.</p> <p>Para a rede IPv4 os seguintes parâmetros devem ser definidos:</p> <p>NETWORKING Especifique sim para ativar a rede IPv4.</p> <p>NETWORKING_IPV6 Especifique sim se a rede IPv6 também for desejada.</p> <p>HOSTNAME Especifique o nome abreviado do host do servidor.</p>

Tabela 6. Diretrizes de Configuração do TCP/IP (continuação)

Seqüência de	Observações
/etc/resolv.conf	<p>O arquivo <code>resolv.conf</code> é usado para definir servidores DNS para a rede e um domínio de procura padrão. Se os servidores DNS não estiverem sendo usados, este arquivo deverá estar vazio.</p> <p>Se um servidor DNS for usado, o <code>resolv.conf</code> deverá conter as seguintes linhas:</p> <pre>search domain_name nameserver first_DNS_server nameserver second_DNS_server</pre> <p>Por exemplo:</p> <pre>search yourcompany.com nameserver 10.75.20.10 nameserver 10.75.20.11</pre> <p>O valor procura especifica o domínio de procura padrão. O primeiro valor do <code>nameserver</code> é o endereço IP do servidor DNS. Um segundo valor do <code>nameserver</code> pode ser usado para especificar um servidor DNS secundário. A segunda especificação do <code>nameserver</code> é opcional.</p>
/etc/modprobe.conf	<p>O arquivo <code>modprobe.conf</code> define as opções de configuração para módulos carregados no sistema.</p> <p>A rede do IPv6 pode requerer que as seguintes linhas sejam comentadas e o servidor reinicializado:</p> <pre>alias ipv6 off options ipv6 disable=1</pre>

Quando configurado corretamente, cada servidor deve transferir com sucesso os seguintes testes:

1. O comando **hostname -s** retorna o nome abreviado do host definido para o servidor.
2. O comando **hostname -f** retorna o nome completo de domínio e do host para o servidor.
3. Os resultados de um comando **ping**, ou do comando **ping6** para ambientes IPV6, com o nome abreviado do host para cada servidor indica que o servidor está acessível.
4. Os resultados de um comando **ping**, ou do comando **ping6** para ambientes IPV6, com o nome completo para cada servidor indica que o servidor está acessível.

Tarefas relacionadas:

“Preparando os Servidores” na página 17

Antes de instalar o IBM Intelligent Operations Center, valide se os requisitos de configuração do servidor foram satisfeitos. A ferramenta de pré-verificação verificará se muitas desses requisitos foram implementados.

“A Rede IPv6 Não é Iniciada” na página 330

Se a rede IPv6 não é iniciada em um servidor, talvez o arquivo `/etc/modprobe.conf` precise de mudanças.

“Executando a Ferramenta de Pré-Verificação” na página 41

Antes de fazer o upload dos pacotes de instalação para os servidores de destino, verifique se os servidores de destino estão prontos para a instalação, executando a ferramenta de Pré-Verificação.

Copiando o Pacote de Instalação para o servidor de instalação

Copie o pacote de instalação do IBM Intelligent Operations Center para o servidor de instalação, antes de instalar o produto.

Antes de Iniciar

Antes de copiar o pacote de instalação para o servidor de instalação, certifique-se de que todos os servidores tenham sido preparados corretamente.

Procedimento

1. Crie um diretório no servidor de instalação para os arquivos de instalação, por exemplo, `/installHome`.
2. Tome nota do caminho completo para o diretório criado. Por exemplo, se o diretório criado for `installHome` para o usuário `ibmadmin`, o caminho completo será `/home/ibmadmin/installHome`. O caminho do diretório será conhecido como `install_home` em outras instruções de instalação.
3. Para cada DVD físico, ou a imagem ISO transferida por download do Passport Advantage, faça o seguinte.
 - a. Crie um diretório para montar o DVD. Por exemplo, execute o comando `mkdir /mnt/ba15`.
 - b. Monte o DVD. Por exemplo, ao usar uma imagem ISO, execute o comando `mount -o loop ISO_directory/ISO_filename /mnt/ba15` em que o `ISO_directory` é a localização da imagem ISO e `ISO_filename` é o arquivo ISO.
 - c. Copie os conteúdos do DVD para o diretório criado na etapa 1. Por exemplo, ao usar uma imagem ISO, execute o comando `cp /mnt/ba15/* install_home`.
 - d. Desmonte o DVD. Por exemplo, ao usar uma imagem ISO, execute o comando `umount /mnt/ba15`.
4. Altere o diretório `install_home`.
5. Execute o comando `ba15_media_prep.sh combine`. Este comando deve ser executado antes de executar quaisquer outras etapas de instalação.

Nota: Se seu diretório `install_home` for algo diferente de `/installMedia`, edite o arquivo `ba15_media_prep.sh` e altere o valor `MEDIA_BASE` para seu diretório `install_home` designado antes de executar o script.

Este comando combina arquivos que são divididos entre DVDs ou imagens ISO.

Conceitos relacionados:

“Local da Mídia de Instalação” na página 29

O IBM Installation Manager permite que o instalador especifique onde os pacotes de instalação estão localizados durante a instalação do IBM Intelligent Operations Center.

Tarefas relacionadas:

“Instalando o IBM Intelligent Operations Center Utilizando o Installation Manager” na página 25

O IBM Intelligent Operations Center pode ser instalado usando o instalador gráfico fornecido.

“Instalando O Java Runtime Environment”

O ambiente de tempo de execução do Java 6 deve ser instalado no servidor de instalação antes da instalação do IBM Intelligent Operations Center.

Instalando O Java Runtime Environment

O ambiente de tempo de execução do Java 6 deve ser instalado no servidor de instalação antes da instalação do IBM Intelligent Operations Center.

Sobre Esta Tarefa

No servidor de instalação, acesse o diretório no qual o pacote de instalação do IBM Intelligent Operations Center foi copiado. Nestas etapas, este diretório é referido como `install_home`.

Procedimento

1. Efetue logon como raiz ou alterne para a conta raiz, executando o comando `su -`.

2. Vá para o diretório onde os arquivos de instalação do IBM Intelligent Operations Center foram copiados.
3. Execute o comando `yum --nogpgcheck install install_media/ibm-java-x86_64-jre-6.0-10.1.x86_64.rpm`.
4. Execute o comando `export JAVA_HOME=/opt/ibm/java-x86_64-60/jre`.
5. Verifique o ambiente Java executando o comando `echo $JAVA_HOME` e confirmando se `/opt/ibm/java-x86_64-60/jre` foi retornado.

Tarefas relacionadas:

“Copiando o Pacote de Instalação para o servidor de instalação” na página 23

Copie o pacote de instalação do IBM Intelligent Operations Center para o servidor de instalação, antes de instalar o produto.

“Configurando o Ferramenta de Controle de Plataforma” na página 58

Depois de instalar o IBM Intelligent Operations Center, se foi instalado um Java™ JRE diferente daquele fornecido com o IBM Intelligent Operations Center, é preciso definir o local do JRE utilizado pelo Ferramenta de Controle de Plataforma.

“Instalando o IBM Intelligent Operations Center Utilizando o Installation Manager”

O IBM Intelligent Operations Center pode ser instalado usando o instalador gráfico fornecido.

Instalando o IBM Intelligent Operations Center Utilizando o Installation Manager

O IBM Intelligent Operations Center pode ser instalado usando o instalador gráfico fornecido.

Antes de Iniciar

O pacote do produto precisa ser copiado para o servidor de instalação no diretório *install-home* antes de seguir estas etapas.

Sobre Esta Tarefa

Um indicador de progresso é exibido durante a instalação. No entanto, como as tarefas de instalação são executadas remotamente nos servidores de destino, o indicador de progresso não indica o tempo restante real para a instalação. O “Componentes de Instalação” na página 28 fornece o tempo de instalação estimado para cada componente.

Se deseja cancelar a instalação a qualquer momento, clique em **Cancelar** na interface com o usuário do IBM Installation Manager.

Importante: Não execute o comando `launchpad.sh` após a instalação bem-sucedida do primeiro componente. Não será fornecida a opção de modificar sua instalação. Use o comando `/opt/IBM/InstallationManager/eclipse/IBMIM` para reiniciar o instalador em vez disso, como observado na etapa24 na página 27.

Procedimento

1. Execute o comando `export JAVA_HOME=/opt/ibm/java-x86_64-60/jre`.
2. Extraia o arquivo `BA_1.5_GUI_Installer_Lite_Launchpad.zip` em *install_home*.
3. Inicie a barra de ativação da instalação executando o comando `install_home/1launchpad.sh`.
4. Instale o IBM Installation Manager.
 - a. Clique em **Instalar IBM Installation Manager**.
 - b. Clique em **Avançar**.
 - c. Leia as informações sobre a licença.

- d. Se estiver de acordo com os termos de licença, selecione Aceito os termos no contrato de licença e clique em **Avançar**. A instalação prosseguirá.
- e. Caso não concorde com os termos da licença, selecione Não aceito os termos do contrato de licença e clique em **Avançar**. A instalação será finalizada.
- f. Selecione onde o IBM Installation Manager será instalado.
- g. Clique em **Avançar**.
- h. Clique em **Instalar**.
- i. Reinicie o IBM Installation Manager.

O IBM Installation Manager esteja instalado.

5. Depois que o IBM Installation Manager estiver instalado, o IBM Installation Manager precisará ser encerrado e reiniciado. Iniciar o IBM Installation Manager a partir da barra de ativação seleciona o arquivo de topologia para o IBM Intelligent Operations Center.
6. Clique em **Instalar IBM Intelligent Operations Center**.
7. Selecione o pacote do IBM Intelligent Operations Center - Versão 1.5.
8. Clique em **Avançar**.
9. Leia as informações sobre a licença.
 - a. Se estiver de acordo com os termos de licença, selecione Aceito os termos no contrato de licença e clique em **Avançar**. A instalação prosseguirá.
 - b. Caso não concorde com os termos da licença, selecione Não aceito os termos do contrato de licença e clique em **Avançar**. A instalação será finalizada.
10. Especifique o Diretório de Recurso Compartilhado para a instalação. Esse diretório será usado toda vez que o IBM Installation Manager for usado para instalar produtos utilizando o servidor de instalação. Certifique-se de especificar uma unidade com o maior espaço disponível no servidor.
11. Clique em **Avançar**.
12. Crie um novo grupo de pacotes selecionando Criar um novo grupo de pacotes. Selecione IBM Intelligent Operations Center.
13. Especifique o nome do Diretório de Instalação. O Diretório de Instalação será criado. O instalador criará subdiretórios neste diretório, conforme necessário.
14. Para Seleção de Arquitetura, selecione o 64 bits.
15. Clique em **Avançar**.
16. Desmarque todas as opções.
17. Selecione **Configurar topologia**.
18. Clique em **Avançar**.
19. Insira as opções de configuração. Anote todas as senhas definidas.
20. Clique em **Avançar**.
21. Revise as opções de instalação e clique em **Avançar** para iniciar a instalação.
22. Depois de concluir a instalação, feche o IBM Installation Manager e a barra de ativação. Não feche a janela do terminal em que a barra de ativação foi iniciada na etapa do 3 na página 25, uma vez que ela tem o ambiente JAVA_HOME configurado. Se a janela do terminal estiver encerrada, o JAVA_HOME deverá ser exportado novamente antes de continuar.
23. Se o valor inserido para a senha de topologia for maior do que 15 caracteres, execute o seguinte para definir uma senha para o ITM.ADMIN.USER.PWD, cujo comprimento seja 15 caracteres ou menos.
 - a. No servidor de instalação, edite o arquivo *install_home/ioc/topology/iop_lite_topo.properties*, onde *install_home* é o diretório para onde o pacote de instalação do IBM Intelligent Operations Center foi copiado.
 - b. Altere o valor definido do ITM.ADMIN.USER.PWD para um valor de 15 caracteres ou menos. Esta senha será usada ao efetuar login no usuário sysadmin, em vez de a senha de topologia.
 - c. Salve as mudanças.

24. Inicie o IBM Installation Manager executando o comando `/opt/IBM/InstallationManager/eclipse/IBMIM`.
25. Clique em **Modificar > Avançar**.
26. Selecione **Preparar Servidores de Destino**.
27. Clique em **Avançar > Modificar**.
28. Se houver erros, revise os arquivos de log no diretório `/var/ibm/InstallationManager/logs/native`. Os nomes dos arquivos de log começam com um registro de data e hora, que pode ser usado para correlacionar o log, quando a ferramenta de instalação foi executada.
29. Corrija todos os erros ou avisos localizados nos logs que pertençam ao seu sistema e conclua a instalação antes de instalar o próximo componente. Alguns avisos e erros podem ser ignorados. Por exemplo, avisos sobre IPv6 se você não tem o IPv6 ativado ou se a configuração não está conectada a um Serviço de Nome de Domínio (DNS).
30. Depois de corrigir todos os erros, retorne à etapa do 25. Você terá a opção de ignorar erros de verificação do sistema. Selecione o próximo componente da lista na etapa do 26. Continue o processo até que o Cyber Hygiene ter de ser instalado.

Importante: Não encerre os servidores entre as fases de instalação. O encerramento dos servidores entre fases não foi testado e pode gerar em resultados imprevisíveis.

O Cyber Hygiene aplica configurações de melhores práticas para fornecer segurança adicional para o sistema IBM Intelligent Operations Center. Antes de instalar o Cyber Hygiene, conclua a configuração de pós-instalação. Após a conclusão da configuração de pós-instalação, retorne à etapa 24 e instale e execute o Cyber Hygiene. Componentes instalados com sucesso, quando o IBM Installation Manager foi executado anteriormente, são verificados. Não desmarque esses componentes ou eles serão desinstalados quando o IBM Installation Manager for executado novamente.

Se estiver executando em um ambiente virtualizado, faça uma captura instantânea com memória de todos os servidores após a conclusão bem-sucedida de uma etapa de instalação e antes de instalar o próxima componente. Essa captura instantânea pode ser usada para reiniciar a instalação em um estado bem sucedido caso um ocorra um erro.

Para reduzir o tempo que o Cyber Hygiene leva para executar varreduras e correções, desmonte qualquer sistema de arquivos que não necessitam de avaliação para segurança. Por exemplo, os diretórios `install_media` em cada servidor podem ser excluídos após concluir todas as etapas de instalação. Esses diretórios podem ser excluídos ou desmontados antes da execução do Cyber Hygiene.

Nota: O Cyber Hygiene é instalado e executado na mesma etapa.

O Cyber Hygiene deve ser a última etapa antes de mover seu sistema para o status de produção ou quando o seu sistema deve tratar das boas práticas de segurança. Todos os aplicativos e soluções devem estar instalados e em execução antes da execução do Cyber Hygiene para que o sistema final possa ser varrido e as correções aplicadas.

Mudanças aplicadas ao sistema pelo Cyber Hygiene podem causar problema com outros aplicativos e soluções. Por exemplo, outros aplicativos e soluções podem ter requisitos no ambiente Linux que não estão de acordo com as boas práticas de segurança. Um aplicativo ou solução pode requerer que o logon do sistema seja efetuado como usuário raiz para que ele seja instalado ou executado. Nesses caso, algumas das mudanças do Cyber Hygiene podem precisar ser temporariamente ou permanentemente mudadas ou outra solução encontrada com o fornecedor do aplicativo ou solução.

Depois que as mudanças do Cyber Hygiene são feitas, não há nenhum método automatizado para alterá-las. Todas as mudanças devem ser feitas por atualizações manuais para o sistema operacional Linux ou alterando as permissões do arquivo ou do diretório.

Conceitos relacionados:

“Removendo os Serviços de Instalação do Sistema de Produção” na página 66

Depois de instalar o IBM Intelligent Operations Center, os serviços de instalação podem ser removidos dos servidores do sistema de produção. É sugerido que o servidor de instalação seja mantido, pois alguns de seus serviços podem ser necessários para atividades de manutenção.

“Configuração da Pós-Instalação do IBM Intelligent Operations Center” na página 51

Após a instalação da arquitetura do IBM Intelligent Operations Center utilizando o Installation Manager ou passo-a-passo, diversas etapas da configuração de pós-instalação precisam ser executadas para concluir a instalação.

“Visão Geral do Cyber Hygiene” na página 80

O recurso Cyber Hygiene do IBM Intelligent Operations Center é designado para fornecer serviços que corrigem exposições de segurança potenciais no sistema instalado.

Tarefas relacionadas:

“Preparando os Servidores” na página 17

Antes de instalar o IBM Intelligent Operations Center, valide se os requisitos de configuração do servidor foram satisfeitos. A ferramenta de pré-verificação verificará se muitas desses requisitos foram implementados.

“Verificando a instalação” na página 50

Depois de instalar o IBM Intelligent Operations Center, verifique se o produto foi instalado corretamente.

“Copiando o Pacote de Instalação para o servidor de instalação” na página 23

Copie o pacote de instalação do IBM Intelligent Operations Center para o servidor de instalação, antes de instalar o produto.

“Instalando O Java Runtime Environment” na página 24

O ambiente de tempo de execução do Java 6 deve ser instalado no servidor de instalação antes da instalação do IBM Intelligent Operations Center.

Componentes de Instalação

O IBM Intelligent Operations Center é instalado como sete componentes.

Tabela 7. Componentes de Instalação do IBM Intelligent Operations Center

Componente	Tempo de instalação estimado	O Que é Instalado
Preparar instalação	Pré-verificação: 10 minutos Upload: 2 horas	Verifica-se o ambiente do servidor atende os requisitos mínimos e os arquivos necessários para a instalação são copiados para os servidores de destino.
Preparar Ambiente	10 minutos	Atualiza o /etc/sudoers e os arquivos ~/.ssh/known_hosts conforme requerido para o IBM Intelligent Operations Center
Instalar e Configurar Plataforma	Fase 1: 12 horas Fase 2: 3 horas	A plataforma requerida é instalada nos servidores de destino. A instalação é executada em duas fases.
Ferramenta de Controle de Plataforma	10 minutos	Ferramentas necessárias para iniciar, parar e consultar o status dos servidores do IBM Intelligent Operations Center são instalados no Servidor de Gerenciamento.
Plataforma Verificação do Sistema	15 minutos	Ferramentas utilizadas para determinar se os recursos-chave da plataforma são instalados no servidor de aplicativos.
Aplicativo	3 horas	O aplicativo do IBM Intelligent Operations Center é instalado nos servidores de destino.

Tabela 7. Componentes de Instalação do IBM Intelligent Operations Center (continuação)

Componente	Tempo de instalação estimado	O Que é Instalado
Cyber Hygiene	até 1,5 horas	Recursos para mitigação e correção de conhecidas exposições de segurança virtuais são instalados nos servidores de destino. O tempo do processamento é determinado pela velocidade do hardware e se arquivos extras e desnecessários estão nos servidores de destino.

Opções de Configuração

O IBM Installation Manager permite que o instalador especifique as opções de configuração durante a instalação do IBM Intelligent Operations Center.

Senha de topologia

O IBM Installation Manager permite que o instalador especifique as senhas a serem usadas com o IBM Intelligent Operations Center.

O instalador pode especificar as senhas mostradas no Tabela 8.

Tabela 8. Senhas do IBM Intelligent Operations Center

Senha	Descrição
Senha de topologia	A senha de topologia é a senha usada para todas as contas criadas pelo instalador do IBM Intelligent Operations Center, exceto para aquelas senhas especificamente solicitadas durante o processo de instalação e a senha <code>iicsystemuser</code> que é definida como <code>passwd</code> e não pode ser mudada. A senha de topologia também protege a chave secreta criada pelo comando <code>createSecretKey</code> . A senha para uma conta não pode exceder 15 caracteres. Se o comprimento da senha de topologia for maior que 15 caracteres, etapas de configuração especiais precisam ser executadas para redefinir a senha para essa conta.
Senha do usuário administrativo	A senha do administrador definida para o usuário Linux <code>ibmadmin</code> . Este usuário é usado pelo Ferramenta de Controle de Plataforma ao gerenciar os componentes do servidor de destino.
Criptografia Inicial	O valor inicial de criptografia é usado para criptografar senhas de usuários e outros dados sensíveis dentro do banco de dados. O valor inicial de criptografia deve ser um valor de caractere ASCII para impressão de 12 a 1016. Deve ser usada uma sequência forte. Por exemplo uma sequência longa composta por letras maiúsculas e minúsculas, números e caracteres especiais sem palavras ou frases comuns.
Valor final de criptografia	O valor salt de criptografia é usado para criptografar senhas de usuários e outros dados sensíveis dentro do banco de dados. A criptografia salt deve ser um valor de caractere ASCII para impressão de 12, entre pontos de códigos 33 e 126.

Local da Mídia de Instalação

O IBM Installation Manager permite que o instalador especifique onde os pacotes de instalação estão localizados durante a instalação do IBM Intelligent Operations Center.

O instalador pode especificar os diretórios de instalação mostrados no Tabela 9 na página 30.

Tabela 9. Diretórios de Instalação do IBM Intelligent Operations Center

Diretório	Descrição	Valor Recomendado
Diretório base de imagem local	O nome do diretório no servidor de instalação que contém os arquivos de instalação do IBM Intelligent Operations Center. Esse é o diretório onde os arquivos de mídia de instalação foram copiados antes da execução da ferramenta de instalação. Esse diretório é chamado <i>install_media</i> em outras instruções de instalação.	/installMedia
Diretório temp de imagem local	O diretório no servidor de instalação usado para armazenar arquivos temporários durante a instalação.	/installMedia
Diretório de backup local	Esse diretório é apenas para uso interno.	/tmp/loc/backup
Diretório de imagem remota	O diretório nos servidores de destino no qual os pacotes a serem instalados nesse servidor serão copiados.	/installMedia/loc/image
Diretório de script remoto	O diretório nos servidores de destino no qual os scripts de instalação a serem executados nesse servidor serão copiados.	/installMedia/loc/script

Tarefas relacionadas:

“Copiando o Pacote de Instalação para o servidor de instalação” na página 23

Copie o pacote de instalação do IBM Intelligent Operations Center para o servidor de instalação, antes de instalar o produto.

local do servidor de dados

O IBM Installation Manager permite que o instalador defina a conexão para o servidor de dados durante a instalação do IBM Intelligent Operations Center.

O instalador pode especificar as opções de conexão do servidor de dados mostradas em Tabela 10.

Tabela 10. Informações sobre a Conexão do IBM Intelligent Operations Center servidor de dados

Opção	Descrição	Valor Recomendado
servidor de dados nome do host	O nome completo do host para o servidor.	Nenhum O valor é dependente da instalação.
servidor de dados usuário	A conta de usuário Linux a ser utilizada durante o processo de instalação.	root
servidor de dados password	A senha para a conta especificada no Usuário do Servidor de Dados .	Nenhum O valor é dependente da instalação.

Para testar a conexão com o servidor, clique em **Testar Conexão**.

local do Servidor de aplicativos

O IBM Installation Manager permite que o instalador defina a conexão para o servidor de aplicativos durante a instalação do IBM Intelligent Operations Center.

O instalador pode especificar as opções de conexão do servidor de aplicativos mostradas em Tabela 11 na página 31.

Tabela 11. Informações sobre a Conexão do IBM Intelligent Operations Center servidor de aplicativos

Opção	Descrição	Valor Recomendado
Servidor de aplicativos nome do host	O nome completo do host para o servidor.	Nenhum O valor é dependente da instalação.
Servidor de aplicativos usuário	A conta de usuário Linux a ser utilizada durante o processo de instalação.	root
Servidor de aplicativos password	A senha para a conta especificada no Usuário do Servidor de Aplicativos .	Nenhum O valor é dependente da instalação.

Para testar a conexão com o servidor, clique em **Testar Conexão**.

local do Servidor de eventos

O IBM Installation Manager permite que o instalador defina a conexão para o durante a instalação do IBM Intelligent Operations Center.

O instalador pode especificar as opções de conexão do mostradas em Tabela 12.

Tabela 12. Informações sobre a Conexão do IBM Intelligent Operations Center

Opção	Descrição	Valor Recomendado
Servidor de eventos nome do host	O nome completo do host para o servidor.	Nenhum O valor é dependente da instalação.
Servidor de eventos usuário	A conta de usuário Linux a ser utilizada durante o processo de instalação.	root
Servidor de eventos password	A senha para a conta especificada no Usuário do Servidor de Eventos .	Nenhum O valor é dependente da instalação.

Para testar a conexão com o servidor, clique em **Testar Conexão**.

local do Servidor de Gerenciamento

O IBM Installation Manager permite que o instalador defina a conexão para o Servidor de Gerenciamento durante a instalação do IBM Intelligent Operations Center.

O instalador pode especificar as opções de conexão do Servidor de Gerenciamento mostradas em Tabela 13.

Tabela 13. Informações sobre a Conexão do IBM Intelligent Operations Center Servidor de Gerenciamento

Opção	Descrição	Valor Recomendado
Servidor de Gerenciamento nome do host	O nome completo do host para o servidor.	Nenhum O valor é dependente da instalação.
Servidor de Gerenciamento usuário	A conta de usuário Linux a ser utilizada durante o processo de instalação.	root
Servidor de Gerenciamento password	A senha para a conta especificada no Usuário do Servidor de Gerenciamento .	Nenhum O valor é dependente da instalação.

Para testar a conexão com o servidor, clique em **Testar Conexão**.

Configuração do Cyber Hygiene

O IBM Installation Manager permite que o instalador especifique as opções necessárias para o Cyber Hygiene durante a instalação do IBM Intelligent Operations Center.

O instalador pode especificar as opções do Cyber Hygiene mostradas na Tabela 14.

Tabela 14. IBM Intelligent Operations Center Opções do Cyber Hygiene

Opção	Descrição	Valor Recomendado
Senha do GRUB	A senha do bootloader para o sistema. Esta senha será usada para todos os servidores de destino.	Uma senha especificada pelo cliente e consistente com a política de senha da organização do cliente.
Desativar login de raiz remota	Define se o acesso remoto é desativado para o usuário raiz em todos os servidores de destino.	Uma caixa de seleção é exibida com a opção marcada. A opção não pode ser excluída. O login de raiz remoto deve ser desativado. A opção é exibida para que o instalador compreenda que o login de raiz remoto está desativado. Esta configuração não desativa o logon como raiz do console ou alterando para o usuário raiz utilizando o comando su quando logado no servidor.

Reiniciando a Instalação Utilizando o Installation Manager

Se a instalação falhar, ela poderá ser reiniciada.

Sobre Esta Tarefa

Se a instalação falhar, a ferramenta de instalação irá recuperar as mudanças feitas durante a sessão. Se diversos componentes de instalações forem selecionados, todas as etapas selecionadas serão recuperadas, até mesmo as que foram concluídas com sucesso.

Para reiniciar uma instalação com falha, faça o seguinte.

Procedimento

1. Clique em **Aplicativos > IBM Installation Manager > IBM Installation Manager**.
2. Se nenhum componente for instalado com sucesso, selecione **novo** para reiniciar a instalação a partir do início.
3. Se um ou mais componentes foram instalados com sucesso, selecione **modificar** para reter mudanças de instalação existentes. Selecione os componentes, ou componentes a serem instalados.

Nota: É recomendado o uso do instalador para instalar os componentes, um por vez. Isso limitará a recuperação de componentes instalados com sucesso, caso falhem as instalações subsequentes do componente.

Passo-a-Passo da Instalação do IBM Intelligent Operations Center

O IBM Intelligent Operations Center pode ser instalado utilizando etapas e scripts do passo-a-passo da instalação.

Preparando o Pacote de Instalação

Antes de executar os scripts de instalação, o pacote de instalação precisa ser descompactado e preparado.

Sobre Esta Tarefa

No servidor de instalação, acesse o diretório no qual o pacote de instalação do IBM Intelligent Operations Center foi copiado. Nestas etapas, este diretório é referido como *install_home*.

Procedimento

1. Copie o pacote de instalação para o *install_home*.
2. Extraia o pacote de instalação.
3. Extraia BA_1.5_GUI_Installer_Lite_Launchpad.zip para o diretório *install_home*.
4. Vá para o diretório *install_home/repository/native*.
5. Extraia com.ibm.iop.ba.lite_1.5.0.9.zip para o diretório *install_home*.
6. Extraia com.ibm.iop.cat.lite_1.5.0.9.zip para o diretório *install_home*.
7. Extraia com.ibm.iop.isp.lite_1.5.0.zip para o diretório *install_home/isp/*.
8. Extraia com.ibm.iop.cyber.hygiene.install.lite_1.5.0.zip para o diretório *install_home/ch*.
9. Execute o comando **cp ../ files/com.ibm.iop.cyber.hygiene.scripts.lite_1.5.0.zip [install-home]/ch/install**.
10. Extraia com.ibm.iop.ioc.solution.lite_1.5.0.20120807.1518.zip para o diretório *install_home/ioc/spec*.
11. Extraia com.ibm.iop.ioc.topology.lite_1.5.0.20120807.1518.zip para o diretório *install_home/ioc/topology*.
12. Execute o comando **find install_home -name *.sh -exec chmod +x {} \;**
13. Execute o comando **find install_home -name *.sh -exec dos2unix {} \;**

Verificando os Scripts de Instalação

Um comando pode ser executado para exibir a documentação no instalador. Isso também mostra que o pacote de instalação está em operação.

Sobre Esta Tarefa

No servidor de instalação, acesse o diretório no qual o pacote de instalação do IBM Intelligent Operations Center foi copiado. Nestas etapas, este diretório é referido como *install_home*.

Procedimento

1. Efetue logon como raiz ou alterne para a conta raiz, executando o comando **su -**.
2. Execute o comando **export JAVA_HOME=/opt/ibm/java-x86_64-60/jre**.
3. Execute o comando *install_home/ioc/bin/ba.sh*. A documentação de instalação é exibida.

Customizando as Propriedades de Instalação

O arquivo de propriedades de instalação e os arquivos de propriedades de topologia fornecem definições requeridas pelos scripts de instalação.

Sobre Esta Tarefa

No servidor de instalação, acesse o diretório no qual o pacote de instalação do IBM Intelligent Operations Center foi copiado. Nestas etapas, este diretório é referido como *install_home*.

Procedimento

Opcional: Edite o arquivo *install_home/ioc/resource/custom.properties* e altere os valores da propriedade a seguir, se desejado. Todos os valores das propriedades no arquivo não listados na Tabela 15 na página 34 não devem ser alterados.

Tabela 15. Propriedades de Instalação do IBM Intelligent Operations Center

Propriedade	Descrição	Valor Padrão
image.basedir.local	O nome do diretório no servidor de instalação que contém os arquivos de instalação do IBM Intelligent Operations Center. Esse é o diretório onde os arquivos de mídia de instalação foram copiados antes da execução da ferramenta de instalação. Esse diretório é chamado <i>install_media</i> em outras instruções de instalação.	/installMedia
image.tempdir.local	O diretório no servidor de instalação usado para armazenar arquivos temporários durante a instalação.	/installMedia
backup.local	Esse diretório é apenas para uso interno.	/tmp/loc/backup
Unix.image.basedir.remote	O diretório nos servidores de destino no qual os pacotes a serem instalados nesse servidor serão copiados.	/installMedia/loc/image
Unix.script.basedir.remote	O diretório nos servidores de destino no qual os scripts de instalação a serem executados nesse servidor serão copiados.	/installMedia/loc/script
connection.timeout	Tempo (em milissegundos) para aguardar uma conexão com os servidores de destino antes de falhar	120000
waiting.time	Tempo (em milissegundos) de espera antes de tentar novamente uma conexão com malsucedida	120000
retry.count	Número de vezes para tentar uma conexão malsucedida antes de a instalação falhar	6

Se não alterados, serão utilizados os valores padrão.

Conceitos relacionados:

“Informações sobre Senha” na página 37

Senhas para vários IDs de usuário na solução IBM Intelligent Operations Center são definidas no arquivo de propriedades de topologia. Por motivos de segurança, as senhas padrão enviadas com o IBM Intelligent Operations Center deverão ser alteradas.

Instalação de Arquivos de Topologia

O IBM Intelligent Operations Center é instalado usando um arquivo de topologia. O arquivo de topologia é um arquivo XML que define os parâmetros e valores usados quando o IBM Intelligent Operations Center é implementado nos servidores e define a sequência usada para implementar componentes.

Editar o arquivo de topologia com um editor de texto pode introduzir erros. Por esse motivo, todas as propriedades customizáveis pelo cliente são definidas em um arquivo de propriedades de topologia. Um arquivo de modelo de topologia fornece a estrutura da topologia.

O comando **parameterizeTopology** obtém os pares nome/valor definidos no arquivo de propriedades de topologia e a estrutura fornecida pelo arquivo de modelo de topologia e cria um arquivo de topologia válido que é, então, usado durante a instalação.

O IBM Intelligent Operations Center fornece os seguintes arquivos de topologia:

Nome do Arquivo	Propósito
<i>install_home/ioc/resource/custom.properties</i>	Define o local da mídia de instalação, dos diretórios ativos e de outras propriedades. Esse arquivo pode ser editado para atender às necessidades do ambiente do cliente.
<i>install_home/ioc/topology/iop_lite_topo.properties</i>	Define as propriedades customizáveis do cliente para a implementação, incluindo nomes do host e senhas. Esse arquivo pode ser editado para atender às necessidades do ambiente do cliente.
<i>install_home/ioc/topology/iop_lite_topo.template.xml</i>	Define a estrutura da topologia a ser implementada. Esse arquivo utiliza os valores definidos no arquivo de propriedades. Esse arquivo não deve ser editado.
<i>install_home/ioc/topology/iop_lite_topo.xml</i>	Define a topologia a ser implementada. Esse arquivo é criado pelo comando parameterizeTopology utilizando as informações nas propriedades e no arquivo de modelo. Esse arquivo não deve ser editado, exceto quando necessário para se recuperar de uma falha na instalação.
<i>install_home/ioc/topology/iop_lite_topo.chk</i>	Define as regras utilizadas pela ferramenta de Pré-Verificação para determinar se os servidores são configurados corretamente para a instalação do IBM Intelligent Operations Center. Esse arquivo não deve ser editado.

Tarefas relacionadas:

“Instalando o Ferramenta de Controle de Plataforma” na página 47

O Ferramenta de Controle de Plataforma é usado para gerenciar o ambiente do servidor do IBM Intelligent Operations Center. A ferramenta é instalada separadamente do produto.

Arquivo de Propriedades de Topologia

O arquivo de propriedades de topologia define as propriedades customizáveis pelo cliente para a implementação do IBM Intelligent Operations Center. Esse arquivo deve ser editado para atender às necessidades do ambiente do cliente. Quaisquer propriedades no arquivo de propriedades de topologia anterior não documentadas aqui não devem ser alteradas.

Após modificar o arquivo de propriedades de topologia, salve uma cópia em um local seguro. O arquivo contém informações sensíveis à segurança, tais como nomes e senhas de usuário para o sistema em texto não criptografado. Se uma pessoa não autorizada tiver acesso a esse arquivo, terá acesso total ao sistema.

O arquivo de propriedades de topologia pode ser usado após a instalação das seguintes maneiras:

- Como repositório de informações de senha, caso uma senha seja esquecida.
- Como repositório para senhas, quando forem alteradas no sistema. O arquivo de propriedades de topologia modificado pode ser usado para atualizar as senhas usadas pelo Ferramenta de Controle de Plataforma.
- Como backup das informações de instalação, caso o sistema precise ser reinstalado. O arquivo de propriedades de topologia pode ser usado sem a necessidade de redefinir todos os parâmetros de instalação.

Tarefas relacionadas:

“Gerando o Arquivo de Topologia” na página 40

Antes de executar as etapas de instalação para o IBM Intelligent Operations Center, gere um arquivo de topologia com os parâmetros necessários para a instalação.

Informações sobre o Servidor de Destino:

A seção SERVERS do arquivo de propriedades de topologia define as propriedades para os servidores de destino.

O Tabela 16 mostra os valores da propriedade do servidor que podem ser especificados no arquivo de propriedades de topologia.

Tabela 16. Propriedades do Servidor de Destino

Propriedade	Descrição
DB.1.HOST	O nome do host do servidor de dados
DB.1.ACCOUNT.PWD	A senha raiz para o servidor de dados
DB.1.SSH_PORT	O número da porta para acesso a ssh para o servidor de dados
APP.1.HOST	O nome do host do servidor de aplicativos
APP.1.ACCOUNT.PWD	A senha raiz para o servidor de aplicativos
APP.1.SSH_PORT	O número da porta para acesso a ssh para o servidor de aplicativos
EVENT.1.HOST	O nome do host do
EVENT.1.ACCOUNT.PWD	A senha raiz para o
EVENT.1.SSH_PORT	O número da porta para acesso a ssh para o
MGMT.1.HOST	O nome do host do Servidor de Gerenciamento
MGMT.1.ACCOUNT.PWD	A senha raiz para o Servidor de Gerenciamento
MGMT.1.SSH_PORT	O número da porta para acesso a ssh para o Servidor de Gerenciamento

Importante: Os valores do nome do host devem ser de nomes completos do host inseridos no caso definido. Por exemplo, I0C15App.I0C15.com não é o mesmo que ioc15app.ioc15.com.

Um número da porta ssh pode ser configurado para cada servidor. No entanto, os números da porta configurados serão usados somente pelo Ferramenta de Controle de Plataforma. A porta 22 deve ser ativada para acesso a ssh em cada servidor. A porta 22 é necessária para acesso SSH pelo IBM Intelligent Operations Center durante a instalação.

Informações sobre Serviços de Diretório:

O arquivo de propriedades de topologia define valores usados para criptografar senhas de usuários e outros dados sensíveis dentro do diretório.

A criptografia é baseada em dois valores: LDAP.SEED e LDAP.SALT.

Os valores devem ser caracteres ASCII para impressão. Os caracteres ASCII para impressão são caracteres com valores de ponto de código de 33 a 126. Um espaço em branco não pode ser utilizado.

Tabela 17. Propriedades de Serviços de Diretório

Propriedade	Descrição
LDAP.SEED	Uma sequência de 12 a 1016 caracteres, consistindo em caracteres ASCII para impressão, entre pontos de código 33 até 126. Uma sequência com criptografia forte deve ser usada. Por exemplo uma sequência longa composta por letras maiúsculas e minúsculas, números e caracteres especiais sem palavras ou frases comuns.
LDAP.SALT	Uma sequência de 12 caracteres, consistindo em caracteres ASCII para impressão, entre pontos de código 33 até 126. Importante: LDAP.SALT deve ter exatamente 12 caracteres de comprimento. Um valor de mais ou menos caracteres causará falha da instalação.

Registre os valores LDAP.SEED e LDAP.SALT fora do sistema. Os valores serão necessários se precisar exportar ou replicar as entradas de diretório.

Informações sobre Senha:

Senhas para vários IDs de usuário na solução IBM Intelligent Operations Center são definidas no arquivo de propriedades de topologia. Por motivos de segurança, as senhas padrão enviadas com o IBM Intelligent Operations Center deverão ser alteradas.

As senhas podem conter somente caracteres alfanuméricos (a-z, A-Z, 0-9). A menos que indicado o contrário, as senhas devem ter 30 caracteres ou menos.

Tabela 18. Propriedades da Senha

Propriedade	Nome do usuário associado	Descrição
LDAP.DB.PWD	dsrdbm01	Banco de dados do diretório LDAP
LDAP.ADMIN.DN.PWD	cn=root	Conexão do administrador LDAP
LDAP.BIND.DN.PWD	cn=bind	Conexão LDAP
LDAP.PROXY.INSTANCE.PWD	tdsproxy	Instância do proxy LDAP
LDAP.PROXY.ADMIN.DN.PWD	cn=root	Conexão do administrador do proxy LDAP
LDAP.PROXY.BIND.DN.PWD	cn=bind	Conexão do proxy LDAP
TAM.SECMASTER.PWD	Nenhum	Senha principal do serviço de segurança São concedidos a este usuário privilégios equivalentes ao usuário raiz nos servidores de destino. Devido ao acesso cedido a esse usuário, certifique-se de que esse senha tenha um valor longo, seja diferente de outras senhas, e seja mantida segura.

Tabela 18. Propriedades da Senha (continuação)

Propriedade	Nome do usuário associado	Descrição
TAM.WEBSEAL.ADMIN.PWD	sec_master	Administrador do Serviço de Segurança São concedidos a este usuário privilégios equivalentes ao usuário raiz nos servidores de destino. Devido ao acesso cedido a esse usuário, certifique-se de que esse senha tenha um valor longo, seja diferente de outras senhas, e seja mantida segura.
WBM.DB.USER.PWD	db2ibm	Banco de dados do serviço de monitoramento de atividades de negócios
WODM.DB.USER.PWD	db2wodm	Banco de dados do serviço do Decision Management
WODM.ADMIN.UID.PWD	resAdmin1	Administrador do serviço do Decision Management
WODM.DEPLOYER.UID.PWD	resDeployer1	Implementador da regra do serviço do Decision Management
WODM.MONITOR.UID.PWD	resMonitor1	Monitor do serviço do Decision Management
WODM.DB.DC.USER.PWD	wodmdc	Banco de dados do console de decisão
WODM.rtsAdmin.UID.PWD	rtsAdmin	Administrador do console de decisão
WODM.rtsConfig.UID.PWD	rtsConfig	Configuração do console de decisão
WODM.rtsUser.UID.PWD	rtsUser	Usuário do console de decisão
UDDI.DB.USER.PWD	db2uddi	Banco de dados do serviço UDDI
IHS.KEYSTORE.PWD	Nenhum	Keystore do servidor HTTP
WAS.ADMIN.ACCOUNT.PWD	waswebadmin	Administrador de serviços de aplicativos
WAS.LTPA.PWD	Nenhum	LTPA token
PORTAL.ADMIN.ACCOUNT.PWD	waswebadmin	Administrador para o console do WebSphere Application Server, para o servidor do WebSphere Portal
PORTAL.ADMIN.UID.PWD	wpsadmin	Administrador para o servidor do WebSphere Portal
PORTAL.DB.USER.PWD	db2port1	Banco de dados WebSphere Portal
OMNIBUS.ADMIN.ACCOUNT.PWD	netcool	Administrador de serviços de eventos
IMPACT.WAS.ACCOUNT.PWD	wasadmin	Administrador dos serviços de eventos do sistema
TSRM.WAS.ADMIN.PWD	waswebadmin	Administrador do gerenciador de solicitação de serviços
TSRM.DB.USER.PWD	maximo	Banco de dados do gerenciador de solicitação de serviços
TSRM.ADMIN.USER.PWD	maxadmin	Administrador do gerenciador de solicitação de serviços

Tabela 18. Propriedades da Senha (continuação)

Propriedade	Nome do usuário associado	Descrição
TSRM.REG.USER.PWD	maxreg	Usuário do gerenciador de solicitação de serviços
TSRM.INITADM.USER.PWD	maxintadm	Usuário de integração do gerenciador de solicitação de serviços
MGMT.WAS.ADMIN.PWD	waswebadmin	Administrador dos serviços de aplicativos
TEPS.DB.USER.PWD	itmuser	Banco de dados do Enterprise Portal
TIM.STORE.PWD	Nenhum	Armazenamento do gerenciamento de identidade
TIM.ADMIN.USER.PWD	waswebadmin	Administrador do gerenciador de identidade
DOMINO.USER.PWD	notes	Usuário de colaboração
DOMINO.ORG.PWD	IBM	Organização de colaboração
DOMINO.ADMIN.PWD	administração de notas	Administrador de colaboração
DOMINO.ST.ADMIN.PWD	wpsadmin	Administrador do portal de colaboração
DOMINO.ST.BIND.PWD	wpsbind	Conexão LDAP de colaboração
DEFAULT.PWD.DAS	dausr1, dausr2, dausr3, dausr4, dausr5, dausr6, dausr7, dausr8	Servidor administrativo de serviços do banco de dados
DEFAULT.PWD.DB2	db2inst1, db2inst2, db2inst3, db2inst4, db2inst5, db2inst6, db2inst7, db2inst8	Servidor de dados de serviços do banco de dados
DEFAULT.PWD.IHS	ihsadmin	servidor HTTP
DEFAULT.PWD.MQM	mqm	Usuário dos serviços do sistema de mensagens
MQM.CONN.USER.PWD	mqmconn	Conexão com serviços de sistema de mensagens
DEFAULT.PWD.TAI	taiuser	Segurança de serviços de aplicativos
ITM.ADMIN.PWD	sysadmin	Administrador do gerenciamento do sistema Restrição: A senha deve ter 15 caracteres ou menos.
IOP.ADMIN.USER.PWD	ibmadmin	Ferramentas de administração do sistema São concedidos a este usuário privilégios equivalentes ao usuário raiz nos servidores de destino. O Ferramenta de Controle de Plataforma é executado sob este nome de usuário. Devido ao acesso cedido a esse usuário, certifique-se de que esse senha tenha um valor longo, seja diferente de outras senhas, e seja mantida segura.
IOP.USER.USER.PWD	ibmuser	Usuário geral do sistema

Conceitos relacionados:

Capítulo 3, “Protegendo a Solução”, na página 67

Segurança é importante dentro do IBM Intelligent Operations Center porque a solução é central para operações essenciais. Para garantir segurança, é importante que você conheça as configurações padrão e que gerencie usuários da solução para fornecer a todos eles o nível correto de acesso.

Tarefas relacionadas:

“Customizando as Propriedades de Instalação” na página 33

O arquivo de propriedades de instalação e os arquivos de propriedades de topologia fornecem definições requeridas pelos scripts de instalação.

Referências relacionadas:

“Usuários de Amostra” na página 69

Durante a implementação do IBM Intelligent Operations Center, são criados usuários de amostra.

Criando a senha de topologia

A senha de topologia é utilizada durante o processo de instalação para criptografar e acessar o arquivo que define a topologia da solução.

Sobre Esta Tarefa

No servidor de instalação, acesse o diretório no qual o pacote de instalação do IBM Intelligent Operations Center foi copiado. Nestas etapas, este diretório é referido como *install_home*.

Procedimento

1. Efetue logon como raiz ou alterne para a conta raiz, executando o comando **su -**.
2. Execute o comando **export JAVA_HOME=/opt/ibm/java-x86_64-60/jre**.
3. Altere para o diretório *install_home/ioc*.
4. Execute o comando **bin/ba.sh createSecretKey -p password** em que *password* é a senha a ser criada para a topologia. Este comando criará o arquivo *install_home/ioc/resource/ioc.keystore*. Esse arquivo contém a chave usada para criptografar as propriedades da topologia. O arquivo *ioc.keystore* também é criptografado com a senha especificada no comando **createSecretKey**. Para alterar a senha e a chave para a instalação, exclua o arquivo *install_home/ioc/resource/ioc.keystore*, e em seguida execute novamente o comando **createSecretKey**. Tome nota da senha para uso em outras etapas da instalação.

Tarefas relacionadas:

“Gerando o Arquivo de Topologia”

Antes de executar as etapas de instalação para o IBM Intelligent Operations Center, gere um arquivo de topologia com os parâmetros necessários para a instalação.

Gerando o Arquivo de Topologia

Antes de executar as etapas de instalação para o IBM Intelligent Operations Center, gere um arquivo de topologia com os parâmetros necessários para a instalação.

Sobre Esta Tarefa

No servidor de instalação, acesse o diretório no qual o pacote de instalação do IBM Intelligent Operations Center foi copiado. Nestas etapas, este diretório é referido como *install_home*.

Procedimento

1. Efetue logon como raiz ou alterne para a conta raiz, executando o comando **su -**.
2. Execute o comando **export JAVA_HOME=/opt/ibm/java-x86_64-60/jre**.
3. Vá para o diretório *install_home/ioc/topology*.
4. Edite o arquivo *iop_lite_topo.properties*, fazendo as mudanças necessárias para o ambiente.

5. Copie o arquivo de modelo de topologia no arquivo de topologia executando o comando **cp iop_lite_topo.template.xml iop_lite_topo.xml**.
6. Altere para o diretório *install_home/ioc*.
7. Execute o comando **bin/ba.sh parameterizeTopology -t iop_lite_topo -r topology/iop_lite_topo.properties -p password** em que *password* é a senha da topologia. Os parâmetros definidos no arquivo de propriedades da topologia são aplicados no arquivo de topologia.
8. Opcional: Para criptografar senhas no arquivo de topologia, execute o comando **bin/ba.sh encryptTopology -t iop_lite_topo -p password** em que *password* é a senha da topologia.

Importante: Somente as senhas no arquivo de topologia serão criptografadas. Senhas em outros arquivos, por exemplo, o arquivo de propriedades de topologia, não serão criptografadas.

Conceitos relacionados:

“Arquivo de Propriedades de Topologia” na página 35

O arquivo de propriedades de topologia define as propriedades customizáveis pelo cliente para a implementação do IBM Intelligent Operations Center. Esse arquivo deve ser editado para atender às necessidades do ambiente do cliente. Quaisquer propriedades no arquivo de propriedades de topologia anterior não documentadas aqui não devem ser alteradas.

Tarefas relacionadas:

“Criando a senha de topologia” na página 40

A senha de topologia é utilizada durante o processo de instalação para criptografar e acessar o arquivo que define a topologia da solução.

Executando a Ferramenta de Pré-Verificação

Antes de fazer o upload dos pacotes de instalação para os servidores de destino, verifique se os servidores de destino estão prontos para a instalação, executando a ferramenta de Pré-Verificação.

Sobre Esta Tarefa

No servidor de instalação, acesse o diretório no qual o pacote de instalação do IBM Intelligent Operations Center foi copiado. Nestas etapas, este diretório é referido como *install_home*.

Procedimento

1. Efetue logon como raiz ou alterne para a conta raiz, executando o comando **su -**.
2. Execute o comando **export JAVA_HOME=/opt/ibm/java-x86_64-60/jre**.
3. Altere para o diretório *install_home/ioc*.
4. Execute o comando **bin/ba.sh precheckTopology -t iop_lite_topo -p password**, onde *password* é a senha de topologia. As mensagens serão exibidas para cada teste de pré-verificação em cada servidor. O status de cada teste será [Pass] ou [Fail]. Após a execução de todos os testes, será exibido um resumo de todos os testes com falha.
5. Se houver falhas, tome a ação apropriada para corrigir o problema e execute novamente a ferramenta de Pré-Verificação até que não haja mais falhas.

Resultados

Se a mensagem CHK0101W for emitida, é porque não existe servidor DNS configurado para o ambiente ou o servidor DNS não possui os servidores definidos. Esse aviso pode ser ignorado se os seus servidores forem definidos usando o endereçamento IP estático no arquivo */etc/hosts*.

Conceitos relacionados:

“Rede TCP/IP” na página 20

Antes de instalar o IBM Intelligent Operations Center, a rede TCP/IP entre os servidores deve ser configurada corretamente.

Configurações de Segurança do Linux

As configurações de segurança do Linux devem ser alteradas para ativar o Ferramenta de Controle de Plataforma.

Essas configurações podem ser alteradas executando uma série de comandos ou utilizando um script.

O script realiza as mudanças indicadas pelos comandos. Se os comandos não atenderem às necessidades de instalação, ou se os processos da empresa não permitirem que alterações de segurança sejam feitas utilizando um script, altere as configurações utilizando comandos individuais.

Adaptando Manualmente as Configurações de Segurança do Linux

As configurações de segurança do Linux exigidas podem ser feitas executando uma série de comandos.

Procedimento

1. No servidor de instalação, efetue logon usando raiz ou execute o comando **su** - para alternar para a conta raiz.
2. Faça o seguinte para ativar o Ferramenta de Controle de Plataforma. Essas etapas precisam ser executadas para cada um dos seguintes servidores de destino:
 - Servidor de aplicativos
 - servidor de dados
 - Servidor de eventos
 - Servidor de Gerenciamento
 - a. Execute o comando **visudo**. O arquivo `/etc/sudoers` será aberto para edição.
 - b. Digite a letra `i` para alterar para o modo de inserção, que permite fazer mudanças no arquivo.
 - c. Localize a seguinte linha:

```
#%wheel ALL=(ALL) NOPASSWD: ALL
```

E altere a linha para:

```
%wheel ALL=(ALL) NOPASSWD: ALL
```
 - d. Inclua a seguinte linha ao final do arquivo:

```
Defaults:%wheel !requiretty
```
 - e. Pressione Esc. O modo de inserção é encerrado.
 - f. Insira `:wq`. O arquivo é salvo.
 - g. Execute o comando **exit**. O sistema retorna ao login do servidor de instalação.

Quando concluído para os quatro servidores, a segurança do Linux permite que os usuários no grupo `wheel` usem o comando **sudo** para executar comandos do sistema localmente ou de uma sessão remota.

Tarefas relacionadas:

“Customizando Configurações de Segurança Linux com um Script”

As configurações de segurança Linux requeridas podem ser realizadas ao executar um script.

Customizando Configurações de Segurança Linux com um Script

As configurações de segurança Linux requeridas podem ser realizadas ao executar um script.

Sobre Esta Tarefa

No servidor de instalação, acesse o diretório no qual o pacote de instalação do IBM Intelligent Operations Center foi copiado. Nestas etapas, este diretório é referido como *install_home*.

Procedimento

1. Altere para o diretório *install_home/ioc*.
2. Execute o comando **bin/install-prepare-env.sh -d *install_home/ioc* -f *topology/iop_lite_topo.properties* -p *password*** em que *password* é a senha da topologia.

Tarefas relacionadas:

“Adaptando Manualmente as Configurações de Segurança do Linux” na página 42

As configurações de segurança do Linux exigidas podem ser feitas executando uma série de comandos.

O Comando **installTopology**

O comando **installTopology** usa as informações no arquivo de topologia para instalar o IBM Intelligent Operations Center.

Antes de usar o arquivo de topologia para instalar o IBM Intelligent Operations Center, o comando **installTopology** verificará se os arquivos de instalação foram copiados para os servidores de destino. Se os arquivos não foram copiados, o comando **installTopology** copiará os arquivos necessários antes de continuar.

Usando o arquivo de topologia como guia, o comando **installTopology** instalará cada componente do IBM Intelligent Operations Center e fará qualquer configuração necessária. As mensagens são exibidas durante a instalação, indicando o progresso da instalação.

Se ocorrer um erro durante o processamento do comando **installTopology**, a instalação poderá ser reiniciada depois de solucionar o motivo da falha de um ou mais componentes da instalação. Instalações com falha são indicadas pelo status de instalação no arquivo de topologia.

Nota: Em um ambiente virtual, é sugerido que uma captura instantânea do ambiente seja feita antes da execução do comando **installTopology** e após cada instalação bem sucedida.

Status da Instalação

O atributo **Status** do arquivo de topologia indica o status de instalação de cada componente. Quando o comando **installTopology** é executado, a ação indicada na Tabela 19 será tomada dependendo do status para o componente.

Tabela 19. Status de Instalação e Ações

Valor	Status	Ação installTopology
Novo	O componente não foi instalado.	O status será alterado para Incerto e o componente será instalado. Quando o componente for instalado com sucesso, o status será alterado para Pronto.
Pronto	O componente foi instalado com sucesso.	A instalação do componente será ignorada quando o comando installTopology for instalado novamente.
Indefinido	O componente não foi instalado com sucesso ou a instalação está em andamento.	O componente será instalado. Quando o componente for instalado com sucesso, o status será alterado para Pronto.

Opções de Instalação dos Componentes do IBM Intelligent Operations Center

A instalação do IBM Intelligent Operations Center pode levar muitas horas. Devido ao tempo exigido, o IBM Intelligent Operations Center pode ser instalado em uma ou diversas fases.

Em uma instalação de fase única, o processo de instalação será executado até que todos os componentes sejam instalados ou haverá uma falha na instalação. Se a instalação falhar, deverá ser reiniciada a partir do início.

Em uma instalação de diversas fases, o processo de instalação é dividido em três fases distintas:

uploadTopology

Copia os arquivos de instalação do servidor de instalação para os servidores de destino.

Fase 1 Instala alguns dos componentes do IBM Intelligent Operations Center criando uma base para a instalação dos componentes restantes.

Fase 2 Instala os componentes restantes do IBM Intelligent Operations Center.

Ao ser executado em um ambiente virtualizado, uma captura instantânea deve ser feita depois de cada fase, caso seja necessário uma reinicialização.

A fase **uploadTopology** é executada como um comando separado. Se os arquivos de instalação já foram copiados para os servidores de destino, não são copiados novamente.

A fase, ou fases, a serem executadas são definidas no arquivo de propriedades da topologia. As propriedades **Status.Phase1** e **Status.Phase2** determinam se as fases da instalação serão executadas quando o comando **installTopology** estiver em execução. Se configurado para Novo, a fase será executada. Se configurado para Pronto, a fase será ignorada.

Instalando Arquitetura do IBM Intelligent Operations Center em uma Única Fase

A arquitetura usada com o IBM Intelligent Operations Center pode ser instalada em uma única fase. Se estiver instalando em um ambiente virtualizado, a execução da instalação em uma única fase não permitirá que capturas instantâneas sejam feitas durante o processo de instalação.

Sobre Esta Tarefa

No servidor de instalação, acesse o diretório no qual o pacote de instalação do IBM Intelligent Operations Center foi copiado. Nestas etapas, este diretório é referido como *install_home*.

Procedimento

1. No servidor de instalação, abra uma janela do terminal e efetue logon como raiz. Se não tiver efetuado logon como raiz, alterne para a conta raiz executando o comando **su -**.
2. Copie os arquivos necessários para a instalação nos servidores de destino e instale o IBM Intelligent Operations Center.
 - a. Altere para o diretório *install_home/ioc*.
 - b. Execute o comando **export JAVA_HOME=/opt/ibm/java-x86_64-60/jre**.
 - c. Execute o comando **bin/ba.sh installTopology -t iop_lite_topo -p password**, em que *password* é a senha de topologia.

Os arquivos de instalação necessários serão copiados nos servidores de destino e o IBM Intelligent Operations Center será instalado.

As mensagens são exibidas indicando o progresso da instalação. As mensagens indicam o status do componente instalado. O status será um dos seguintes:

[OK] Componente instalado com êxito.

[Fail]

A instalação do componente falhou.

Resultados

O processo de instalação pode ser executado em aproximadamente 14 horas. A arquitetura do IBM Intelligent Operations Center é instalada com sucesso quando as mensagens forem concluídas com um status [OK].

Instalando a Arquitetura do IBM Intelligent Operations Center em Várias Fases

A arquitetura usada com o IBM Intelligent Operations Center pode ser instalada em várias fases. Uma instalação multi-fase irá permitir resolver mais cedo problemas de instalação, ao invés de esperar pela conclusão de todo o processo. Se estiver instalando em um ambiente virtualizado, a execução da instalação em várias fases também permitirá fazer capturas instantâneas durante o processo de instalação.

Sobre Esta Tarefa

Importante: Não encerre os servidores entre as fases de instalação. O encerramento dos servidores entre fases não foi testado e pode gerar em resultados imprevisíveis.

Procedimento

1. No servidor de instalação, abra uma janela do terminal e efetue logon como raiz. Se não tiver efetuado logon como raiz, alterne para a conta raiz executando o comando **su -**.
2. Execute o comando **export JAVA_HOME=/opt/ibm/java-x86_64-60/jre**.
3. Copie os arquivos de instalação para os servidores de destino.
 - a. Altere para o diretório *install_home/ioc*.
 - b. Execute o comando **bin/ba.sh uploadImage -t iop_lite_topo -threadCount 4 -p password** em que *password* é a senha de topologia. O parâmetro **-threadCount** especifica o número de encadeamentos usados ao copiar os arquivos de instalação. O valor pode ser alterado, se necessário.

Os arquivos necessários para cada servidor de destino são copiados do servidor de instalação para os servidores de destino. Esta etapa pode ser executada em aproximadamente 2 horas.

As mensagens são exibidas, indicando o progresso do upload. As mensagens indicam o status do componente transferido por upload. O status será um dos seguintes:

[OK] Componente transferido por upload com sucesso.

[Fail]

Falha no upload do componente.

4. Opcional: Se estiver instalando em um ambiente virtualizado, faça uma captura instantânea de todos os servidores de destino. Encerre as máquinas virtuais antes de fazer a captura instantânea, para salvar o espaço em disco e o tempo de processamento. Após obter a captura instantânea, reinicie as máquinas virtuais. A captura instantânea pode ser usada para reiniciar a instalação deste ponto, se ocorrerem erros durante o processo de instalação subsequente.
5. Preparar a execução da fase de instalação 1.
 - a. Usando um editor de texto, edite o arquivo de propriedades da topologia: *install_home/ioc/topology/iop_lite_topo.properties*.
 - b. Altere os valores do status conforme mostrado:

```
Status.Phase1="New"
Status.Phase2="Ready"
```

Isso irá solicitar que o programa de instalação instale a primeira fase e ignore a segunda.
 - c. Altere para o diretório *install_home/ioc*.

- d. Execute o comando **cp topology/iop_lite_topo.template.xml topology/iop_lite_topo.xml**. O arquivo de modelo de topologia será copiado para o arquivo de topologia.
 - e. Execute o comando **bin/ba.sh parameterizeTopology -t iop_lite_topo -r topology/iop_lite_topo.properties -p password** em que *password* é a senha de topologia. Os valores da propriedade definidos no arquivo de propriedades da topologia serão aplicados no arquivo de topologia.
 - f. Opcional: Execute o comando **bin/ba.sh encryptTopology -t iop_lite_topo -p password** em que *password* é a sua senha de topologia. As senhas no arquivo de topologia serão criptografadas usando a senha de topologia fornecida.
6. Execute a fase 1 da instalação.
 - a. Altere para o diretório *install_home/ioc*.
 - b. Execute o comando **export JAVA_HOME=/opt/ibm/java-x86_64-60/jre**.
 - c. Execute o comando **bin/ba.sh installTopology -t iop_lite_topo -p password**, em que *password* é a senha de topologia.

A instalação dos componentes necessários é feita para o IBM Intelligent Operations Center. Esta etapa pode ser executada em aproximadamente 9 horas.

As mensagens são exibidas indicando o progresso da instalação. As mensagens indicam o status do componente instalado. O status será um dos seguintes:

[OK] Componente instalado com êxito.

[Fail]

A instalação do componente falhou.

7. Opcional: Se estiver instalando em um ambiente virtualizado, faça uma captura instantânea de todos os servidores de destino. Não encerre os servidores virtuais antes de fazer a captura instantânea. Ao fazer a captura instantânea, inclua uma captura instantânea da memória da máquina virtual. A captura instantânea pode ser usada para reiniciar a instalação deste ponto, se ocorrerem erros durante o processo de instalação subsequente.
8. Preparar a execução da fase de instalação 2.
 - a. Usando um editor de texto, edite o arquivo de propriedades da topologia: *install_home/ioc/topology/iop_lite_topo.properties*.
 - b. Altere os valores do status conforme mostrado:


```
Status.Phase1="Ready"
Status.Phase2="New"
```

Isso irá solicitar que o programa de instalação instale a segunda fase e ignore a primeira.
 - c. Altere para o diretório *install_home/ioc*.
 - d. Execute o comando **cp topology/iop_lite_topo.template.xml topology/iop_lite_topo.xml**. O arquivo de modelo de topologia será copiado para o arquivo de topologia.
 - e. Execute o comando **bin/ba.sh parameterizeTopology -t iop_lite_topo -r topology/iop_lite_topo.properties -p password** em que *password* é a senha de topologia. Os valores da propriedade definidos no arquivo de propriedades da topologia serão aplicados no arquivo de topologia.
 - f. Opcional: Execute o comando **bin/ba.sh encryptTopology -t iop_lite_topo -p password** em que *password* é a sua senha de topologia. As senhas no arquivo de topologia serão criptografadas usando a senha de topologia fornecida.
9. Execute a fase 2 da instalação.
 - a. Altere para o diretório *install_home/ioc*.
 - b. Execute o comando **export JAVA_HOME=/opt/ibm/java-x86_64-60/jre**.
 - c. Execute o comando **bin/ba.sh installTopology -t iop_lite_topo -p password**, em que *password* é a senha de topologia.

A instalação dos componentes necessários restantes é feita para o IBM Intelligent Operations Center. Esta etapa pode ser executada em aproximadamente 4 horas.

As mensagens são exibidas indicando o progresso da instalação. As mensagens indicam o status do componente instalado. O status será um dos seguintes:

[OK] Componente instalado com êxito.

[Fail]

A instalação do componente falhou.

Resultados

A arquitetura do IBM Intelligent Operations Center é instalada com sucesso quando as mensagens forem concluídas com um status [OK].

Reiniciando a Instalação de Arquitetura do IBM Intelligent Operations Center Durante uma Instalação Passo-a-Passo

Se a instalação da arquitetura falhar, a instalação poderá ser reiniciada.

Sobre Esta Tarefa

Para reiniciar uma instalação malsucedida, faça o seguinte.

Procedimento

1. Edite o arquivo de topologia para determinar qual componente falhou. Isso será indicado por `Status="Uncertain"`.
2. Determine e resolva a causa do erro. A ferramenta de coleta de informações da instalação pode ser usada para coletar os logs de instalação para revisão.
3. Execute novamente o comando `installTopology`. A instalação será reativada. Todos os componentes com `Status="New"` e `Status="Uncertain"` serão instalados. Componentes com `Status="Ready"` foram instalados com sucesso e serão ignorados.

O que Fazer Depois

Algumas vezes uma instalação do componente com falha não será bem sucedida. Nesse caso, será necessário recriar o ambiente antes da execução do comando `installTopology` e, em seguida, reiniciar a instalação. Para o ambiente com virtualização, as capturas instantâneas do ambiente podem ser utilizadas para reverter rapidamente o sistema para o estado em que estava antes da execução do comando `installTopology`.

Tarefas relacionadas:

“Executando a Ferramenta de Instalação Coleta de Informações” na página 299

Os arquivos de log são gerados enquanto o IBM Intelligent Operations Center é instalado. Uma ferramenta está disponível para reunir esses arquivos de log para análise.

Instalando o Ferramenta de Controle de Plataforma

O Ferramenta de Controle de Plataforma é usado para gerenciar o ambiente do servidor do IBM Intelligent Operations Center. A ferramenta é instalada separadamente do produto.

Antes de Iniciar

O produto do IBM Intelligent Operations Center deve ser instalado antes de instalar o Ferramenta de Controle de Plataforma.

Sobre Esta Tarefa

No servidor de instalação, acesse o diretório no qual o pacote de instalação do IBM Intelligent Operations Center foi copiado. Nestas etapas, este diretório é referido como *install_home*.

Procedimento

1. No servidor de instalação, abra uma janela do terminal e efetue logon como raiz. Se não tiver efetuado logon como raiz, alterne para a conta raiz executando o comando `su -`.
2. Altere para o diretório `install_home/isp/mgmt/setup`.
3. Execute o comando `./iopmgmt-install.sh -f install_home/ioc/topology/iop_lite_topo.properties -p password` em que *password* é a senha que você deseja usar para acessar a ferramenta. Lembre-se dessa senha, pois precisará dela quando executar a ferramenta. O Ferramenta de Controle de Plataforma está instalado com êxito no Servidor de Gerenciamento quando todos os componentes são mostrados instalados com o status [OK].
4. Opcional: Se não estiver usando o Java fornecido pelo IBM Intelligent Operations Center, no Servidor de Gerenciamento edite os arquivos `/opt/IBM/ISP/mgmt/scripts/CommandEngine.sh` e `/opt/IBM/ISP/mgmt/scripts/UpdateProperty.sh`. Mude o valor de `export JAVA_HOME=` em cada arquivo para o local do Java JRE no servidor.

O que Fazer Depois

Verifique se o Ferramenta de Controle de Plataforma foi instalado corretamente iniciando, parando e consultando serviços usando o Ferramenta de Controle de Plataforma.

Conceitos relacionados:

“Instalação de Arquivos de Topologia” na página 34

O IBM Intelligent Operations Center é instalado usando um arquivo de topologia. O arquivo de topologia é um arquivo XML que define os parâmetros e valores usados quando o IBM Intelligent Operations Center é implementado nos servidores e define a sequência usada para implementar componentes.

Tarefas relacionadas:

“Iniciando os Serviços” na página 195

O Ferramenta de Controle de Plataforma está disponível para iniciar os serviços em execução nos servidores IBM Intelligent Operations Center.

“Parando os Serviços” na página 199

O Ferramenta de Controle de Plataforma está disponível para parar os serviços do IBM Intelligent Operations Center.

“Consultando o Status dos Serviços” na página 202

O Ferramenta de Controle de Plataforma está disponível para determinar o status dos serviços do IBM Intelligent Operations Center.

Instalando a Ferramenta de Verificação do Sistema

A ferramenta de Verificação do Sistema é usada para verificar o status operacional dos componentes no IBM Intelligent Operations Center. A ferramenta é instalada separadamente do produto.

Antes de Iniciar

O produto do IBM Intelligent Operations Center deve ser instalado antes da instalação da ferramenta de Verificação do Sistema.

Sobre Esta Tarefa

No servidor de instalação, acesse o diretório no qual o pacote de instalação do IBM Intelligent Operations Center foi copiado. Nestas etapas, este diretório é referido como *install_home*.

Procedimento

1. No servidor de instalação, abra uma janela do terminal e efetue logon como raiz. Se não tiver efetuado logon como raiz, alterne para a conta raiz executando o comando **su -**.
2. Execute o comando **export JAVA_HOME=/opt/ibm/java-x86_64-60/jre**.
3. Vá para o diretório do *install_home/cat/bin*.
4. Execute o comando **./install-cat-lite.sh -d install_home/cat -f install_home/ioc/topology/iop_lite_topo.properties -p password** em que *password* é a senha da topologia.

Nota: O comando deve ser executado a partir do diretório *install_home/cat/bin*.

A ferramenta de Verificação do Sistema será instalada com sucesso quando todos os componentes forem exibidos com o status [OK].

5. Reinicie todos os servidores IBM Intelligent Operations Center.
 - a. Encerre todos os servidores IBM Intelligent Operations Center usando o Ferramenta de Controle de Plataforma.
 - b. Encerre e reinicie todos os servidores a partir do sistema operacional.
 - c. Inicie todos os servidores IBM Intelligent Operations Center usando o Ferramenta de Controle de Plataforma.

O que Fazer Depois

Verifique se a ferramenta de Verificação do Sistema foi instalada corretamente, executando a ferramenta Verificação do Sistema.

Tarefas relacionadas:

“Como Usar a Ferramenta Verificação do Sistema” na página 210

A ferramenta de Verificação do Sistema é usada para determinar o status operacional dos serviços que abrangem o sistema IBM Intelligent Operations Center.

“Parando os Serviços” na página 199

O Ferramenta de Controle de Plataforma está disponível para parar os serviços do IBM Intelligent Operations Center.

“Iniciando os Serviços” na página 195

O Ferramenta de Controle de Plataforma está disponível para iniciar os serviços em execução nos servidores IBM Intelligent Operations Center.

Instalando o aplicativo do IBM Intelligent Operations Center

Instale o aplicativo do IBM Intelligent Operations Center depois que a arquitetura do IBM Intelligent Operations Center, incluindo a do Verificação do Sistema e do Ferramenta de Controle de Plataforma, for instalada.

Antes de Iniciar

A arquitetura do IBM Intelligent Operations Center deve ser instalada e todos os serviços iniciados.

Procedimento

1. No servidor de instalação, abra uma janela do terminal e efetue logon como raiz. Se não tiver efetuado logon como raiz, alterne para a conta raiz executando o comando **su -**.
2. Execute o comando **export JAVA_HOME=/opt/ibm/java-x86_64-60/jre**.
3. Altere para o diretório *install_home/ioc*.
4. Execute o comando **cp topology/iop_lite_topo.xml topology/iop_lite_topo_phase2.xml**.
5. Execute o comando **bin/ba.sh installTopology -t ioc_lite_topo -p password**, onde *password* é a senha de topologia. O aplicativo do IBM Intelligent Operations Center é instalado. Esta etapa pode ser executada em aproximadamente uma hora.

As mensagens são exibidas indicando o progresso da instalação. As mensagens indicam o status do componente instalado. O status será um dos seguintes:

[OK] Componente instalado com êxito.

[Fail]

A instalação do componente falhou.

Resultados

O aplicativo do IBM Intelligent Operations Center foi instalado com sucesso quando todas as mensagens são concluídas com um status [OK].

Verificando a instalação

Depois de instalar o IBM Intelligent Operations Center, verifique se o produto foi instalado corretamente.

Procedimento

Inicie todos os serviços.

1. Inicie todos os serviços do IBM Intelligent Operations Center executando o Ferramenta de Controle de Plataforma com o parâmetro **iniciar todos**.
2. Verifique se todos os serviços foram iniciados com sucesso, revisando as mensagens exibidas.
3. Execute todos os testes na ferramenta do Verificação do Sistema.
4. Verifique se todos os testes foram executados com sucesso.

Como opção, encerre e reinicie todos os serviços.

5. Interrompa todos os serviços do IBM Intelligent Operations Center, executando o Ferramenta de Controle de Plataforma com o parâmetro **interromper todos**.
6. Verifique se todos os serviços foram interrompidos com sucesso, revisando as mensagens exibidas.
7. Encerre o sistema operacional Linux em todos os servidores.
8. Desligue e ligue todos os servidores de runtime ou reinicialize todos os servidores.
9. Inicie todos os serviços do IBM Intelligent Operations Center executando o Ferramenta de Controle de Plataforma com o parâmetro **iniciar todos**.
10. Verifique se todos os serviços foram iniciados com sucesso, revisando as mensagens exibidas.
11. Execute todos os testes na ferramenta do Verificação do Sistema.
12. Verifique se todos os testes foram executados com sucesso.

O que Fazer Depois

Se algum erro for observado, resolva os erros e execute novamente essas etapas.

Conceitos relacionados:

“Sobre” na página 195

Use o portlet Sobre para visualizar detalhes da versão do IBM Intelligent Operations Center e IBM Smarter Cities Software Solutions integrado que você instalou. Também é possível visualizar detalhes de quaisquer atualizações aplicadas desde sua instalação.

Tarefas relacionadas:

“Iniciando os Serviços” na página 195

O Ferramenta de Controle de Plataforma está disponível para iniciar os serviços em execução nos servidores IBM Intelligent Operations Center.

“Instalando o IBM Intelligent Operations Center Utilizando o Installation Manager” na página 25

O IBM Intelligent Operations Center pode ser instalado usando o instalador gráfico fornecido.

“Parando os Serviços” na página 199

O Ferramenta de Controle de Plataforma está disponível para parar os serviços do IBM Intelligent Operations Center.

“Como Usar a Ferramenta Verificação do Sistema” na página 210

A ferramenta do Verificação do Sistema é usada para determinar o status operacional dos serviços que abrangem o sistema IBM Intelligent Operations Center.

Configuração da Pós-Instalação do IBM Intelligent Operations Center

Após a instalação da arquitetura do IBM Intelligent Operations Center utilizando o Installation Manager ou passo-a-passo, diversas etapas da configuração de pós-instalação precisam ser executadas para concluir a instalação.

Importante: Todo o trabalho de configuração pós-instalação precisa ser feito antes que o Cyber Hygiene seja instalado.

Tarefas relacionadas:

“Instalando o IBM Intelligent Operations Center Utilizando o Installation Manager” na página 25

O IBM Intelligent Operations Center pode ser instalado usando o instalador gráfico fornecido.

Configurando os Serviços de Colaboração para IPv6

Se a sua instalação utiliza a rede IPv6, as etapas de configuração são necessárias para os serviços de colaboração.




Sobre Esta Tarefa

A arquitetura do IBM Intelligent Operations Center precisa ser instalada antes de configurar a rede IPv6 para serviços de configuração.

Procedimento

1. Siga as etapas na documentação do Lotus Domino para configurar o Lotus Domino para endereçamento do IPv6.
2. Siga as etapas na documentação do Lotus Sametime Standard para configurar o Lotus Sametime Standard para endereçamento do IPv6.
3. Siga as etapas na documentação do WebSphere Portal para configurar confiança para o portlet Lista de Contatos do Sametime se não estiver usando uma rede IPv4 com um endereço IPv4 designado para o.

Informações relacionadas:

-  Configurando o Lotus Domino para endereçamento do IPv6
-  Configurando o Sametime Community Server para dar suporte ao IPv6
-  Configurando confiança para o portlet Lista de Contatos do Sametime

Configurando Conexão Única para Serviços de Colaboração

Importe o token SSO LTPA do WebSphere Portal para o , a fim de permitir que usuários acessem os serviços de colaboração sem precisar inserir novamente suas credenciais.

Sobre Esta Tarefa

A arquitetura do IBM Intelligent Operations Center precisa ser instalada antes de importar o token Lightweight Third-Party Authentication (LTPA).

Este token foi criado durante a instalação da arquitetura do IBM Intelligent Operations Center.

Procedimento

1. Instale um cliente do Lotus Notes 8.5.x em uma estação de trabalho. Uma instalação existente pode ser utilizada. A estação de trabalho deve ser capaz de se conectar ao sobre o TCP/IP, usando o nome completo do host.
2. Copie o arquivo `/opt/pdweb/etc/stproxy.ltpa` do servidor de aplicativos para a estação de trabalho que está executando o Lotus Notes. Esse é o token LTPA que será importado para o diretório de serviços de colaboração.
3. Copie o arquivo `/local/notesdata/admin.id` do para a estação de trabalho que está executando o Lotus Notes. Esse é o arquivo de ID para o administrador de serviços de colaboração. Ele usará este ID para efetuar login no diretório de serviços de colaboração.
4. Na estação de trabalho, inicie o cliente do Lotus Notes e efetue o logon com o arquivo `admin.id`.
 - a. No log do Lotus Notes no painel, clique em **Nome de Usuário**.
 - b. Navegue até o diretório em que o arquivo `admin.id` foi copiado e o selecione.
 - c. Insira a senha definida no arquivo de propriedades da topologia para a propriedade `DOMINO.ADMIN.PWD`.
 - d. Clique em **Sim** se um aviso de segurança for exibido.
5. Abra o arquivo `names.nsf`.
 - a. Clique em **Arquivo > Abrir > Aplicativo Lotus Notes**.
 - b. Insira o nome completo do host do em **Consultar**.
 - c. Insira `names.nsf` em **Nome do Arquivo**.
 - d. Clique em **Abrir**.
6. Navegue até o **Web > Configurações da Web**.
7. Selecione Configuração SS0 da Web para Token LTPA e clique em **Editar Documento**.
8. Clique em **Chaves > Importar Chaves WebSphere LTPA**. Clique em **OK** se for recebido um aviso sobre a sobrescrição de chaves existentes.
9. Insira o caminho para onde o arquivo `stproxy.ltpa` foi copiado. Clique em **OK**.
10. Insira a senha para o token LTPA. A senha é definida no arquivo de propriedades da topologia `WAS.LTPA.PWD`.
11. Clique em **OK > Salvar e Fechar**.
12. Reinicie o serviço de colaboração utilizando o Ferramenta de Controle de Plataforma.
 - a. Efetue logon no Servidor de Gerenciamento e abra uma janela do terminal.

- b. Execute `su -ibmadmin`.
- c. Execute `/opt/IBM/ISP/mgmt/scripts/IOControl.sh stop st password` em que *password* é a senha para o Ferramenta de Controle de Plataforma definida quando o Ferramenta de Controle de Plataforma foi instalado.
- d. Execute `/opt/IBM/ISP/mgmt/scripts/IOControl.sh start st password` em que *password* é a senha para o Ferramenta de Controle de Plataforma definida quando o Ferramenta de Controle de Plataforma foi instalado.

Configurando o Tempo Limite da Sessão

O tempo limite da sessão determina o tempo que um usuário pode permanecer inativo antes de a sessão ser finalizada e o usuário ter de efetuar novamente o login. O tempo limite da sessão inclui administradores que efetuaram login por meio do serviço do portal.

Sobre Esta Tarefa

Quando o IBM Intelligent Operations Center é instalado, nenhum tempo limite de sessão é definido. Os usuários permanecerão conectados até que seja efetuado o logout, mesmo que a sessão esteja inativa.

Se sua organização possuir políticas de segurança exigindo que as sessões efetuem logout depois de um período de inatividade, utilize as seguintes etapas para definir um tempo limite de sessão para o sistema do IBM Intelligent Operations Center.

Procedimento

1. Utilizando um navegador da web, acesse `http://application_server:9060/ibm/console`, onde *application_server* é o nome do host do servidor de aplicativos.
2. Efetue logon como o usuário `waswebadmin` com a senha definida para `PORTAL.ADMIN.ACCOUNT.PWD` no arquivo de propriedades de topologia.
3. Clique em **Servidores > Tipo de Servidor > WebSphere Application Servers > WebSphere Portal**.
4. Clique em **Configurações de Contêiner > Gerenciamento de sessão > Configurar Tempo Limite**.
5. Insira o valor do tempo limite desejado em minutos.
6. Clique em **OK**.
7. Clique em **Salvar**.
8. Clique em **Servidores > Tipo de Servidor > WebSphere Application Servers > STProxyServer1**.
9. Clique em **Configurações de Contêiner > Gerenciamento de sessão > Configurar Tempo Limite**.
10. Insira o valor do tempo limite desejado em minutos.
11. Clique em **OK**.
12. Clique em **Salvar**.
13. Clique em **Servidores > Tipo de Servidor > WebSphere Application Servers > CongnosX_GW1**.
14. Clique em **Configurações de Contêiner > Gerenciamento de sessão > Configurar Tempo Limite**.
15. Insira o valor do tempo limite desejado em minutos.
16. Clique em **OK**.
17. Clique em **Salvar**.
18. Clique em **Servidores > Tipo de Servidor > WebSphere Application Servers > CongnosX_Displ1**.
19. Clique em **Configurações de Contêiner > Gerenciamento de sessão > Configurar Tempo Limite**.
20. Insira o valor do tempo limite desejado em minutos.
21. Clique em **OK**.
22. Clique em **Salvar**.
23. Interrompa e reinicie o servidor de aplicativos

24. No servidor de aplicativos, efetue logon como o usuário `ibmadmin` com a senha definida para `IOP.ADMIN.USER.PWD` no arquivo de propriedades de topologia.
25. Execute o comando `sudo su -` para alternar para o usuário raiz.
26. Edite o arquivo `/opt/pdweb/etc/webseald-default.conf` com um editor de texto.
27. Na seção **CONFIGURAÇÕES DE CACHE DA SESSÃO**, altere o valor `timeout = 0` para o tempo limite da sessão desejada em segundos. O tempo limite deve ser o mesmo que o tempo configurado para o serviço do portal. No entanto, o valor do portal é configurado em minutos e a configuração de cache da sessão é especificada em segundos. O valor de tempo limite das configurações de cache da sessão deve ser exatamente 60 vezes o valor configurado para o serviço do portal. Por exemplo, se o valor do portal é 30 (minutos), as configurações de cache da sessão devem ser 1800 (segundos).
28. Execute o comando `/usr/bin/pdweb restart` para reiniciar o serviço de segurança.

Instalando e Configurando o serviços de modelo semântico

O IBM Intelligent Operations Center fornece um aplicativo e um modelo de amostra do serviços de modelo semântico. Esse serviço precisa ser instalado e configurado antes da utilização.

Configurando o Jazz Team Server

O IBM Intelligent Operations Center serviços de modelo semântico é instalado em um Jazz Team Server. O Jazz Team Server precisa ser configurado antes de os IBM Intelligent Operations Center serviços de modelo semântico serem instalados.

Sobre Esta Tarefa

A arquitetura do IBM Intelligent Operations Center precisa ser instalada antes de configurar o Jazz Team Server.

Procedimento

1. Em um navegador da web, acesse `http://management_host:82/jts/setup`, onde *management_host* é o nome completo do host do Servidor de Gerenciamento.
2. Efetue logon com o ID de usuário `iicsystemuser` e a senha `passwd0rd`.
3. Clique em **Avançar**.
4. Na página Configurar URI Pública, forneça um valor **Raiz de URI Pública** no formulário `https://management_host:9448/jts` e selecione Entendo que após a URI Pública ser configurada, ela não poderá ser modificada.. Clique em **Avançar**.
5. Clique em **Testar Conexão**. Deve ser exibida uma mensagem, informando que o teste de configuração foi bem sucedido.
6. Clique em **Avançar** para salvar as configurações e continue.
7. Configure o banco de dados na página Configurar Banco de Dados.
 - a. Selecione DB2 para **Fornecedor de Banco de Dados**.
 - b. Selecione JDBC para **Tipo de Conexão**.
 - c. Insira a senha do bando de dados DB2 definida como a propriedade do `DEFAULT.PWD.DB2` no arquivo de propriedades de topologia para **Senha JDBC**. Ignore a mensagem de senha exibida.
 - d. Para **Local JDBC** insira `//db_host:50005/JTS:user=db2inst5;password={password};`, onde *db_host* é o nome do host do servidor de dados. A {senha} sequência deve ser inserida conforme mostrado. Não substitua com um valor de senha.
 - e. Clique em **Testar Conexão**. Se um erro ocorrer, verifique e corrija todas as entradas. Se as entradas estiverem corretas, certifique-se de que os serviços do banco de dados sejam iniciados no servidor de dados usando o Ferramenta de Controle de Plataforma.
 - f. Depois que uma mensagem de que não há tabelas do Jazz presentes no banco de dados é exibida, clique em **Criar Tabelas**. O processamento levará alguns minutos para ser concluído.
 - g. Clique em **Avançar**.

8. Na página Ativar Notificação de E-mail configure o valor para **Desativado** e clique em **Avançar**.
9. A página Registrar Aplicativos deverá exibir "Nenhum aplicativo novo detectado." Clique em **Avançar**.
10. Selecione **LDAP** para o **Tipo de Registro do Usuário** na Etapa 1 na página Configurar Registro do Usuário.
11. Na Etapa 2 configure LDAP para o registro do Jazz Team Server.
 - a. Insira `ldap://mgmt_host:389` para **Local de Registro de LDAP**, onde *mgmt_host* é o nome completo do host do Servidor de Gerenciamento.
 - b. Insira `OU=USERS,OU=SWG,O=IBM,C=US` para **DN do Usuário de Base**.
 - c. Insira `userId=uid,name=cn,emailAddress=mail` para **Mapeamento de Nomes de Propriedades**.
 - d. Insira `OU=GROUPS,OU=SWG,O=IBM,C=US` para **DN Grupo de Base**.
 - e. Para **Jazz para Mapeamento do Grupo LDAP**, certifique-se de que o valor seja configurado para `JazzAdmins=JazzAdmins, JazzUsers=JazzUsers, JazzDWAdmins=JazzDWAdmins, JazzProjectAdmins=JazzProjectAdmins, JazzGuests=JazzGuests`.
 - f. Insira `cn` para **Propriedade de Nome do Grupo**.
 - g. Insira `cn` para **Propriedade do Membro do Grupo**.
12. Clique em **Testar Conexão**. Se uma mensagem de aviso for exibida, clique em **exibir detalhes**. Se a mensagem for sobre a propriedade correio, a mensagem poderá ser ignorada.
13. Para **Tipo de Licença de Acesso do Cliente** selecione **IBM Integrated Information Core - IIC Model Server**.
14. Clique em **Avançar**.
15. Para **Configurar o Data Warehouse**, marque a caixa de seleção **Não desejo configurar o Data Warehouse** desta vez.
16. Clique em **Concluir** na página Resumo.

Resultados

O Jazz Team Server está em operação.

Instalando o serviços de modelo semântico

O serviços de modelo semântico e um aplicativo de amostra são fornecidos com o IBM Intelligent Operations Center.

Sobre Esta Tarefa

A configuração do Jazz Team Server no Servidor de Gerenciamento é necessário, antes de usar o serviços de modelo semântico.

Procedimento

1. Em um navegador da web, acesse `http://management_host:82/jts/admin` onde *management_host* é o nome completo do host do Servidor de Gerenciamento.
2. Na página de Administração do Servidor, clique em **Server > Configuração > Registrar Aplicações**.
3. Clique em **Incluir** na página Aplicativos Registrados.
4. Inclua o aplicativo do Servidor de Modelo na página Incluir Aplicativo.
 - a. Insira Servidor do Modelo para **Nome do Aplicativo**.
 - b. Insira `http://management_host:82/modelserver/scr`, onde *management_host* é o nome completo do host do Servidor de Gerenciamento, para a **URL de Descoberta**.
 - c. Insira um valor de sua escolha para **Segredo do Consumidor**. Este valor será usado para fornecer acesso ao aplicativo. O valor deve ser tratado com a mesma segurança de uma senha.
 - d. Insira `iicsystemuser` para **ID Funcional**

O **Tipo de Aplicativo** será alterado para Servidor do Modelo.

5. Se não houver erros, clique em **Concluir**.

Verificando a Configuração do serviços de modelo semântico

Um aplicativo de amostra do serviços de modelo semântico é fornecido com o IBM Intelligent Operations Center e pode ser usado para verificar a instalação e configuração corretas do serviços de modelo semântico.

Procedimento

1. Preparar arquivos de modelo de amostra.
 - a. No servidor de instalação, localize o arquivo `iic15_2_stagebuiltdtoserver.xx.jar` no diretório `install_media`.
 - b. Expanda o arquivo `iic15_2_stagebuiltdtoserver.xx.jar` em um diretório de sua escolha. No restante dessas etapas, este diretório será conhecido como `model_home`.
2. Instale o modelo de amostra.
 - a. Em um navegador da web no servidor onde está localizado o `model_home`, acesse `http://mgmt_host:82/iic/console`, onde `mgmt_host` é o nome completo do host do Servidor de Gerenciamento.
 - b. Efetue login como usuário `iicssystemuser`, com `passwd` como senha.
 - c. Clique em **Gerenciador de Modelos > Ontologias > Navegar**.
 - d. Navegue até o diretório `install_media/ioc/image/IIC/install/modelServices/post_install/`.
 - e. Abra o arquivo `rsm.owl`.
 - f. Clique em **Carregar**. O arquivo será carregado.
 - g. Clique em **Gerenciador de Modelos > Ontologias > Navegar**.
 - h. Navegue até o diretório `install_media/ioc/image/IIC/install/modelServices/post_install/`.
 - i. Abra o arquivo `modelServer.owl`.
 - j. Clique em **Carregar**. O arquivo será carregado.
 - k. Clique em **Gerenciador de Modelos > Ontologias > Navegar**.
 - l. Navegue até o diretório `install_media/ioc/image/IIC/install/ktpRuntimeServices/post_install/`.
 - m. Abra o arquivo `kpi.owl`.
 - n. Clique em **Carregar**. O arquivo será carregado.
 - o. Clique em **Gerenciador de Modelos > Carregar > Navegar**.
 - p. Navegue até o diretório `install_media/ioc/image/IIC/samples/rdf/rsm/`.
 - q. Abra o arquivo `IBMOilDownstreamSampleRDF.xml`.
 - r. Clique em **Carregar**. O arquivo será carregado.
 - s. Clique em **Gerenciador de Modelos > Carregar > Navegar**.
 - t. Navegue até o diretório `install_media/ioc/image/IIC/samples/rdf/rsm/`.
 - u. Abra o arquivo `IBMOilUpstreamSampleRDF.xml`.
 - v. Clique em **Carregar**. O arquivo será carregado.
 - w. Clique em **Gerenciador de Modelos > Carregar > Navegar**.
 - x. Navegue até o diretório `install_media/ioc/image/IIC/samples/rdf/rsm/`.
 - y. Abra o arquivo `IBMOilDownstreamSampleReferenceRDF.xml`.
 - z. Clique em **Carregar**. O arquivo será carregado.
 - aa. Clique em **Gerenciador de Modelos > Carregar > Navegar**.
 - ab. Navegue até o diretório `install_media/ioc/image/IIC/samples/rdf/rsm/`.
 - ac. Abra o arquivo `IBMOilUpstreamSampleReferenceRDF.xml`.

- ad. Clique em **Carregar**. O arquivo será carregado.
- 3. Verifique se o modelo de amostra está instalado corretamente.
 - a. Clique em **Gerenciador de Modelos > Consultar > Consultar**. Será executada uma consulta predefinida. Será exibida uma estrutura XML exibida com os resultados da consulta. Uma tag de nível superior deve ser `spargl` e possuir tags secundárias `cabeçote` e `resultados`.
 - b. Clique em **Model Explorer** e certifique-se de que possa pesquisar o modelo.
- 4. Utilize o modelo para verificar a instalação do gerenciador de modelos.
 - a. Em um navegador da web no Servidor de Gerenciamento, acesse `http://mgmt_host:82/iic/ibmoil`, onde `mgmt_host` é o nome completo do host no Servidor de Gerenciamento.
 - b. Clique em **IBM Oil Company > Variáveis**. Serão exibidas as URLs de serviços da web.

Resultados

O serviços de modelo semântico e o modelo de amostra IBMOil serão instalados.

Melhorando o Desempenho do serviços de modelo semântico

Configure o serviços de modelo semântico fornecido pelo IBM Intelligent Operations Center para melhorar o desempenho ao executar as consultas relacionadas aos modelos.

Procedimento

1. Em um navegador da web, acesse `http://management_host:82/iic/console`, onde `management_host` é o nome completo do host do Servidor de Gerenciamento.
2. Inclua os valores da propriedade em Tabela 20 para a categoria **OPCWEBSERVICE**.

Tabela 20. Propriedades OPCWEBSERVICE

Propriedade	Valor
cache.browse.timetolive.second	3600
cache.timetolive.second	2592000
cache.wait.second.after.create.action	1

3. Atualize ou inclua as seguintes propriedades e valores do Tabela 21 na categoria RSM.

Tabela 21. Propriedades RSM

Propriedade	Valor
mvmViewPath.0	<code>http://iec.ch/TC57/CIMgeneric# ISA95_Enterprise##http://iec.ch/TC57/CIMgeneric# RSM_OrganizationalEntity.ManagesAspectOf_PhysicalEntity ##iec.ch/TC57/CIMgeneric# ISA95_Site##http://iec.ch/TC57/CIMgeneric# RSM_PhysicalEntity.contains_PhysicalEntity##http:// iec.ch/TC57/CIMgeneric# ISA95_Area##http://iec.ch/TC57/CIMgeneric# RSM_PhysicalEntity.contains_PhysicalEntity##http:// iec.ch/TC57/CIMgeneric# ISA95_ProductionUnit##http:// iec.ch/TC57/CIMgeneric# RSM_PhysicalEntity.ManagedBy_OrganizationalEntity##http:// iec.ch/TC57/CIMgeneric# RSM_OrganizationalEntity##http:// iec.ch/TC57/CIMgeneric# RSM_OrganizationalEntity.has_measurement##http:// iec.ch/TC57/CIM-generic#RSM_Measurement##http:// iec.ch/TC57/CIMgeneric# RSM_Measurement.HasA_MeasurementValue##http:// iec.ch/TC57/CIM-generic#RSM_MeasurementValue</code>

Tabela 21. Propriedades RSM (continuação)

Propriedade	Valor
mvmViewPath.1	http://iec.ch/TC57/CIMgeneric# ISA95_Enterprise##http://iec.ch/TC57/CIMgeneric# RSM_OrganizationalEntity.ManagesAspectOf_PhysicalEntity ##iec.ch/TC57/CIMgeneric# ISA95_Area##http://iec.ch/TC57/CIMgeneric# RSM_PhysicalEntity.contains_PhysicalEntity##http:// iec.ch/TC57/CIMgeneric# ISA95_ProductionUnit##http://iec.ch/TC57/CIMgeneric# ISA95_WorkCenter.Contains_Equipment##http:// iec.ch/TC57/CIMgeneric# RSM_WorkEquipment##http:// iec.ch/TC57/CIMgeneric# RSM_PhysicalEntity.has_measurement##http:// iec.ch/TC57/CIM-generic#RSM_Measurement##http:// iec.ch/TC57/CIMgeneric# RSM_Measurement.HasA_MeasurementValue##http:// iec.ch/TC57/CIM-generic#RSM_MeasurementValue
mvmDownLevelPreRequest	3
mvmCacheProperty.0	cim:RSM_IdentifiedObject.name
mvmMaxQueryURI	500
mvmMaxSparqlEntry	4000

4. Clique em **Publicar**. As propriedades novas e as modificadas serão salvas.
5. Reinicie o serviços de modelo semântico utilizando o Ferramenta de Controle de Plataforma.
6. Em um navegador da web, acesse http://management_host:82/iic/console, onde *management_host* é o nome completo do host do Servidor de Gerenciamento.
7. Faça qualquer solução ou alterações específicas do aplicativo como necessário. Se alterações são necessárias, as alterações serão identificadas na documentação do produto ou da solução.

Configurando o Ferramenta de Controle de Plataforma

Depois de instalar o IBM Intelligent Operations Center, se foi instalado um Java JRE diferente daquele fornecido com o IBM Intelligent Operations Center, é preciso definir o local do JRE utilizado pelo Ferramenta de Controle de Plataforma.

Procedimento

1. No Servidor de Gerenciamento, edite o arquivo `/opt/IBM/ISP/mgmt/scripts/CommandEngine.sh`.
2. Altere o `export JAVA_HOME=` para o local do Java JRE.
3. Salve as mudanças.
4. No Servidor de Gerenciamento, edite o arquivo `/opt/IBM/ISP/mgmt/scripts/UpdateProperty.sh`.
5. Altere o `export JAVA_HOME=` para o local do Java JRE.
6. Salve as mudanças.

Tarefas relacionadas:

“Instalando O Java Runtime Environment” na página 24

O ambiente de tempo de execução do Java 6 deve ser instalado no servidor de instalação antes da instalação do IBM Intelligent Operations Center.

Criptografando a Senha Administrativa do Tivoli Service Request Manager

Utilize o procedimento a seguir para criptografar a senha administrativa do Tivoli Service Request Manager no Tivoli Netcool/Impact.

Procedimento

1. Efetue logon no console administrativo do Tivoli Netcool/Impact em `http://event_host:9080/nci/main` em que `event_host` é o nome do host do . Efetue logon como o usuário `admin` com a senha `netcool`.
2. Clique em **Projeto IOC**.
3. Na seção Políticas, clique duas vezes na política **IOC_Sample_Password_Encoder**. A política é aberta na janela Editor de Política.
4. No campo **Insira a Senha Aqui**, insira a senha para `Maxadmin`. A senha `Maxadmin` é a senha do usuário administrativo inserida durante a instalação.
5. Para salvar a política, clique em **Salvar**.
6. Clique no ícone **Política do Acionador**.
7. Clique em **Executar**.
8. Na seção Status de Serviço, role para **PolicyLogger**, clique em **Visualizar log para PolicyLogger** (ícone com a seta para baixo).
9. Na janela do criador de logs de política, localize a instrução que é similar à seguinte instrução:
`11 May 2012 14:19:12,260: [IOC_Sample_Password_Encoder][pool-1-thread-46]Parser log: {aes}FF877B74ADF4DF1C2002F94ACB38FAFF`
10. Copie a senha criptografada **Maxadmin** a partir da instrução, por exemplo:
`{aes}FF877B74ADF4DF1C2002F94ACB38FAFF`
11. No console administrativo do Tivoli Netcool/Impact, na seção Políticas, clique duas vezes na política **UTILS_LIBRARY_IOC_TSRM**. A política é aberta na janela Editor de Política.
12. Substitua o valor do `MAXAdminPassword` pelo valor criptografado copiado na Etapa 10:
`MAXAdminPassword = "{aes}FF877B74ADF4DF1C2002F94ACB38FAFF";`
13. Para salvar a política, clique em **Salvar**.
14. Clique em **Projeto IOC**.
15. Na seção Políticas, clique duas vezes na política **IOC_Sample_Password_Encoder**. A política é aberta na janela Editor de Política.
16. No campo **Insira Senha Aqui**, exclua a senha para `Maxadmin`.
17. Para salvar a política, clique em **Salvar**.

Configurando o Número Mínimo de Encadeamentos para o EventProcessor

O número mínimo de encadeamentos para o `EventProcessor` precisa ser configurado para 25 por motivos de desempenho.

Procedimento

1. Efetue logon no console administrativo do Tivoli Netcool/Impact em `http://event_host:9080/nci/main` em que `event_host` é o nome do host do .
2. Clique em **Status do Serviço > EventProcessor**.
3. Especifique 25 para **Número Mínimo de Encadeamentos**.

Nota: O valor **Número Mínimo de Encadeamentos** não pode ser maior que o valor para **Número Máximo de Encadeamentos**.

4. Clique em **OK**.
5. Clique no ícone de parar processo para parar o `EventProcessor`.
6. Clique no ícone de iniciar processo para iniciar o `EventProcessor`.

Mudando o Tamanho do Conjunto de Encadeamentos Padrão e do Contêiner da Web

As configurações de tamanho do conjunto de encadeamentos Padrão e Contêiner da web precisam ser mudadas para melhorar o desempenho de procedimentos padrão de operação.

Procedimento

1. No na Interface de Administração do WebSphere Portal, clique em **Operações Inteligentes > Ferramentas de Administração > Consoles de Administração**.
2. Sob o Servidor de Eventos, clique em **Servidor de Aplicativos de Procedimento Padrão de Operação**.
3. Efetue logon como o administrador do WebSphere Application Server. O ID do usuário foi definido na propriedade WAS.ADMIN.ACCOUNT e a senha foi definida na propriedade WAS.ADMIN.ACCOUNT.PWD no arquivo Propriedades da Topologia quando o IBM Intelligent Operations Center foi instalado.
4. Clique em **Servidores > Servidores de aplicativos > MXServer1 > Conjuntos de Encadeamentos > WebContainer**.
5. Insira 50 para **Tamanho Mínimo**.
6. Insira 50 para **Tamanho Máximo**.
7. Clique em **OK**.
8. Clique em **Servidores > Servidores de aplicativos > MXServer1 > Conjuntos de Encadeamentos > Padrão**.
9. Insira 20 para **Tamanho Mínimo**.
10. Insira 50 para **Tamanho Máximo**.
11. Clique em **OK**.
12. Reinicie o TSRMCluster.
 - a. Clique em **Servidores > Clusters**.
 - b. Selecione TSRMCluster.
 - c. Clique em **Parar**.
 - d. Aguarde o status mudar para vermelho.
 - e. Clique em **Iniciar**.

Instalando e Executando o Cyber Hygiene Passo a Passo

O Cyber Hygiene é instalado e executado separadamente do IBM Intelligent Operations Center e deve ser instalado e executado após todos os outros componentes do IBM Intelligent Operations Center estarem instalados, configurados e operacionais. O Cyber Hygiene muda a configuração padrão do sistema operacional para um conjunto mais seguro de opções que ajudam a assegurar uma base mais segura para o sistema IBM Intelligent Operations Center.

Antes de Iniciar

Nota: O Cyber Hygiene é instalado e executado na mesma etapa. Se estiver instalando o IBM Intelligent Operations Center usando o IBM Installation Manager, não use essas etapas. A instalação do IBM Installation Manager fornece uma opção para instalar e executar o Cyber Hygiene.

Para reduzir o tempo que o Cyber Hygiene leva para executar varreduras e correções, desmonte qualquer sistema de arquivos que não necessitam de avaliação para segurança. Por exemplo, os diretórios *install_media* em cada servidor podem ser excluídos após concluir todas as etapas de instalação. Esses diretórios podem ser excluídos ou desmontados antes da execução do Cyber Hygiene.

No servidor de instalação, acesse o diretório no qual o pacote de instalação do IBM Intelligent Operations Center foi copiado. Nestas etapas, este diretório é referido como *install_home*.

Sobre Esta Tarefa

O Cyber Hygiene deve ser a última etapa após a instalação do IBM Intelligent Operations Center. A varredura e as correções lidam com exposições de segurança da configuração que existem após a instalação do sistema operacional padrão e do produto IBM Intelligent Operations Center. As correções aplicadas foram testadas para confirmar que os serviços do IBM Intelligent Operations Center irão operar corretamente.

Mudanças aplicadas ao sistema pelo Cyber Hygiene podem causar problema com outros aplicativos e soluções. Por exemplo, talvez os outros aplicativos e soluções tenham requisitos no ambiente Linux que não estão de acordo com as boas práticas de segurança. Um aplicativo ou solução pode requerer que o logon do sistema seja efetuado como usuário raiz para ser instalado ou executado. Nesses casos, algumas das mudanças do Cyber Hygiene podem precisar ser temporariamente ou permanentemente mudadas ou outra solução encontrada com o fornecedor do aplicativo ou solução.

Depois que as mudanças do Cyber Hygiene são feitas, não há nenhum método automatizado para alterá-las. Todas as mudanças devem ser feitas por atualizações manuais para o sistema operacional Linux ou alterando as permissões do arquivo ou do diretório.

Procedimento

1. No servidor de instalação, abra uma janela do terminal e efetue logon como raiz. Se não tiver efetuado logon como raiz, alterne para a conta raiz executando o comando **su -**.
2. Execute o comando **export JAVA_HOME=/opt/ibm/java-x86_64-60/jre**. A variável JAVA_HOME é configurada para o Java runtime environment (JRE).
3. Vá para o diretório *install_home/ch/install*.
4. Edite o arquivo *iop-ch-install.xml* usando um editor de texto.
5. Substitua os parâmetros no arquivo *iop-ch-install.xml* com os valores apropriados para a sua instalação.

Tabela 22. Parâmetros de Instalação do Cyber Hygiene

Parâmetro	Valor
<code>\${APP.1.HOST}</code>	O host do servidor de aplicativos
<code>\${APP.1.ACCT}</code>	O nome de usuário do Linux para acesso SSH ao servidor de aplicativos
<code>\${APP.1.ACCT.PWD}</code>	A senha para o <code>\${APP.1.ACCT}</code>
<code>\${APP.1.SSH_PORT}</code>	A porta SSH do servidor de aplicativos
<code>\${DB.1.HOST}</code>	O nome completo do host do servidor de dados
<code>\${DB.1.ACCT}</code>	O nome de usuário do Linux para acesso SSH ao servidor de dados
<code>\${DB.1.ACCT.PWD}</code>	A senha para <code>\${DB.1.ACCT}</code>
<code>\${DB.1.SSH_PORT}</code>	A porta SSH do servidor de dados
<code>\${EVENT.1.HOST}</code>	O nome completo do host do
<code>\${EVENT.1.ACCT}</code>	O nome de usuário do Linux para acesso SSH ao
<code>\${EVENT.1.ACCT.PWD}</code>	A senha para o <code>\${EVENT.1.ACCT}</code>
<code>\${EVENT.1.SSH_PORT}</code>	A porta SSH do
<code>\${MGMT.1.HOST}</code>	O nome completo do host do Servidor de Gerenciamento
<code>\${MGMT.1.ACCT}</code>	O nome de usuário do Linux para acesso SSH ao Servidor de Gerenciamento
<code>\${MGMT.1.ACCT.PWD}</code>	A senha para <code>\${MGMT.1.ACCT}</code>

Tabela 22. Parâmetros de Instalação do Cyber Hygiene (continuação)

Parâmetro	Valor
<code> \${MGMT.1.SSH_PORT}</code>	A porta SSH do Servidor de Gerenciamento

6. Salve o arquivo.
7. Vá para o diretório `install_home/ch`.
8. Execute o comando `install_home/ch/install/iop-ch-install.sh -r iop-ch-install-messages.properties -f 'com.ibm.iop.cyber.hygiene.scripts.lite_1.5.0.zip' -d install_media/ioc/image -p GRUB_password`, em que `GRUB_password` é a senha para o carregador de inicialização do GRUB nos servidores. A `GRUB_password` será aplicada a todos os servidores de destino. Normalmente, quando os servidores são reiniciados, nenhuma senha é necessária. No entanto, uma vez que o Cyber Hygiene esteja instalado, se um servidor for iniciado com uma opção do Linux, como iniciar em modo de usuário único, a `GRUB_password` terá de ser inserida no console do servidor.

Resultados

O tempo do processamento é determinado pela velocidade do hardware e se arquivos extras e desnecessários estão nos servidores de destino. O processamento pode ser executado em até 1,5 horas. Durante esse tempo os servidores de destino serão verificados e as correções adequadas serão aplicadas.

O que Fazer Depois

Verifique o log do Cyber Hygiene para quaisquer erros. Os logs também mostrarão as correções aplicadas e as etapas manuais opcionais.

Conceitos relacionados:

“Visão Geral do Cyber Hygiene” na página 80

O recurso Cyber Hygiene do IBM Intelligent Operations Center é designado para fornecer serviços que corrigem exposições de segurança potenciais no sistema instalado.

Mudanças no Sistema Operacional Linux

O Cyber Hygiene varre o sistema operacional Linux para exposições de segurança bem conhecidas e faz as mudanças apropriadas. Os logs descrevem as exposições varridas e as mudanças feitas nas políticas e configurações do sistema operacional Linux.

Os logs também listam exposições que foram detectadas, mas nas quais nenhuma mudança foi feita. Eles podem incluir:

- O sistema já está configurado da maneira como o Cyber Hygiene o alterou.
- A mudança requer que um administrador do sistema tome uma ação ou decida se a mudança é adequada para o ambiente.
- A mudança não pode ser feita por um script automatizado. Por exemplo, a exposição relacionada às políticas de segurança gerais da organização.

Qualquer correção aplicada pelo Cyber Hygiene pode ser mudada posteriormente, se necessário. Os logs do Cyber Hygiene fornecem informações sobre as mudanças que se aplicam ao sistema. Mudanças podem ser necessárias para usar o sistema com outros aplicativos ou soluções se as mudanças feitas pelo Cyber Hygiene forem incompatíveis com esses sistemas.

Revisando o Log do Cyber Hygiene

Após o Cyber Hygiene estar instalado e em execução, revise o log para entender as mudanças que foram feitas no sistema e quaisquer exposições restantes.

Sobre Esta Tarefa

No servidor de instalação, acesse o diretório no qual o pacote de instalação do IBM Intelligent Operations Center foi copiado. Nestas etapas, este diretório é referido como *install_home*.

Procedimento

1. Revise o log do Cyber Hygiene no diretório `/var/ibm/InstallationManager/logs/native` no servidor de instalação quanto à totalidade para garantir que todas as ações foram executadas em todos os servidores. O log pode ser localizado por meio da execução do comando **fgrep yber *.log**. O arquivo de log mostrará as informações para cada servidor. Em geral, as etapas com informações de log incluem:
 - Preparando o ambiente para executar as tarefas do Cyber Hygiene.
 - Executar o corretor independente. Isso corrige exposições que não requerem varredura. Por exemplo, configurar uma senha de carregador de GRUB e ativar auditoria.
 - Desativar o logon de raiz remota.
 - Varreduras de exposições. Elas são executadas no plano de fundo e as tarefas principais esperam a conclusão da varredura.
 - Varredura da exposição para tratar de exposições localizadas durante a varredura.
 - Varrer após a correção. Isso identifica exposições não localizadas durante a varredura inicial.
 - Varredura do corretor para tratar de exposições adicionais localizadas durante a segunda varredura. As correções não concluídas serão registradas.
2. Revise os logs detalhados do Cyber Hygiene localizados no diretório `/var/BA15/CH/results` em cada um dos servidores de destino. O `standrem-date_time.log` mostra os resultados do corretor independente. O `standrem-disableRemoteRoot-date_time.log` mostra os resultados da desativação do logon de raiz remota. O `scanrem-combined-log-date_time.log` mostra os resultados das ações do corretor verificadas. Existem dois logs para as etapas de varredura/correção.
 - a. Revise os arquivos de log para linhas que começam com o texto Vulnerabilidade. Cada linha indica a ação tomada e inclui:
 - As provas da varredura.
 - As correções selecionadas.
 - Os detalhes sobre as correções aplicadas.
 - b. No log para a segunda varredura e correção, talvez as correções observadas com o texto NÃO EXECUTADA precisem ser investigadas para outras ações manuais.

Reativando Logon de Raiz Remoto

O Cyber Hygiene desativa o logon remoto para a conta raiz por meio do comando **ssh**. Os comandos **telnet** e **rsh** serão totalmente desativados no sistema operacional Linux. Se necessário, o logon remoto poderá ser reativado.

Sobre Esta Tarefa

A reativação do logon remoto para o usuário raiz talvez não seja necessária. Um usuário com privilégios adequados pode utilizar os comandos **su** e **sudo** para operar como o usuário raiz. Usuários privilegiados que operam como o usuário raiz são registrados para fins de auditoria.

O IBM Intelligent Operations Center define o usuário `ibmadmin` no grupo `wheel`. Os usuários do grupo `wheel` podem utilizar o comando **sudo su -** para ser executado como raiz.

Procedimento

Execute o seguinte para ativar o logon de raiz utilizando o comando **ssh**.

1. Edite o arquivo `/etc/ssh/sshd_config` no servidor no qual login remoto como raiz usando SSH ou um terminal remoto é necessário.
2. Altere o parâmetro `PermitRootLogin` para `sim` e salve o arquivo. Altere este parâmetro para `não`, se o login remoto que utiliza o comando `ssh` precisar ser desativado.
3. Salve o arquivo.
4. Reinicie o serviço `ssh` executando o comando **`service sshd restart`**.

O logon remoto na conta raiz usando terminais remotos é desativado pelo Cyber Hygiene. Somente a tela e o teclado conectados fisicamente ao servidor poderão efetuar o logon como usuário raiz. Execute o seguinte para reativar o logon de raiz remoto para um servidor a partir de um terminal remoto.

5. Edite o arquivo `/etc/securetty` no servidor no qual logon remoto como raiz usando SSH ou um terminal remoto é necessário.
6. Inclua os nomes de dispositivos Linux aos terminais autorizados para efetuar logon remotamente como usuário raiz. Por exemplo, se desejar incluir `tty1`, altere a lista para ler:

```
console
tty1
```

Para desativar um terminal, coloque um caractere `#` antes que o terminal seja desativado. Por exemplo:

```
console
#tty1
```

7. Salve o arquivo.

Configurando Usuários que Requerem Acesso ssh

O IBM Intelligent Operations Center requer que alguns usuários sejam configurados com acesso e senhas ssh.

Sobre Esta Tarefa

Os seguintes usuários devem ser configurados no servidor de instalação e em todos os servidores de destino para terem acesso e senhas ssh.

- `ibmadmin`
- `ibmuser`
- `mqconn`

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 WebSphere Business Monitor Development Toolkit

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

Conceitos relacionados:

“Criando e Integrando KPIs” na página 109

Modelos de principais indicadores de desempenho (KPI) podem, ser criados e modificados usando um kit de ferramentas de desenvolvimento de monitoramento de negócios e um portlet de gerenciamento de KPI.

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

Excluindo Usuários de Amostra

O IBM Intelligent Operations Center é fornecido com usuários de amostra. Por motivos de segurança esses usuários devem ser excluídos após a instalação do IBM Intelligent Operations Center em um ambiente de produção.

Sobre Esta Tarefa

Para excluir os usuários pré-definidos, conclua as seguintes etapas:

Procedimento

1. No servidor de aplicativos, faça login no WebSphere Portal.
2. No portal **Administração**, clique em **Acessar > Usuários e Grupos > Todos os Usuários do Portal Autenticados**.
3. Clique no ícone excluir para os seguintes usuários:
 - tdelorne
 - scollins
 - akelly

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

- admin
- iicsystemuser
- maxadmin
- maxintadm
- maxreg
- notesadmin
- resAdmin1

- resDeployer1
- resMonitor1
- rtsAdmin
- rtsConfig
- rtsUser
- taiuser
- SRMSELFSERVICEUSR
- wasadmin
- waswebadmin
- wpsadmin
- wpsbind
- Todos os IDs de usuário que começam com "PM"

Referências relacionadas:

“Usuários de Amostra” na página 69

Durante a implementação do IBM Intelligent Operations Center, são criados usuários de amostra.

Removendo os Serviços de Instalação do Sistema de Produção

Depois de instalar o IBM Intelligent Operations Center, os serviços de instalação podem ser removidos dos servidores do sistema de produção. É sugerido que o servidor de instalação seja mantido, pois alguns de seus serviços podem ser necessários para atividades de manutenção.

Após a conclusão e a verificação da instalação, os componentes que são usados apenas no processo de instalação podem ser removidos dos servidores do sistema de produção (servidor de aplicativos, , Servidor de Gerenciamento, servidor de dados). Elas incluem:

- O diretório definido pela propriedade `Unix.image.basedir.remote` no arquivo de propriedades de topologia.
- O diretório definido pela propriedade `Unix.script.basedir.remote` no arquivo de propriedades de topologia.
- O diretório *install_media*, definido pela propriedade `image.basedir.local` no arquivo de propriedades de topologia.

Nota: O servidor de instalação deve ser mantido se for necessário para uso futuro. Como o arquivo de propriedades de topologia contém senhas em texto não criptografado, esse servidor deve estar em um local seguro.

Tarefas relacionadas:

“Instalando o IBM Intelligent Operations Center Utilizando o Installation Manager” na página 25
 O IBM Intelligent Operations Center pode ser instalado usando o instalador gráfico fornecido.

Capítulo 3. Protegendo a Solução

Segurança é importante dentro do IBM Intelligent Operations Center porque a solução é central para operações essenciais. Para garantir segurança, é importante que você conheça as configurações padrão e que gerencie usuários da solução para fornecer a todos eles o nível correto de acesso.

Senhas Padrão

Sua primeira tarefa na proteção da solução é garantir que todas as senhas padrão sejam mudadas. Para obter informações adicionais sobre as senhas padrão, consulte o link no final do tópico.

Conexão Segura

O IBM Intelligent Operations Center é ativado para HTTPS por padrão. É possível mudar as configurações de HTTPS para os seguintes serviços individuais dentro do IBM Intelligent Operations Center:

- O serviço de monitoramento de negócios que processa os KPIs
- O serviço de administração de procedimento padrão de operação e de recurso

Qualquer mudança na configuração de HTTPS para um serviço individual deve ser realizada por uma atualização da configuração de porta correspondente. Para obter mais detalhes sobre a mudança dessas configurações notabela de propriedades de sistema, consulte o link no final do tópico

Autenticação de Usuário

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 de usuário do IBM Intelligent Operations Center são gerenciadas por meio de usuários e grupos e usuários do WebSphere Portal. O WebSphere Portal usa o banco de dados do Lightweight Directory Access Protocol (LDAP) fornecido pelo Tivoli Directory Server em execução no servidor de dados.

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 e inclua pelo menos o ID, nome e senha do usuário.

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.

Portal

O serviço do portal fornece uma plataforma que pode ser escalada para acomodar o conjunto de usuários requerido. Também fornece acesso baseado em função que pode ser ajustado para refletir a estrutura de organização necessária. 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. Para obter informações adicionais sobre esse portlet, consulte o link no final deste tópico.

Conceitos relacionados:

“Informações sobre Senha” na página 37

Senhas para vários IDs de usuário na solução IBM Intelligent Operations Center são definidas no arquivo de propriedades de topologia. Por motivos de segurança, as senhas padrão enviadas com o IBM Intelligent Operations Center deverão ser alteradas.

Informações relacionadas:

 [Documentação do Produto IBM WebSphere Portal 7](#)

Funções e Acesso do Usuário

O IBM Intelligent Operations Center implementa segurança limitando acesso a recursos baseados em funções de usuários.

Para utilizar um recurso específico do IBM Intelligent Operations Center, um usuário deve ser um membro do grupo de funções de usuário que fornece o acesso necessário para esse recurso. Um usuário torna-se um membro de um grupo de funções de usuários por um administrador. A tabela a seguir mostra como funções reais podem ser mapeadas para os grupos de funções de usuários com níveis de acesso de login no IBM Intelligent Operations Center.

Tabela 23. Funções de tarefa e grupos de funções de usuários do IBM Intelligent Operations Center

Função da Tarefa	Responsabilidades	Grupo de Funções de Usuários
Executivo	<ul style="list-style-type: none">• Define os requisitos e limites de entrada para ocorrências, incidentes e Key Performance Indicators (KPIs)• Visualiza resumos visuais, detalhes e relatórios de alto nível abrangendo:<ul style="list-style-type: none">– KPIs– Ocorrências• Comunica decisões ligadas a políticas, direção a longo prazo e decisões de alto nível	Executivo de Toda a Cidade

Tabela 23. Funções de tarefa e grupos de funções de usuários do IBM Intelligent Operations Center (continuação)

Função da Tarefa	Responsabilidades	Grupo de Funções de Usuários
Gerente ou Supervisor	<ul style="list-style-type: none"> • Gerencia ocorrências e incidentes • Produz e monitora relatórios de KPI • Emite alertas • Analisa ocorrências em busca de mudanças de status ou requisitos de ação • Toma decisões sobre medidas corretivas a curto prazo 	Supervisor de Toda a Cidade
Operador	<ul style="list-style-type: none"> • Monitora informações sobre ocorrências • Monitora alertas • Visualiza detalhes • Emite comunicações • Atualizar dados de ocorrências ou incidentes com mais informações, por exemplo: <ul style="list-style-type: none"> – Relatórios por telefone – Opiniões da equipe de construção ou manutenção 	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.	wpsadmins

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

Tarefas relacionadas:

“Incluindo um Usuário ou Grupo” na página 74

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 70

Um conjunto de permissões para acessar os recursos no IBM Intelligent Operations Center está associado a cada grupo de funções do usuário.

“Grupo de Categorias de Usuários e Permissões de Dados” na página 73

A permissão para acessar uma categoria de dados no IBM Intelligent Operations Center está associada a cada grupo de categorias de usuários.

Usuários de Amostra

Durante a implementação do IBM Intelligent Operations Center, são criados usuários de amostra.

Usuários de amostra genéricos são definidos com grupos de funções de usuários e permissões de acessos correspondentes. Estes usuários de amostra são definidos apenas como exemplos são listados na tabela a seguir. Outros usuários são necessários para a administração da solução.

Tabela 24. Usuários Definidos no IBM Intelligent Operations Center

ID do usuário	Grupo de Funções de Usuários
Usuários de Amostra	
tdelorne	Executivo de Toda a Cidade
scollins	Supervisor de Toda a Cidade

Tabela 24. Usuários Definidos no IBM Intelligent Operations Center (continuação)

ID do usuário	Grupo de Funções de Usuários
akelly	Operador de Toda a Cidade
Usuário Solicitado	
wpsadmin	wpsadmins

Quando estiver pronto para definir usuários para a sua organização, exclua apenas os usuários de amostra. Você não deve excluir o usuário wpsadmin. O usuário wpsadmin é essencial para tarefas de administração associadas com o IBM Intelligent Operations Center. Para obter informações adicionais sobre usuários necessários, consulte o link no final deste tópico.

Importante: Substitua a senha padrão do usuário wpsadmin por uma nova senha. Para obter informações sobre atualização de IDs e senhas do usuário administrador do portal, consulte a documentação WebSphere Portal.

Conceitos relacionados:

“Informações sobre Senha” na página 37

Senhas para vários IDs de usuário na solução IBM Intelligent Operations Center são definidas no arquivo de propriedades de topologia. Por motivos de segurança, as senhas padrão enviadas com o IBM Intelligent Operations Center deverão ser alteradas.

Tarefas relacionadas:

“Excluindo Usuários de Amostra” na página 65

O IBM Intelligent Operations Center é fornecido com usuários de amostra. Por motivos de segurança esses usuários devem ser excluídos após a instalação do IBM Intelligent Operations Center em um ambiente de produção.

Informações relacionadas:



Documentação do Produto IBM WebSphere Portal 7

Grupos de Funções de Usuários e Permissões de Autorização

Um conjunto de permissões para acessar os recursos no IBM Intelligent Operations Center está associado a cada grupo de funções do usuário.

Um administrador designa uma função a um usuário, tornando-o membro do grupo de funções de usuários correspondentes. Cada usuário tem associação designada de um ou mais grupos de funções de usuários.

A tabela a seguir lista as permissões para cada grupo de funções de usuários fornecidos com o IBM Intelligent Operations Center. Para cada grupo de funções do usuário, é concedida uma permissão de autorização para cada recurso no IBM Intelligent Operations Center.

Tabela 25. Recursos e Permissões do Grupo de Funções de Usuários Associados do IBM Intelligent Operations Center

Tipo de recurso	Nome do recurso	Executivo de Toda a Cidade	Supervisor de Toda a Cidade	Operador de Toda a Cidade	wpsadmins

Tabela 25. Recursos e Permissões do Grupo de Funções de Usuários Associados do IBM Intelligent Operations Center (continuação)

Página	Supervisor: Status	Permissão de Usuário	Permissão de Usuário	Nenhuma	Permissão de Administrador
	Supervisor: Operações	Permissão de Usuário	Nenhuma	Nenhuma	Permissão de Administrador
	Supervisor: Relatórios	Nenhuma	Permissão de Usuário	Nenhuma	Permissão de Administrador
	Operador: Operações	Nenhuma	Nenhuma	Permissão de Usuário	Permissão de Administrador
	Operador: Relatórios	Nenhuma	Nenhuma	Permissão de Usuário	Permissão de Administrador
	Mapa de Localização	Nenhuma	Permissão de Usuário	Permissão de Usuário	Permissão de Administrador
	Administração	Nenhuma	Nenhuma	Nenhuma	Permissão de Administrador

Tabela 25. Recursos e Permissões do Grupo de Funções de Usuários Associados do IBM Intelligent Operations Center (continuação)

Portlet	Status	Permissão de Usuário	Permissão de Usuário	Nenhuma	Permissão de Administrador
	Drill Down de Key Performance Indicator	Permissão de Usuário	Permissão de Usuário	Nenhuma	Permissão de Administrador
	Notificações	Permissão de Usuário	Permissão de Usuário	Permissão de Usuário	Permissão de Administrador
	Contatos	Permissão de Usuário	Permissão de Usuário	Permissão de Usuário	Permissão de Administrador
	Mapa	Permissão de Usuário	Nenhuma	Permissão de Usuário	Permissão de Administrador
	Detalhes	Permissão de Usuário	Nenhuma	Permissão de Usuário	Permissão de Administrador
	Mínhas Atividades	Permissão de Usuário	Permissão de Usuário	Permissão de Usuário	Permissão de Administrador
	Mapa de Localização	Nenhuma	Permissão de Usuário	Permissão de Usuário	Permissão de Administrador
	Relatórios	Nenhuma	Permissão de Usuário	Permissão de Usuário	Permissão de Administrador
	Intelligent Operations Center - Sobre	Nenhuma	Nenhuma	Nenhuma	Permissão de Administrador
	Consoles de Administração	Nenhuma	Nenhuma	Nenhuma	Permissão de Administrador
	Verificação do Sistema	Nenhuma	Nenhuma	Nenhuma	Permissão de Administrador
	Resumo de Permissões do Usuário	Nenhuma	Nenhuma	Nenhuma	Permissão de Administrador
	Principais Indicadores de Desempenho	Nenhuma	Nenhuma	Nenhuma	Permissão de Administrador
	Gerenciador de Mapa de Localização	Nenhuma	Nenhuma	Nenhuma	Permissão de Administrador
	Procedimentos Padrão de Operação	Nenhuma	Nenhuma	Nenhuma	Permissão de Administrador
	Script do Evento	Nenhuma	Nenhuma	Nenhuma	Permissão de Administrador
	Publicador de Amostra	Nenhuma	Nenhuma	Nenhuma	Permissão de Administrador
	Usuário e Grupos	Nenhuma	Nenhuma	Nenhuma	Permissão de Administrador

As permissões de autorização do IBM Intelligent Operations Center são designadas com base em grupos do Lightweight Directory Access Protocol (LDAP). As permissões são definidas da seguinte forma:

- A permissão do usuário é a autoridade concedida a um usuário para fornecer acesso para visualizar e trabalhar com recursos.

- A permissão do administrador é a autoridade concedida a um administrador para fornecer acesso a:
 - Configurar recursos
 - Criar, modificar ou excluir usuários e grupos de usuários

Para acessar dados no IBM Intelligent Operations Center, um usuário deve ser um membro do grupo de categorias do usuário que fornece permissões para os dados necessários.

Conceitos relacionados:

“Resumo de Permissões do Usuário” na página 79

Use o portlet Resumo de Permissões do Usuário para visualizar as permissões associadas aos usuários e grupos do IBM Intelligent Operations Center.

“Funções e Acesso do Usuário” na página 68

O IBM Intelligent Operations Center implementa segurança limitando acesso a recursos baseados em funções de usuários.

Tarefas relacionadas:

“Incluindo um Usuário ou Grupo” na página 74

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 76

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

Referências relacionadas:

“Grupo de Categorias de Usuários e Permissões de Dados”

A permissão para acessar uma categoria de dados no IBM Intelligent Operations Center está associada a cada grupo de categorias de usuários.

Informações relacionadas:

 [Documentação do Produto IBM WebSphere Portal 7](#)

Grupo de Categorias de Usuários e Permissões de Dados

A permissão para acessar uma categoria de dados no IBM Intelligent Operations Center está associada a cada grupo de categorias de usuários.

Um administrador designa acesso a dados para um usuário, tornando-o membro do grupo de categorias de usuários apropriados. Cada usuário tem associação designada de um ou mais grupos de categorias de usuários.

A tabela a seguir lista as categorias de dados abrangidos pelo IBM Intelligent Operations Center e os grupos de categorias de usuários correspondentes utilizados para identificar eventos, Principais Indicadores de Desempenho(KPIs) e dados de alerta. Por exemplo, se um usuário deseja ser capaz de consultar eventos relacionados ao departamento de água da cidade, o usuário deverá ser um membro do grupo `ioc_base_infrastructure`.

Tabela 26. Descrições e Identificadores do Grupo de Categorias de Usuários

Categoria de Dados	Descrição	Grupo de categorias de usuários
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> , <code>ioc_base_explosive</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>

Tabela 26. Descrições e Identificadores do Grupo de Categorias de Usuários (continuação)

Categoria de Dados	Descrição	Grupo de categorias de usuários
Saúde	Medicina e saúde pública	ioc_base_health
Infra	Infraestrutura: Utilidade pública, telecomunicações, outra infraestrutura que não seja de transporte	ioc_base_infrastructure
Met	Meteorologia (incluindo enchentes)	ioc_base_meteorological
Resgate	Resgate e recuperação	ioc_base_rescue
Proteção	Emergência geral e segurança pública	ioc_base_safety
Segurança	Cumprimento da lei, segurança local/privada, da pátria e militar	ioc_base_security
Transporte	Transporte público e privado	ioc_base_transportation
Outro	Outras ocorrências, KPIs ou alertas	ioc_base_other

Para efetuar login e acessar recursos do IBM Intelligent Operations Center, um usuário deve ser membro do grupo de funções de usuários que fornece as permissões para autorizações necessárias.

Conceitos relacionados:

“Resumo de Permissões do Usuário” na página 79

Use o portlet Resumo de Permissões do Usuário para visualizar as permissões associadas aos usuários e grupos do IBM Intelligent Operations Center.

“Funções e Acesso do Usuário” na página 68

O IBM Intelligent Operations Center implementa segurança limitando acesso a recursos baseados em funções de usuários.

Tarefas relacionadas:

“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.

“Visualizando ou Modificando a Associação ao Grupo” na página 76

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

Referências relacionadas:

“Grupos de Funções de Usuários e Permissões de Autorização” na página 70

Um conjunto de permissões para acessar os recursos no IBM Intelligent Operations Center está associado a cada grupo de funções do usuário.

Informações relacionadas:

 [Documentação do Produto IBM WebSphere Portal 7](#)

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://app-host/wpsv70/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 permissões de autorização, consulte o link Documentação do Produto IBM WebSphere Portal 7 no final do tópico e procure informações sobre como designar acesso às páginas.
- Atribua o novo usuário a um grupo de segurança e a grupo de pessoas no Tivoli Service Request Manager.

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.

Conceitos relacionados:

“Funções e Acesso do Usuário” na página 68

O IBM Intelligent Operations Center implementa segurança limitando acesso a recursos baseados em funções de usuários.

Tarefas relacionadas:

“Configurando Novos Usuários no Tivoli Service Request Manager” na página 126

Ao incluir um usuários no IBM Intelligent Operations Center, designe permissões e grupos de pessoas para o usuário no Tivoli Service Request Manager.

Referências relacionadas:

“Grupos de Funções de Usuários e Permissões de Autorização” na página 70

Um conjunto de permissões para acessar os recursos no IBM Intelligent Operations Center está associado a cada grupo de funções do usuário.

“Grupo de Categorias de Usuários e Permissões de Dados” na página 73

A permissão para acessar uma categoria de dados no IBM Intelligent Operations Center está associada a cada grupo de categorias de usuários.

Informações relacionadas:

 Documentação do Produto IBM WebSphere Portal 7

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://app-host/wpsv70/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.

Referências relacionadas:

“Grupos de Funções de Usuários e Permissões de Autorização” na página 70

Um conjunto de permissões para acessar os recursos no IBM Intelligent Operations Center está associado a cada grupo de funções do usuário.

“Grupo de Categorias de Usuários e Permissões de Dados” na página 73

A permissão para acessar uma categoria de dados no IBM Intelligent Operations Center está associada a cada grupo de categorias de usuários.

Informações relacionadas:

 [Documentação do Produto IBM WebSphere Portal 7](#)

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://app-host/wpsv70/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 Produto IBM WebSphere Portal 7](#)

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.

Nota: Saiba que excluir um usuário do IBM Intelligent Operations Center também remove seu acesso a outras soluções dentro da família de produtos do IBM Smarter Cities™ Software Solutions. Excluir um grupo também removerá esse grupo de outras soluções.

Procedimento

1. Efetue login em `http://app-host/wpsv70/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 Produto IBM WebSphere Portal 7](#)

Importando Usuários e Grupos

É possível importar usuários em lote para o IBM Intelligent Operations Center por meio do serviço do portal.

Sobre Esta Tarefa

Como um administrador do portal, é possível importar usuários em lote para o IBM Intelligent Operations Center por meio do console de administração do portal. O arquivo XML requerido para essa tarefa pode ser localizado no servidor de aplicativos: `/opt/IBM/WebSphere/PortalServer/doc/xml-samples/CreateUser.xml`. Esse arquivo XML pode ser modificado para incluir usuários no IBM Intelligent Operations Center.

Nota: Ao incluir diversos usuários, inclua todos os usuários primeiro, antes de incluir os usuários nos grupos. Consulte o exemplo no final do tópico.

Como uma alternativa ao procedimento a seguir, é possível executar da linha de comandos o script `xmlaccess.sh` que está localizado no servidor de aplicativos.

Procedimento

1. Atualize o arquivo `CreateUser.xml` para conter novos usuários e os grupos aos quais eles pertencem.
2. Efetue login em `http://app-host/wpsv70/wps/myportal/` como um usuário administrativo.
3. Clique em **Administração**.
4. Em **Configurações do Portal**, clique em **Importar XML**.
5. Navegue para localizar o seu arquivo XML atualizado.
6. Clique em **Importar**.

Resultados

O WebSphere Portal Server automaticamente cria as entradas associadas no diretório no Tivoli Directory Server e no Tivoli Access Manager WebSEAL.

Exemplo

O exemplo a seguir modifica o arquivo XML para incluir dois usuários no IBM Intelligent Operations Center e para incluir cada um deles em um grupo de funções e um grupo de categorias:

```
<?xml version="1.0" encoding="UTF-8"?>
<request xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="PortalConfig_7.0.0.xsd" type="update"
create-oids="true">
<portal action="locate">
<user action="update" name="cityuser003" firstname="City"
lastname="user003" password="passw0rd">
<parameter name="preferredLanguage" type="string"
update="set">en_US</parameter>
<parameter name="cn" type="string" update="set">City user003</parameter>
</user>
<user action="update" name="cityuser004" firstname="City"
lastname="user003" password="passw0rd">
<parameter name="preferredLanguage" type="string"
update="set">en_US</parameter>
<parameter name="cn" type="string" update="set">City user004</parameter>
</user>
<group action="update" name="City Executive">
<member-user update="set" id="cityuser003">
</group>
<group action="update" name="ioc_base_fire">
<member-user update="set" id="cityuser003">
<group action="update" name="City Executive">
<member-user update="set" id="cityuser004">
</group>
<group action="update" name="ioc_base_fire">
<member-user update="set" id="cityuser004">
</group>
</portal>
</request>
```

Conceitos relacionados:

“Consoles de Administração” na página 203

Utilize o portlet do Consoles de Administração para administrar os serviços fornecidos pela solução.

Informações relacionadas:

 [Documentação do Produto IBM WebSphere Portal 7](#)

 [Centro de Informações do Tivoli Directory Server](#)

 [Centro de Informações do Tivoli Access Manager](#)

Resumo de Permissões do Usuário

Use o portlet Resumo de Permissões do Usuário para visualizar as permissões associadas aos usuários e grupos do IBM Intelligent Operations Center.

O portlet Resumo de Permissões do Usuário exibe detalhes de uma associação ao grupo e permissões concedidas a usuários.

Para acessar o portlet Resumo de Permissões do Usuário, na interface de administração do WebSphere Portal, clique em **Intelligent Operations > Ferramentas de Administração > Resumo de Permissões do Usuário**.

Use a guia **Usuário** para verificar permissões para um usuário. Insira o ID do usuário para visualizar as seguintes informações:

- Uma lista completa de todas as categorias de dados e grupos de categorias do usuário disponíveis no IBM Intelligent Operations Center.
- Uma lista das permissões de categorias de dados designadas ao usuário especificado.
- Uma lista de todos os grupos, grupos de função do usuário e grupos de categorias do usuário, dos quais o usuário especificado é membro.
- Uma lista de cada categoria de dados indica se o usuário especificado tem permissão para essa categoria.

Use a guia **Resumo** para verificar estatísticas de resumo para permissões de usuários e grupos. É possível visualizar as seguintes informações:

- Número total de grupos no IBM Intelligent Operations Center.
- Número total de usuários autorizados a acessar o IBM Intelligent Operations Center.
- Uma lista do número total de usuários por categoria de dados.
- Uma lista do número total de usuários por grupo de função de usuário.

Referências relacionadas:

“Grupos de Funções de Usuários e Permissões de Autorização” na página 70

Um conjunto de permissões para acessar os recursos no IBM Intelligent Operations Center está associado a cada grupo de funções do usuário.

“Grupo de Categorias de Usuários e Permissões de Dados” na página 73

A permissão para acessar uma categoria de dados no IBM Intelligent Operations Center está associada a cada grupo de categorias de usuários.

Visão Geral do Cyber Hygiene

O recurso Cyber Hygiene do IBM Intelligent Operations Center é designado para fornecer serviços que corrigem exposições de segurança potenciais no sistema instalado.

Nota: Comumente, o termo "vulnerabilidade" é usado para se referir a ambos, vulnerabilidades de segurança e exposições do sistemas. O Cyber Hygiene define uma vulnerabilidade como um erro de programação em um aplicativo que possibilita violações de segurança. O Cyber Hygiene define uma exposição como um seleção de configuração de aplicativo ou sistema operacional que é menos segura. Exposições podem ser tratadas por meio da escolha de uma opção de configuração mais segura. Por exemplo, um diretório pode ser configurado para permitir que todos os usuários armazenem arquivos lá. Ele também pode ser configurado com mais segurança para que somente o proprietário possa armazenar arquivos no diretório.

O Cyber Hygiene tem dois elementos-chave:

- Mitigação e correção de exposições de segurança conhecidas no sistema operacional Linux e seus usuários, diretórios e arquivos associados. Isso é executado por meio de um conjunto de ferramentas e scripts.
- Documentação da avaliação de quase 1000 vulnerabilidades e exposições conhecidas no sistema operacional, produtos e configuração do sistema.

Ao manipular exposições de segurança durante o processo de instalação, menos trabalho é requerido do cliente para atingir um nível de segurança aumentado no sistema implementado.

Por exemplo, uma agência do governo pode usar a correção e documentação do Cyber Hygiene para ajudar a dar suporte à certificação e credenciamento do sistema para implementação em uma rede segura. Clientes de negócios comerciais podem utilizar o mesmo processo para melhorar a segurança do seu ambiente.

A segurança do Cyber fornece a mitigação de risco, e não a prevenção do risco. Como os sistemas devem ser executados e serem acessíveis para fornecer valor, há sempre um risco de que as informações de um sistema ou seu controle sejam comprometidas.

O Cyber Hygiene não trata de vulnerabilidades específicas do aplicativo, que incluem a forma como ameaças do tipo Negação de Serviço, injeção SQL, e assim por diante, são manipuladas pelo aplicativo. Em vez disso, o Cyber Hygiene fornece uma base para a segurança do aplicativo ao lidar com exposições de usuário, diretório e arquivo de um modo geral; não destinado a nenhum aplicativo específico. O Cyber Hygiene é executado após a instalação do produto para corrigir essas vulnerabilidades gerais para usuários, diretórios e arquivos de aplicativo e sistema. Qualquer aplicativo usado com o sistema operacional Linux deve ser avaliado separadamente para vulnerabilidades específicas do aplicativo.

O catálogo de vulnerabilidades e exposições conhecidas usado no Cyber Hygiene se baseia em listas de verificação não classificadas e não confidenciais da United States Defense Information Services Agency (DISA). Os itens dessas listas são avaliados para aplicabilidade ao Cyber Hygiene. Scripts de varredura procuram e registram instâncias de uma exposição e depois, onde aplicável, os arquivos de log são usados como entrada para scripts de correção que tratam do problema. Um pequeno subconjunto de descobertas de segurança requer uma manipulação diferente.

Vulnerabilidades conhecidas na lista de documentação nos componentes do IBM Intelligent Operations Center, e as ações tomadas pelo Cyber Hygiene para mitigá-las, são fornecidas pelo IBM Intelligent Operations Center.

Tarefas relacionadas:

“Lista de Verificação - Instalação Usando o IBM Installation Manager” na página 14

Utilize esta lista de verificação para controlar as etapas de instalação, ao instalar o IBM Intelligent Operations Center utilizando o IBM Installation Manager.

“Lista de Verificação - Instalação Passo-a-Passo” na página 15

Utilize esta lista de verificação para controlar as etapas de instalação ao instalar o IBM Intelligent Operations Center, utilizando scripts e comandos.

“Instalando o IBM Intelligent Operations Center Utilizando o Installation Manager” na página 25

O IBM Intelligent Operations Center pode ser instalado usando o instalador gráfico fornecido.

“Instalando e Executando o Cyber Hygiene Passo a Passo” na página 60

O Cyber Hygiene é instalado e executado separadamente do IBM Intelligent Operations Center e deve ser instalado e executado após todos os outros componentes do IBM Intelligent Operations Center estarem instalados, configurados e operacionais. O Cyber Hygiene muda a configuração padrão do sistema operacional para um conjunto mais seguro de opções que ajudam a assegurar uma base mais segura para o sistema IBM Intelligent Operations Center.

Segurança Cibernética

A proteção do ambiente de TI tem sido por muito tempo uma preocupação para governos nacionais e está se tornando cada vez mais importante para sistemas de infraestrutura crítica. Os produtos e soluções que fornecem infraestrutura crítica, tais como o IBM Intelligent Operations Center, devem, quando possível, ter as vulnerabilidades conhecidas removidas antes de esses produtos e soluções se tornarem disponíveis.

A segurança cibernética é uma mitigação de risco, não uma prevenção de risco. Como os sistemas de TI devem estar em execução e acessíveis para fornecer valor, sempre há algum risco de que as informações ou o controle de um sistema sejam comprometidos. A segurança cibernética consiste em elementos estáticos e dinâmicos. O Cyber hygiene no IBM Intelligent Operations Center aborda os elementos estáticos de segurança cibernética. Outras ferramentas e processos são necessários para abordar os elementos dinâmicos para segurança cibernética. Essas ferramentas e processos podem incluir procedimentos de segurança física e de equipe ou um conjunto de ferramentas de intrusão de rede.

Os recursos cyber hygiene fornecidos pelo IBM Intelligent Operations Center foram projetados para abordar áreas, como configurações de segurança fracas, erros de software, erros de administração do sistema e erros de processo de segurança do sistema. Para fornecer esse suporte, o cyber hygiene fornece recursos de instalação e configuração que configuram o sistema operacional e recursos de administração que definem configurações seguras e instalam fix packs relacionados à segurança de chave. Por exemplo, os sistemas são configurados para que não existam IDs do usuário sem uma senha e serviços Linux não seguros, como ftp, snmp, rlogin, são desativados. No entanto, os sistemas não podem ser configurados automaticamente para atender a práticas de segurança corporativa específicas.

Listas de Verificação do Cyber Hygiene

O Cyber hygiene usa listas de verificação baseadas em listas de verificação irrestritas do Defense Information Systems Agency (DISA) e em alertas de vulnerabilidade periódicos.

Análise de Itens da Lista de Verificação

Cada vulnerabilidade identificada na lista de verificação do Defense Information System Agency (DISA) define dados relacionados à vulnerabilidade.

As informações fornecidas para cada vulnerabilidade incluem o seguinte:

- Um identificador exclusivo. O identificador é composto de um ID do Security Implementation Technical Guide (STIG) e de uma chave de Vulnerability Management System (VMS).
- Um nome abreviado que resume a vulnerabilidade.
- A gravidade da vulnerabilidade. Os níveis de gravidade documentados são:
 - I Gravidade alta
 - II Gravidade média
 - III Gravidade baixa
- O produto ou produtos afetados.
- A versão ou versões do produto afetado.
- Uma descrição da vulnerabilidade, incluindo quaisquer casos de uso, contexto ou interações com outro software.
- As ações recomendadas. Se a correção não estiver disponível por meio de uma correção ou um upgrade, poderá ser incluída uma mitigação recomendada.
- Qualquer alerta que o alerta substitui.

Para cada vulnerabilidade, é importante entender se ela afeta ou não o IBM Intelligent Operations Center. Por exemplo:

- A liberação e o nível de correção do produto estão incluídos no IBM Intelligent Operations Center afetado? Uma liberação ou correção anterior do produto pode não ser afetada porque o problema pode ter sido introduzido em uma liberação ou correção posterior.
- O produto incluído com o IBM Intelligent Operations Center que está sendo usado expõe a vulnerabilidade de alguma maneira? Por exemplo, pode existir um problema apenas quando o produto está usando serviços de outro produto. Se esses serviços não forem usados na configuração do IBM Intelligent Operations Center, a correção pode não ser necessária.
- A vulnerabilidade do produto afeta o sistema operacional que está sendo usado? Algumas vulnerabilidades podem existir apenas durante a execução de sistemas operacionais específicos.

Para cada item em uma lista de verificação, esses fatores foram analisados para determinar a ação necessária para o IBM Intelligent Operations Center. Essa análise e correção resultam em uma de quatro avaliações:

Não Aplicável (NA)

O produto ou configuração afetada não faz parte do ambiente do IBM Intelligent Operations Center.

Não É uma Descoberta (NF)

O nível de versão e correção instalado do produto não é afetado, ou o produto não é usado de uma maneira que expõe a vulnerabilidade. Essa avaliação também será usada se a configuração não expuser a vulnerabilidade.

Liberado

A vulnerabilidade se aplica ao nível de versão e correção do produto instalado, no entanto, nenhuma correção está disponível para o produto. Essa avaliação também será usada se o sistema estiver configurado de uma maneira que expõe a vulnerabilidade. Por exemplo, aceitar permissões globais em um diretório porque um produto as requer. Essa avaliação também será usada quando a aplicação de uma correção depender de políticas de organização, tais como políticas de senha no comprimento ou combinação de caracteres.

Corrigido

Uma correção de uma vulnerabilidade aberta foi aplicada e verificada.

A Tabela 27 mostra uma análise de exemplo. O segundo exemplo mostra a manipulação de um produto não instalado em nenhum servidor IBM Intelligent Operations Center.

Tabela 27. Avaliações de vulnerabilidade de exemplo

ID	Nome	Severidade	Servidor de aplicativos	Servidor de eventos	servidor de dados	Servidor de Gerenciamento	Explicação
2011-B-0082	Diversas Vulnerabilidades no IBM Websphere Application Server	I	NF	Liberado	NA	NF	Afeta a versão anterior a 6.1.0.39 e 7.0.0.19
2011-B-0085	Diversas Vulnerabilidades de Negação de Serviço no Wireshark	I	NA	NA	NA	NA	Wireshark não instalado

Seleção de Listas de Verificação

As listas de verificação usadas para cada servidor são baseadas no software instalado nesse servidor. As listas de verificação específicas abordam vulnerabilidades para tipos de produtos, por exemplo, bancos de dados. Outras abordam problemas com produtos específicos em uma categoria, por exemplo, DB2.

Nem todos os tipos de produtos possuem listas de verificação específicas. As vulnerabilidades gerais são documentadas na lista de verificação Segurança do Aplicativo ou em uma lista relacionada ao sistema operacional.

Os seguintes tipos de listas de verificação são usados pelo cyber hygiene:

Segurança do aplicativo

Lista as vulnerabilidades em nível do sistema. Algumas estão relacionadas às práticas de desenvolvimento e teste de software e outras abordam vulnerabilidades específicas do aplicativo, como o não uso de senhas criptografadas durante a autenticação do usuário.

Unix/Linux

Lista vulnerabilidades relacionadas à configuração, gerenciamento de senha, particionamento do sistema de arquivos, etc.

Servidor da Web

Lista vulnerabilidades relacionadas a servidores HTTP.

Banco de Dados

Lista vulnerabilidades relacionadas a servidores de banco de dados.

Servidores de Diretório

Lista vulnerabilidades relacionadas a servidores LDAP.

Gerenciamento de Sistemas Corporativos

Lista vulnerabilidades relacionadas ao conjunto de ferramentas de gerenciamento de sistemas corporativos e a processos de gerenciamento de sistemas.

A segurança de rede não é abordada pelas listas de verificação, pois a configuração de segurança de rede deve ser determinada por políticas e arquitetura de rede de um cliente. A configuração de segurança de rede deve ser manipulada de acordo com as necessidades de cada instalação.

Configuração Padrão do Cyber Hygiene

O recurso cyber hygiene define configurações padrão e políticas do Linux como opções mais seguras do que as definidas na instalação do sistema operacional padrão. Essas configurações padrão podem facilmente se modificadas pelos administradores do sistema para estarem em conformidade com as políticas de segurança para a instalação.

Um grupo administrativo de operações de TI de uma empresa é responsável pela segurança de seus sistemas. Isso inclui o gerenciamento de acesso à rede e as políticas de segurança e processos internos.

Onde as configurações padrão do cyber hygiene são inconsistentes com a política corporativa, as políticas corporativas devem ter precedência. Lembre-se de que as configurações de política de segurança local não foram testadas para seu impacto na funcionalidade do sistema. O mesmo cuidado tomado ao aplicar a política de segurança a produtos não implementados com o cyber hygiene deve ser tomado ao aplicar a política de segurança ao IBM Intelligent Operations Center.

Embora o IBM Intelligent Operations Center não possa ser automaticamente configurado para políticas de segurança corporativa individual, o IBM Intelligent Operations Center pode ser configurado para remover vulnerabilidades conhecidas. O Cyber hygiene configura o IBM Intelligent Operations Center com um conjunto de políticas de melhor prática padrão que criam uma base para administradores de sistema usarem ao aplicar políticas e práticas organizacionais específicas

Políticas de Gerenciamento de Senhas Padrão

O Cyber Hygiene configura as políticas de gerenciamento de senha do sistema operacional Linux.

As políticas de gerenciamento de senha padrão configuradas pelo Cyber Hygiene são mostradas no Tabela 28.

Tabela 28. Políticas de Gerenciamento de Senha Padrão do Cyber Hygiene

Diretiva	Valor ou Configuração
Comprimento máximo da senha	8 caracteres
Caracteres Aceitos	letras maiúsculas, letras minúsculas, números, caracteres especiais (: ; ! ` ~ @ # \$ % ^ & * () - _ = + [{] } \ ' " , < . > / ? e o caractere de espaço)
Regras de Conteúdo	Nenhum
Número de tentativas falhas de logon antes de bloquear o usuário	3
Tempo Mínimo entre as Alterações de Senha	1 dia
Tempo Máximo entre Mudanças de Senha	60 dias
São necessárias senhas em contas?	yes
Quando uma senha pode ser reutilizada?	após 5 senhas diferentes
Efetue o login obrigatório após inatividade	15 minutos de inatividade
Atraso entre Falhas de Logon	4 segundos

Os arquivos `/etc/pam.d/system-auth` e `/etc/login.defs` são modificados na configuração das políticas padrão do Cyber Hygiene.

Estas configurações pretendem ser o mínimo necessário para práticas de segurança razoáveis. É preciso modificar estas configurações, a fim de corresponder às políticas de segurança da organização. Algumas áreas nas quais talvez você queira alterar as configurações padrão são as seguintes:

- Embora a configuração padrão defina o comprimento mínimo de senha para 8 caracteres, as melhores práticas para sistemas seguros geralmente consideram senhas seguras as que possuem 14 ou mais caracteres.
- O tempo máximo entre as mudanças de senha deve ser configurado como um valor apropriado para sua organização. Isso é definido no parâmetro **inactive** no arquivo `/etc/shadow`. No momento específico definido, o usuário é forçado a alterar a senha no login. Se o usuário não alterar a senha, a senha deverá ser reconfigurada por um usuário privilegiado. Se o valor especificado no arquivo `/etc/shadow` será usado depende da ação padrão especificada no arquivo `/etc/default/useradd`. Se o arquivo `/etc/default/useradd` especificar `-1`, a senha não expirará. Se `/etc/default/useradd` especificar `0`, a conta será bloqueada. Se qualquer outro valor no arquivo `/etc/default/useradd` estiver definido, o valor de parâmetro **inactive** em `/etc/shadow` será usado para expiração de senha.
- As regras referentes à complexidade de conteúdo de senhas devem ser abordadas e implementadas de acordo com a política de segurança corporativa.

Consulte a documentação do Linux para obter mais informações sobre o gerenciamento das políticas de senhas.

Serviços Linux Desativados

O Cyber Hygiene desativa ou desinstala serviços vulneráveis do Linux. Esses serviços podem permitir o acesso ao sistema e devem ser iniciados ou instalados apenas se forem necessários.

Por padrão, serviços Linux a seguir (daemons) não serão iniciados. Eles poderão ser iniciados, se necessário.

- `inetd/xinetd`
- `portmap`
- `avahi-daemon`
- `bluetooth`
- `cups`
- `hidd`
- `isdn`
- `rhnsd`
- `canna`
- `pcmcia`
- `yplib`
- `autofs`
- `smartd`
- `netfs`
- `snmpd`
- `nfs`
- `samba`

Esses serviços podem ser iniciados utilizando o comando **serviço** `service_name` **iniciar**.

Nota: Esses serviços, se não configurados apropriadamente, podem ser comprometidos e permitir acesso não autorizado ao sistema. É por isso que, para segurança do sistema, eles não são iniciados por padrão.

Os seguintes serviços do Linux serão removidos. Eles podem ser reinstalados, se necessário, usando os comandos **rpm** ou **yum**. Por exemplo, o comando **yum install httpd** instalará o pacote daemon de HTTP.

- tcpdump
- sendmail
- squid
- vnc-server
- httpd
- mod_python
- mod_perl
- mod_ssl
- webalizer
- httpd-manual

Nota: Esses serviços serão removidos do Linux, porque eles possuem um potencial elevado em causar exposições de segurança em ambientes do servidor.

IDs de Usuário Removidos

Uma instalação Linux padrão contém uma série de IDs de usuário não desejáveis em um ambiente de produção seguro. O Cyber hygiene remove esses IDs do usuário do registro do usuário do Linux e do arquivo `/etc/passwd`. Os diretórios iniciais associados também são removidos.

Os seguintes IDs do usuário serão excluídos e poderão ser recriados, se necessário.

- jogos
- notícias
- ftp
- parada
- encerramento
- reinicialização
- who
- Gopher
- lp
- rpcuser
- uucp

Se esses IDs de usuários forem necessários, os procedimentos de administração padrão do Linux poderão ser utilizados para criá-los.

Regras de Auditoria

A auditoria padrão no Linux é mínima, pois os arquivos de auditoria podem crescer rapidamente. No entanto, quando a segurança é um problema, a auditoria adicional é crítica para poder determinar o que aconteceu em um incidente. Os scripts do Cyber Hygiene incluem um conjunto de regras de auditoria adicionais para todos os níveis de execução do Linux. Eventos que correspondem a essas regras serão registrados nos arquivos de logs do sistema padrão.

As regras de auditoria do Linux a seguir são incluídas e podem ser modificadas, se necessário.

- Tentativas com falha de acesso a programas e arquivos
- Exclusão de programas e arquivos
- Ações administrativas, de segurança e privilegiadas
- Mudanças na Permissão do Controle de Acesso

Ter bons logs de auditoria é uma boa prática de segurança. Se, por algum motivo, a auditoria definido pelo Cyber Hygiene precisar ser mudada, os arquivos `/etc/audit/auditd.conf` e `/etc/audit/audit.rules` precisarão ser modificados. O Cyber hygiene ativa a auditoria para todos os cinco níveis de tempo de execução do Red Hat Enterprise Linux.

Permissões de Arquivos e Diretórios

Cyber Hygiene altera as permissões existentes de arquivos e diretórios para atender às melhores práticas de segurança.

As mudanças de permissão de arquivo e diretório feitas pelo Cyber Hygiene são as seguintes:

Restrição de Scripts do Sistema

Os scripts sensíveis ao sistema de segurança não podem ser acessados por usuários sem os privilégios apropriados.

Remoção da Permissão de Gravação Geral

Os usuários não poderão gravar em diretórios que não forem públicos. Os aplicativos e usuários que precisam modificar arquivos e diretórios devem ser o proprietário ou um membro do grupo, para o arquivo ou diretório.

Remoção da Permissões Gerais de Leitura e de Execução

As permissões gerais de execução e leitura serão removidas para muitos arquivos e diretórios. Em especial, essas permissões são removidas dos diretórios iniciais do usuário. Os aplicativos e usuários que precisam ler ou executar arquivos devem ser o proprietário ou membro do grupo, para o arquivo ou diretório.

Outras Mudanças

O Cyber Hygiene faz outras mudanças para tratar de exposições de segurança.

Programas em Lote - Comando `at`

Para impedir que usuários sem privilégio usem o comando `at` para executar programas em lote em um determinado horário, o Cyber Hygiene exclui o arquivo `at.deny` e cria um arquivo `at.allow` vazio.

O arquivo `at.allow` define os usuários que podem executar o comando `at`. Um arquivo `at.allow` que não contém IDs do usuário implica que nenhum usuário, a não ser IDs do sistema privilegiado, pode executar o comando `at`. Se existir o arquivo `at.deny`, que define usuários que explicitamente não podem usar o comando `at`, mas o arquivo `at.allow` não existir, todos os usuários, exceto os contidos no arquivo `at.deny`, poderão executar o comando `at`. Se nenhum arquivo existir, apenas o superusuário poderá executar o comando `at`.

Por padrão, o Red Hat Enterprise Linux é configurado para permitir que os usuários executem o comando `at`.

Programas em Lote - Comando `cron`

Usuários sem privilégios administrativos não têm permissão para executar o comando `cron` para planejar programas em lote.

Ctrl-Alt-Del

A combinação de teclas Ctrl-Alt-Del é desativada, portanto, não pode ser usada para encerrar o sistema.

Ferramentas de Correção

A funcionalidade cyber hygiene do IBM Intelligent Operations Center fornece ferramentas de correção para corrigir vulnerabilidades no sistema IBM Intelligent Operations Center instalado.

As ferramentas de correção são executadas quando o cyber hygiene é executado após a conclusão da instalação do IBM Intelligent Operations Center. Essas ferramentas também podem ser executadas quando o sistema está em produção para localizar e corrigir vulnerabilidades que podem ser criadas quando outros produtos são instalados nos servidores ou como um resultado do uso do sistema.

Scanner de Vulnerabilidade

O scanner consiste em scripts que revisam o sistema IBM Intelligent Operations Center e identificam vulnerabilidades. Por exemplo, o scanner identifica diretórios com privilégios de gravação para qualquer usuário.

O scanner cria um arquivo de descobertas usado pelos scripts de correção. O arquivo de descobertas lista as vulnerabilidades identificadas no sistema IBM Intelligent Operations Center.

Os scripts do scanner não fazem mudanças no sistema IBM Intelligent Operations Center. O scanner apenas identifica vulnerabilidades. Ele pode ser usado após a correção para validar as mudanças feitas pelos scripts de correção.

Scripts de Correção de Vulnerabilidade

O Cyber hygiene possui três tipos de scripts de correção:

- Scripts que fazem mudanças na configuração que não requerem varredura, que podem ser facilmente revertidas ou não têm nenhum impacto significativo de tempo de execução no sistema. Por exemplo, mudar a permissão de acesso a arquivo padrão das man pages para 644.
- Um script para desativar o logon remoto com a conta raiz.
- Um script que processa o arquivo de descobertas criado pelo scanner e resolve vulnerabilidades identificadas.

É necessário ter cuidado ao usar esse script após a instalação de produtos adicionais. Alguns produtos requerem menos configurações estritas e podem apresentar mau funcionamento após a execução desses scripts. Revise os arquivos de descobertas criados pelos scripts de scanner para possíveis riscos antes de executar qualquer script de correção.

Logs de Correção

Os scripts de varredura e correção registram suas ações em quatro arquivos de log em cada servidor IBM Intelligent Operations Center. Esses logs estão localizados no diretório `/var/BA15/CH/results`. Os subdiretórios contêm cópias de trabalho dos resultados de varredura e de correção.


O scanner é executado duas vezes: uma vez para corrigir vulnerabilidades e uma segunda vez para registrar correções não feitas. O log da segunda execução pode ser usado pelo administrador para determinar se as etapas de correção manual são necessárias.

Documentação do Cyber Hygiene

A documentação está disponível para ajudar o cliente a avaliar as mudanças aplicadas no sistema instalado do IBM Intelligent Operations Center. Esta documentação auxilia na certificação e no credenciamento de sistemas para uso da produção.

A documentação inclui uma visão geral da estratégia geral do Cyber Hygiene, a lógica para o motivo de alguns padrões terem sido implementados e uma planilha documentando o status de cada vulnerabilidade sinalizada pelo DISA. A planilha pode ser usada durante as avaliações de segurança do produto.

Informações relacionadas:

 Implementação do Cyber Hygiene no IBM Intelligent Operations Center 1.5

Capítulo 4. Integrando a Solução

Produtos e serviços podem ser integrados com o IBM Intelligent Operations Center incorporando dados relacionados a eventos.

Dados do evento comunicados ao IBM Intelligent Operations Center podem estar no Protocolo de Alerta Comum ou em outros protocolos.

Eventos podem estar relacionados a principais indicadores de desempenho (KPI) monitorados pelo IBM Intelligent Operations Center. Eventos no IBM Intelligent Operations Center podem estar relacionados também ao procedimentos padrão de operação e a recursos disponíveis. A solução fornece um serviço de administração de relatórios para que você possa produzir relatórios e resumos atualizados dos seus dados de evento.

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 100

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 93

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

Outros sistemas podem ser integrados com a solução por meio dos serviços e políticas do IBM Intelligent Operations Center. Dados podem ser recebidos no formato Common Alerting Protocol (CAP); outros protocolos também são suportados.

Eventos e KPIs

O IBM Intelligent Operations Center processa eventos e principais indicadores de desempenho (KPIs) para determinar como as informações serão exibidas.

Outros produtos e serviços podem ser integrados com o IBM Intelligent Operations Center por meio de um serviço de barramento de mensagem. KPIs são monitorados pelo serviço de monitoramento de negócios.

Os eventos são recebidos pelo IBM Intelligent Operations Center. Esses eventos podem ser exibidos em um portlet Detalhes e podem afetar o que será exibido em portlets de mapa.

A definição de KPI determina como os KPIs serão exibidos nos portlets Status e Drill Down de Key Performance Indicator. A definição de KPI também pode determinar como as informações sobre eventos serão exibidas. Por exemplo, se um limite de KPI for excedido, o evento pode ser sinalizado com uma urgência ou gravidade maior. Eventos sem definições de KPI correspondentes serão exibidos de acordo com as informações recebidas sobre o evento.

Para obter informações adicionais sobre como os KPIs são criados e integrados, consulte o link no final deste tópico.

Conceitos relacionados:

“Criando e Integrando KPIs” na página 109

Modelos de principais indicadores de desempenho (KPI) podem, ser criados e modificados usando um kit de ferramentas de desenvolvimento de monitoramento de negócios e um portlet de gerenciamento de KPI.

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 WebSphere Business Monitor para processamento.

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

Tabela 29. Propriedades de Ocorrência de KPI de Amostra

Propriedade	Valor
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
Descrição	Assalto
Data / hora de envio	17-02-2012T17:06:00+01:00
Data / hora de início	16-02-2012T15:47:00+01:00
Data / hora respondido	17-02-2012T17:06:00+01:00

A tabela a seguir mostra os parâmetros de KPI de amostra associados à atualização da ocorrência de KPI na Tabela 29.

Tabela 30. 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 290

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

“Notificações” na página 286

Use o portlet Notificações para visualizar as mensagens de alerta e os seus detalhes.

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 96

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 99

Também é possível usar dados CAP para fornecer dados sobre eventos não associados com cálculos de KPI.

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 96

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 99

Também é possível usar dados CAP para fornecer dados sobre eventos não associados com cálculos de KPI.

Tipos de Ocorrência

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

Ocorrência Real/Prevista

Mensagens do evento reais/previstas são mensagens não solicitadas enviadas por diversos 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.

Resposta

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

- 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.

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. Eventos relacionados são eventos cujo valor <referências> é o mesmo que o valor <identificador> do evento do incidente.

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

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

- 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.

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 31 na página 97 lista os elementos de dados utilizados em cálculos de KPI:

Tabela 31. 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 em que a mensagem foi enviada. Por exemplo: 2011-02-07T 16:49:00-05:00 contém a data e hora em que uma mensagem foi enviada. Os últimos seis caracteres indicam o fuso horário do evento CAP, em relação à Hora de Greenwich (GMT). Nesse caso, o evento ocorreu às 16:49:00, em GMT menos 5 horas, que é o Horário Padrão do Leste (EST). Esse código significa que quando o evento é exibido, ele é convertido de EST para o fuso horário do usuário. Se desejar codificar seus eventos CAP em GMT, mude o sufixo para -00:00 como nesse exemplo: 2011-02-07T 16:49:00-00:00.
Necessário	MessageStatus (status)	Status da mensagem, pode ser uma das seguintes opções: <ul style="list-style-type: none"> • Real • Exercício • Sistema • Teste • Rascunho
Necessário	MessageType (tipo mensagem)	Tipo da mensagem, pode ser uma das seguintes opções: <ul style="list-style-type: none"> • Alerta • Atualização • Cancelar • Confirmação • Erro
Opcional	Source (origem)	Origem da mensagem
Necessário	Scope (escopo)	Contém o valor Público
Necessário	Code (código)	Contém o valor KPI para ocultar esse evento da lista de portlets do Eventos.
Necessário	EventCategory (categoria)	Um dos seguintes valores: <ul style="list-style-type: none"> • Geo • Met • Proteção • Segurança • Resgate • Incêndio • Saúde • Amb • Transport • Infra • CBRNE • Outro

Tabela 31. Elementos CAP Usados em Cálculos de KPIs no IBM Intelligent Operations Center (continuação)

Necessário ou Opcional	Elemento de Dados (normativo)	Descrição
Necessário	EventType (ocorrência)	Descrição do evento ou KPI. Por exemplo: Police_Department_Budget
Necessário	Urgency (urgência)	Um dos seguintes valores: <ul style="list-style-type: none"> • Imediato • Esperado • Futuro • Passado • Desconhecido
Necessário	Severity (gravidade)	A severidade é indicada por uma das seguintes opções: <ul style="list-style-type: none"> • Extrema • Grave • Moderado • Baixa • Desconhecido
Necessário	Certainty (certeza)	A certeza é indicada por uma das seguintes opções: <ul style="list-style-type: none"> • Observada • Provável • Possível • Improvável • Desconhecido
Opcional	EventCode (código ocorrência)	Pares nome-valor para definição de tipo de evento.
Opcional	OnsetDateType (início)	Data e hora em que o evento inicia 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 do evento ou KPI
Opcional	Parameter (parâmetro)	Dados adicionais associados com o evento ou KPI.
Opcional	AreaGeocode (código geográfico)	Um campo que pode ser usado para fornecer informações quando o evento ou KPI é dependente de local

Para obter informações adicionais, consulte o link relacionado no final desse tópico para a especificação OASIS Protocolo de Alerta Comum.

O código a seguir é um exemplo de um evento que relata 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>

```

Conceitos relacionados:

“Localizando a Interface com o Usuário” na página 141

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.

“Problemas Conhecidos e Soluções” na página 328

Esta seção contém uma lista de problemas comuns de ocorrer e uma solução para cada item.

Informações relacionadas:

 OASIS Common Alerting Protocol Versão 1.2

Usando o CAP para Eventos não KPI

Também é possível usar dados CAP para fornecer dados sobre eventos não associados com cálculos de KPI.

Dados CAP recebidos pelo IBM Intelligent Operations Center que não estão associados com KPIs definidos são incluídos nos portlets Eventos e Mapa no IBM Intelligent Operations Center.

O seguinte código é para um evento não KPI de exemplo. Note que para eventos não KPI, você deve configurar o valor da tag code para Event.

```

<p>
<alert xmlns="urn:oasis:names:tc:emergency:cap:1.2">
  <identifier>f30f190c-41fd-431e-ace9-88b725f1a3fc</identifier>
  <sender>TestGenerator</sender>
  <sent>2012-03-26T15:47:24-00:00</sent>
  <status>Actual</status>
  <msgType>Alert</msgType>
  <scope>Public</scope>
  <restriction/>
  <code>Event</code>
  <info>
    <language>en_US</language>
    <category>Infra</category>
    <event>Water Main Break</event>
    <urgency>Immediate</urgency>
    <severity>Moderate</severity>
    <certainty>Observed</certainty>
    <headline>Vazamento grave de duto de água em NW 20th St.</headline>
    <description>O vazamento está localizado na intersecção da NW 20th Street e NW 9th Avenue. Inundação da rua começando. Ação imediata requerida.</description>
    <area>

```

```
<circle>25.79518,-80.21110 0</circle>
</area>
</info>
</alert>
</p>
```

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 seguintes recursos JMS são criados quando o IBM Intelligent Operations Center é instalado:

- Queue Connection Factory
 - Nome: `ioc.mb.con.factory`
 - Nome JNDI: `jms/ioc.mb.con.factory`
- Queue
 - Nome: `ioc.cap.in.q`
 - Nome JNDI: `jms/ioc.cap.in.q`

Conceitos relacionados:

“Comunicação de Evento de KPI Entre o IBM WebSphere Business Monitor e o IBM Intelligent Operations Center” na página 116

O IBM WebSphere Business Monitor pode enviar eventos de saída de um contexto de monitoramento ou de principal indicador de desempenho (KPI) para o IBM Intelligent Operations Center.

Criando Eventos Utilizando o Serviço do Publicador

É possível enviar eventos para o IBM Intelligent Operations Center por meio de serviços da web para o serviço do Publicador.

É possível criar aplicativos cliente que podem ser integrados a uma instância do IBM Intelligent Operations Center. É possível utilizar um aplicativo cliente para transferir alertas CAP de um aplicativo cliente de terceiros para um IBM Intelligent Operations Center chamando os métodos expostos pela classe do utilitário do serviço do Publicador do servlet do Publicador do IBM Intelligent Operations Center.

Desenvolvendo com as Classes Comuns dos Utilitários

Se deseja criar um aplicativo cliente que chama o serviço do Publicador, antes de começar, você deve configurar as classes comuns dos utilitários. Depois de concluir o desenvolvimento do aplicativo cliente, exporte-o como um arquivo WAR que você, em seguida, importe no WebSphere Application Server.

Sobre Esta Tarefa

Utilize o procedimento a seguir se desejar desenvolver um aplicativo cliente com as classes comuns dos utilitários:

- Antes de desenvolver o aplicativo cliente, inclua os arquivos JAR `iss_common` e `icu4j-4_4_2` no caminho de construção do projeto. Os arquivos JAR são necessários durante o tempo de compilação.
- Após desenvolver o aplicativo cliente, exporte-o como um arquivo WAR.
- Importe o arquivo WAR para o WebSphere Application Server e configure-o para referenciar as bibliotecas compartilhadas.

Procedimento

1. Localize o arquivo `iss_common.jar` e o arquivo `icu4j-4_8_1_1.jar` no diretório de instalação do IBM Intelligent Operations Center, `/opt/IBM/iss/common/lib`.
2. Copie o arquivo `iss_common.jar` e o arquivo `icu4j-4_8_1_1.jar` para um local na sua máquina de implementação.
3. Para incluir os arquivos JAR para o caminho de construção de projeto, na API do IBM Intelligent Operations Center, execute as seguintes subetapas para `iss_common.jar` e `icu4j-4_8_1_1.jar`:
 - a. Clique com o botão direito do mouse no **Projeto de Portlet**.
 - b. Clique em **Caminho de Construção > Configurar Caminho de Construção**.
 - c. Clique na guia **Bibliotecas** e clique em **Incluir JARs Externos...**
 - d. Navegue até o diretório que contém o arquivo JAR.
 - e. Clique no arquivo JAR, e em seguida clique em **Abrir**.
4. Após concluir o desenvolvimento do aplicativo cliente, exporte-o em um arquivo WAR.
5. No console administrativo do WebSphere Application Server, utilize o assistente de importação para importar arquivo WAR do aplicativo cliente.
6. Para configurar o arquivo WAR para referenciar a biblioteca compartilhada, execute as seguintes subetapas:
 - a. No console administrativo do WebSphere Application Server marque a caixa de seleção ao lado do arquivo WAR importado, e em seguida clique em **Atualizar**.
 - b. Clique em **Referências da biblioteca compartilhada**.
 - c. Na janela Referências de biblioteca compartilhada, marque a caixa de seleção **Aplicativo**.
 - d. Clique em **Fazer Referência às Bibliotecas Compartilhadas**.
 - e. Mova **ISSCommonJars** e **IOCCCommonJars** na lista Disponível para a lista Seleccionado, e em seguida clique em **OK**.
 - f. Para salvar suas alterações, clique em **OK**.

Utilizando o Serviço do Publicador

A ferramenta injetora de eventos do serviço do Publicador é fornecida como um utilitário Java. É possível criar um aplicativo cliente que passe o XML CAP no IBM Intelligent Operations Center, chamando os métodos expostos pelo serviço do Publicador. É possível também passar em notificações.

O serviço do Publicador é uma classe do utilitário no projeto `iss_common_utils`, que é construído no arquivo `iss_common.jar`. O serviço do Publicador expõe os métodos estáticos `publishEvent` e `publishNotification`. Antes de criar aplicativos cliente para o serviço do Publicador, é necessário configurar as classes de utilitário comuns. Para obter informações adicionais, consulte o link no final do tópico.

Para garantir que o código usado para chamar o serviço do Publicador tem acesso às configurações de fila de JMS corretas, você deve implementá-lo no servidor de aplicativos.

O código de amostra a seguir mostra como chamar o serviço do Publicador:

```
import com.ibm.iss.common.publisher.Publisher;

String capMessage = request.getParameter(EVENT_TEXT_KEY);

int status = Publisher.publishEvent(capMessage);

if (status == Publisher.STATUS_SUCCESS) {
    logger.traceFine(this, methodName, "Event submit request was performed successfully");
}
else if (status == Publisher.STATUS_EXCEPTION_NAMING) {
    logger.traceFine(this, methodName, "Error sending CAP Event Message. Requires defining JMS Resources.");
}
else if (status == Publisher.STATUS_EXCEPTION_JMS) {
```

```

logger.traceFine(this, methodName, "Error sending CAP Event Message. Failed to connect to JMS resources.");
}
else { //Other error code
logger.traceFine(this, methodName, "Error sending CAP Event Message. Returned status = " + status);
}

```

Se utilizar o portlet do Publicador de Amostra, não será necessário criar o código para chamar o serviço do Publicador, ou para gravar quaisquer mensagens CAP.

Conceitos relacionados:

“Publicador de Amostra” na página 103

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

Tarefas relacionadas:

“Desenvolvendo com as Classes Comuns dos Utilitários” na página 100

Se deseja criar um aplicativo cliente que chama o serviço do Publicador, antes de começar, você deve configurar as classes comuns dos utilitários. Depois de concluir o desenvolvimento do aplicativo cliente, exporte-o como um arquivo WAR que você, em seguida, importe-o no WebSphere Application Server.

Utilizando o Servlet do Publicador

O servlet do Publicador aceita parâmetros em solicitações de POST para publicar um XML de CAP, criar eventos novos ou criar eventos modificados a partir de eventos existentes ou incidentes.

Enviando Solicitações de POST para o Servlet do Publicador

O servlet do Publicador chama o serviço do Publicador para colocar o XML CAP nas filas que alimentam o IBM Intelligent Operations Center. O servlet do Publicador está localizado no `/ibm/iss/common/rest/publisher`. A tabela a seguir mostra como enviar solicitações de POST para o servlet do Publicador.

Tabela 32. Solicitações de POST do Servlet do Publicador

Tipo de evento a ser publicado	Código de Solicitação do POST
Publicar um novo evento de CAP	<code>action=publishEvent&source=xml&xml=CAP_event_XML</code>
Modificar um evento existente	<code>action=publishEvent&source=existing&id=event_id</code>
Publicar um novo evento em branco	<code>action=publishEvent&source=new</code>

Parâmetros opcionais

É possível aplicar parâmetros opcionais para cada uma das opções de publicação, anexando o seguinte código para a solicitação de POST: `¶meter_name=new_value`

Os seguintes parâmetros opcionais estão disponíveis:

- areaDesc
- categoria
- confirmação
- code
- contato
- descrição
- ocorrência
- Título
- latitude
- longitude
- msgType

- randomizar
- randomizado
- randomizeArea
- randomizeTime
- Emissor
- senderName
- gravidade
- status
- urgência

Por exemplo, para publicar um evento novo, em branco, e em seguida configurar o título para Tráfego, o código de solicitação de POST é: `servletURL&action=publishEvent&source=new&headline=Traffic Accident`

Criando e Publicando Eventos de Teste

O IBM Intelligent Operations Center fornece o portlet do Publicador de Amostra e o portlet do Script do Evento para criar e publicar eventos de teste.

Conceitos relacionados:

“Criando Eventos Utilizando o Serviço do Publicador” na página 100

É possível enviar eventos para o IBM Intelligent Operations Center por meio de serviços da web para o serviço do Publicador.

Publicador de Amostra

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

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

Criando Eventos e Notificações

Para ativar o portlet Publicador de Amostra, na interface de administração do WebSphere Portal, clique em **Intelligent Operations > Ferramentas de Demonstração > Publicador de Evento de Amostra**.

Na guia **CAP de Evento** do portlet Publicador de Amostra, é possível preencher um formulário para projetar eventos com XML. Envie o formulário para ativar um fluxo de ocorrências CAP de amostra no sistema.

O portlet Publicador de Amostra também contém uma guia **Formulário de Evento** para criar novos eventos quando não for necessário editar o XML. Preencha o formulário na guia **Formulário de Evento** para enviar os detalhes do evento do CAP. Se desejar criar novos eventos com propriedades baseadas nas propriedades de um evento existente, insira o ID de Alerta do CAP para o evento existente no campo **ID**.

O portlet Publicador de Amostra contém uma guia **Notificação** para testar o subsistema de notificações do IBM Intelligent Operations Center. Na guia **Notificação**, é possível preencher um formulário para enviar uma notificação de alerta para grupos especificados. Os valores inseridos no campo **Enviado para Grupos** devem corresponder aos grupos de usuários existentes, por exemplo, **CityWideOperator**, **CityWideExecutive**, porque apenas os alertas correspondentes são exibidos na lista de portlets do **Notificações**.

Valores Aleatórios

Nas guias **CAP de Evento** e **Formulário de Evento**, se você selecionar a caixa de seleção **Escolher Eventos Aleatoriamente**, o portlet alterará automaticamente as propriedades dos eventos publicados, 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.

Customizando o Portlet Publicador de Amostra

É possível customizar este portlet. Clique no botão no canto superior direito do portlet para ver as opções de customização do menu de portlet. As configurações compartilhadas afetam o conteúdo desse portlet para todos os usuários, mas apenas para esta ocorrência do portlet.

Referências relacionadas:

“Configurações do Portlet do Publicador de Amostra” na página 163

Customize o portlet do Publicador de Amostra alterando as configurações nos campos da janela **Configurações Compartilhadas**.

Criando Ocorrências de Amostra com XML

Na guia **CAP de Evento**, é possível selecionar um modelo de evento CAP de amostra que pode ser usado para visualizar, modificar e publicar eventos.

Antes de Iniciar

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

Tabela 33. 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
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

Sobre Esta Tarefa

Para obter informações adicionais sobre propriedades de eventos, consulte o link no final do tópico para o tópico de portlet do Detalhes.

Procedimento

1. Na interface de Administração do WebSphere Portal, clique em **Intelligent Operations > Ferramentas de Demonstração > Publicador de Evento de Amostra**.
2. Clique na guia **CAP de Evento**.
3. Na lista **Categoria**, selecione uma categoria de evento.
4. Para o campo **Mensagem de Evento**, escolha uma das seguintes opções:
 - Para inserir o XML para a mensagem CAP correspondente, pré-gravada automaticamente no campo **Mensagem de Evento**, na lista **Evento de Amostra**, selecione um evento. Se desejar, edite o XML para que ajuste aos seus requisitos.
 - No campo **Mensagem de Evento**, insira manualmente o XML para a mensagem CAP a partir do zero.
5. No campo **Contagem de Instância de Evento**, insira o número de mensagens necessárias ou utilize as setas para selecionar o número de mensagens necessárias. É possível enviar uma única mensagem CAP ou uma sequência de mensagens automatizadas.
6. Opcional: Marque a caixa de seleção **Randomizar Eventos**. Se você selecionar **Randomizar Eventos**, será publicada uma sequência de mensagens CAP com IDs aleatórios aplicados. As mensagens são publicadas em intervalos de tempo incrementais e em locais aleatórios em um intervalo.
7. Clique em **Enviar Ocorrência**.

Resultados

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

Conceitos relacionados:

“Detalhes” na página 272

Use o portlet Detalhes para visualizar, monitorar e gerenciar eventos no IBM Intelligent Operations Center.

Criando Novos Eventos CAP ou Atualizando Eventos de Atualização Existentes sem XML

Na guia **Formulário de Evento**, é possível concluir um formulário para criar novos eventos CAP ou atualizar eventos existentes, sem utilizar 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 um evento baseado em um evento existente, utilize o ID do Alerta CAP para fazer referência ao evento existente. Quaisquer valores inseridos no formulário substituem os valores herdados do evento CAP existente. Para obter informações adicionais sobre propriedades de eventos, consulte o link no final do tópico para o tópico de portlet do Detalhes.

Procedimento

1. Na interface de Administração do WebSphere Portal, clique em **Intelligent Operations > Ferramentas de Demonstração > Publicador de Evento de Amostra**.
2. Clique na guia **Formulário de Evento**.
3. 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 um evento com valores baseados em um evento existente na tabela de eventos CAP e usar o ID do Alerta CAP, clique em **Existente**.
4. No campo **ID**, insira um ID dependendo de se você vai criar um novo evento ou um evento baseado em um ID de alerta de CAP existente:
 - 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 um evento baseado em um valor de ID de Alerta de CAP existente, insira o valor do ID do Alerta CAP para **ID**. Quaisquer valores inseridos no formulário substituem os valores herdados do evento CAP existente.
 5. Se estiver criando um novo evento, no campo **Tipo de Evento**, insira um dos seguintes tipos de eventos:

Alerta Um novo evento.

Atualização

Uma atualização para um evento criado anteriormente.

Cancelamento

Cancelamento de um evento criado anteriormente.

6. No campo **Título**, insira um título.
7. A partir da lista **Tipo de Mensagem**, selecione um tipo de mensagem.
8. Se estiver criando um novo evento, na lista **Código de Evento**, selecione **Evento** ou **Incidente**. Um incidente tem mais importância do que um evento.
9. Na lista **Categoria**, selecione uma categoria.
10. Na lista **Urgência**, selecione a urgência.
11. Na lista **Gravidade**, selecione a gravidade.
12. Na lista **Certeza**, selecione a certeza.
13. No campo **Descrição**, insira uma descrição.
14. No campo **Remetente**, insira uma descrição do remetente da ocorrência.
15. 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.
16. Opcional: Marque a caixa de seleção **Randomizar Eventos**. Se você selecionar **Randomizar Eventos**, será publicada uma sequência de mensagens CAP com IDs aleatórios aplicados. As mensagens são publicadas em intervalos de tempo incrementais e em locais aleatórios em um intervalo.
17. Clique em **Enviar Ocorrência**.

Conceitos relacionados:

“Detalhes” na página 272

Use o portlet Detalhes para visualizar, monitorar e gerenciar eventos no IBM Intelligent Operations Center.

Testando Notificações

Use a guia **Notificação** para criar notificações de teste para testar o subsistema de notificações no IBM Intelligent Operations Center.

Sobre Esta Tarefa

Na guia **Notificação**, preencha o formulário para enviar um alerta para grupos especificados. Para um determinado usuário, uma mensagem de notificação de alerta é exibida no portlet do Notificações apenas se o usuário for um membro de um dos Grupos Enviado Para especificado na notificação.

Procedimento

1. Na interface de Administração do WebSphere Portal, clique em **Intelligent Operations > Ferramentas de Demonstração > Publicador de Evento de Amostra**.
2. Clique na guia **Notificação**.
3. Para criar um alerta, na lista **Tipo**, selecione **Alerta**.
4. Opcional: Na lista **Categoria**, selecione uma categoria.
5. Opcional: No campo **Título**, insira um título.
6. Opcional: No campo **Descrição**, insira uma descrição.
7. Opcional: No campo **Remetente**, insira uma descrição do remetente da ocorrência.
8. Opcional: No campo **Enviado para Grupos**, insira uma lista de grupos, separada por ponto e vírgula, para enviar o alerta, por exemplo, ;CityWideOperator;CityWideExecutive;.

Nota: Além de inserir um ponto e vírgula entre cada nome do grupo, certifique-se de inserir um ponto e vírgula no início e no final da lista. Quando publicadas, essa notificação de alerta é exibida no portlet Notificações apenas para usuários que são membros dos grupos CityWideOperator e CityWideExecutive.

9. Opcional: Execute uma das seguintes etapas conforme necessário:
 - No campo **Referir-se a Alertas**, insira uma lista de identificadores de eventos CAP, separada por ponto e vírgula, aos quais se refere o novo alerta.
 - No campo **Referir-se a Alertas**, insira uma lista de KPIs, separada por ponto e vírgula, aos quais se refere o novo alerta.
10. Clique em **Enviar Notificação**.

Conceitos relacionados:

“Notificações” na página 286

Use o portlet Notificações para visualizar as mensagens de alerta e os seus detalhes.

Script do Evento

Use o portlet Script do Evento para gravar um script para criar uma lista sequencial de eventos a serem publicados em intervalos de tempo predefinidos.

Para ativar o portlet Script do Evento, na interface de administração do WebSphere Portal, clique em **Intelligent Operations > Ferramentas de Demonstração > Script do Evento**.

No portlet Script do Evento, é possível gravar um script que faz referência a eventos a serem publicados pelos IDs de eventos que são registrados no tabela de eventos de amostra no Banco de dados do IBM Intelligent Operations Center. No script, é possível especificar um atraso entre os eventos a serem publicados. Quando você executa o script, o sistema publica os eventos por meio de back end. Entretanto, o fluxo de evento é o mesmo para eventos que entram no sistema a partir de origens externas.

Também é possível limpar os eventos do Banco de dados do IBM Intelligent Operations Center. Se você limpar os eventos do Banco de dados do IBM Intelligent Operations Center, todos os eventos exibidos no portlet Mapa e no portlet Detalhes serão excluídos.

Antes de usar o portlet Script do Evento, é possível visualizar os eventos no tabela de eventos de amostra no Banco de dados do IBM Intelligent Operations Center.

No portlet Script do Evento, siga o exemplo para criar um script JSON que define uma lista sequencial de eventos a serem publicados em intervalos de tempo predefinidos. Antes de executar o script, você deve limpar e validar o script clicando no botão **Limpar e Validar**.

É possível publicar um evento com um determinado ID apenas uma vez. Você deve excluir todos os eventos do Banco de dados do IBM Intelligent Operations Center antes de poder publicar um evento com

o mesmo ID novamente. No entanto, se você selecionar a caixa de seleção **Escolher IDs Aleatoriamente**, o portlet de script do evento publicará os mesmos eventos novamente e aplicará IDs aleatórios aos eventos.

Visualizando Eventos de Amostra e Eventos de KPI notabela de eventos de amostra

O portlet do Script do Evento publica eventos de amostra a partir do tabela de eventos de amostra no Banco de dados do IBM Intelligent Operations Center. Utilize o procedimento a seguir para visualizar os eventos no tabela de eventos de amostra.

Procedimento

1. Use um cliente VNC para efetuar logon no servidor de dados como um usuário raiz, e depois abra um a janela de comando. Nas etapas a seguir, insira comandos na janela de comando que acabou de ser aberta no servidor de dados.
2. Para conseguir abrir o DB2 Control Center, é necessário desligar temporariamente o controle de acesso; insira o seguinte comando: `xhost +`
3. No DB2 Control Center, visualize os eventos de amostra que estão no tabela de eventos de amostra, e obtenha os números de ID dos eventos de amostra:
 - a. Para abrir o DB2 Control Center, insira os seguintes comandos:

```
su - db2inst1
db2cc
```
 - b. No DB2 Control Center, clique em **Todos os Bancos de Dados > IOADB > Tabelas > REF_SAMPLEEVENTS**.
 - c. Clique com o botão direito do mouse na tabela **REF_SAMPLEEVENTS**, e em seguida clique em **Abrir**. Existem 40 na tabela de eventos de amostra, mas, depois que os eventos são publicados, apenas os eventos de 1 a 8 são exibidos no portlet do Detalhes. Os outros eventos são para testar os KPIs. Se você marcar a caixa de seleção **Randomizar IDs** no portlet do Script do Evento, será possível publicar repetidamente os mesmos oito eventos.
 - d. Observe que **SAMPLEID** para cada evento de amostra, para fazer referência ao criar scripts de evento no portlet do Script do Evento. O valor do **SAMPLEID** corresponde ao ID de evento.
4. Ao terminar de visualizar os eventos de amostra, feche o DB2 Control Center.
5. Para retornar para o usuário raiz, insira o seguinte comando: `exit`
6. Para ativar o controle de acesso novamente, insira o seguinte comando: `xhost-`

Conceitos relacionados:

“KPIs de Amostra” na página 121

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

Criando um Script de Evento

Crie um script de evento que publica uma sequência de eventos em intervalos de tempo predefinidos.

Antes de Iniciar

Antes de utilizar o portlet do Script do Evento para publicar eventos, é possível visualizar os eventos no tabela de eventos de amostra no Banco de dados do IBM Intelligent Operations Center.

Sobre Esta Tarefa

Utilize as seguintes etapas para criar um script de evento no portlet do Script do Evento.

Nota: É possível publicar um evento com um determinado ID apenas uma vez. Para conseguir publicar novamente um evento com o mesmo ID, clique em **Reconfigurar Banco de Dados** para excluir todos os eventos do Banco de dados do IBM Intelligent Operations Center. Como alternativa, para publicar novamente os mesmos eventos com IDs aleatórios aplicados, marque a caixa de seleção **Randomizar IDs**.

Procedimento

1. Na interface de Administração do WebSphere Portal, clique em **Intelligent Operations > Ferramentas de Demonstração > Script do Evento**.
2. Utilize o exemplo fornecido no portlet do Script do Evento para criar um script JSON que define uma lista seqüencial de eventos a serem publicadas em intervalos de tempo predefinido; insira o script no campo no lado esquerdo do exemplo. O script de exemplo JSON fornecido no portlet do Script do Evento também é mostrado no código a seguir:

```
[
  {
    "id": 2
    //ID of element in Sample Events table
    "delayAfter": 4000
    //Milliseconds to wait after publishing the event with the current ID
  },
  {}, //Empty objects are ignored
  {
    "id": 1
    //If the command specifies only an ID, the next command is processed
    //directly after the previous command
  },
  {
    "delayAfter": 0
    //If the command specifies only a delay, no event is published and the
    //script waits until the next command is due
  }
]
```

3. Opcional: Para publicar novamente os mesmos eventos com IDs aleatórios aplicados, marque a caixa de seleção **Randomizar IDs**.
4. Necessário: Para limpar e validar o script antes de executá-lo, clique em **Limpar e Validar**. A sintaxe do script é validado e os comentários, removidos. Se a marcação incorreta for detectada no script que não pode ser resolvido, será exibida uma mensagem.
5. Para executar o script, clique em **Executar Script de Evento**.
6. Para excluir todos os eventos do Banco de dados do IBM Intelligent Operations Center e impedir que o script publique mais algum evento, clique em **Reconfigurar o Banco de Dados**.

Tarefas relacionadas:

“Visualizando Eventos de Amostra e Eventos de KPI notabela de eventos de amostra” na página 108
O portlet do Script do Evento publica eventos de amostra a partir do tabela de eventos de amostra no Banco de dados do IBM Intelligent Operations Center. Utilize o procedimento a seguir para visualizar os eventos no tabela de eventos de amostra.

Criando e Integrando KPIs

Modelos de principais indicadores de desempenho (KPI) podem, ser criados e modificados usando um kit de ferramentas de desenvolvimento de monitoramento de negócios e um portlet de gerenciamento de KPI.

O Kit de Ferramenta de Desenvolvimento do IBM WebSphere Business Monitor pode ser instalado com o Rational Application Developer; ambos são fornecidos com o IBM Intelligent Operations Center. O IBM WebSphere 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 a inclusão ou modificação de um KPI dessa maneira, ele deve ser implementado para o servidor do IBM WebSphere Business Monitor.

Para obter informações adicionais sobre o uso do IBM WebSphere Business Monitor e do Kit de Ferramentas de Desenvolvimento do IBM WebSphere Business Monitor, consulte o Centro de Informações do IBM WebSphere Business Monitor.

Após estabelecer modelos e métricas de KPI por meio do IBM WebSphere Business Monitor, é possível usar o portlet Principais Indicadores de Desempenho para desenvolver e modificar KPIs.

Conceitos relacionados:

“KPIs de Amostra” na página 121

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

“Eventos e KPIs” na página 91

O IBM Intelligent Operations Center processa eventos e principais indicadores de desempenho (KPIs) para determinar como as informações serão exibidas.

“Customizando KPIs” na página 167

No IBM Intelligent Operations Center é possível customizar os modelos do Principal Indicador de Desempenho (KPI), a fim de se adequarem aos processos de negócios.

Referências relacionadas:

“Instalando Ferramentas Fornecidas com a Solução” na página 64

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 WebSphere Business Process Management Versão 7.0

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 121

KPIs de amostra são fornecidos com o IBM Intelligent Operations Center. Os KPIs de amostra são projetados para fornecer orientação para a implementação de diferentes tipos de KPI usando o Kit de Ferramentas de Desenvolvimento do IBM WebSphere Business Monitor. Modelos de monitor de amostra são fornecidos para água, transporte e segurança 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 de contexto de monitoramento corresponde a 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 121

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

Informações relacionadas:



Centro de Informações do IBM Business Monitor

Modelando KPIs

Modele KPIs com o Rational Application Developer ou o WebSphere Integration Developer, com o kit de ferramentas de desenvolvimento do IBM WebSphere Business Monitor instalado. O Rational Application Developer e o kit de ferramentas de desenvolvimento do IBM WebSphere Business Monitor estão incluídos como parte do IBM Intelligent Operations Center.

Sobre Esta Tarefa

Os KPIs são modelados usando o Rational Application Developer ou o WebSphere Integration Developer, com o kit de ferramentas de desenvolvimento do IBM WebSphere Business Monitor. 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 usando os assistentes de monitoramento de negócios do Rational Application Developer fornecidos pelo kit de ferramentas de desenvolvimento do IBM WebSphere Business Monitor.

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 WebSphere Business Monitor.
4. No Rational Application Developer ou no WebSphere Integration Developer, com o Kit de ferramentas de desenvolvimento do IBM WebSphere Business Monitor instalado, defina o evento de entrada, chave e conjunto de métricas para o contexto do monitoramento. 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 WebSphere Business Monitor.
8. Defina quaisquer filtragens desejadas de 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 34. Definições de Faixa e de Cor de KPI de Amostra

Nome	Cor	RGB
Aceitável	verde	699037
Cuidado	amarelo	FDBA1A
Execute uma ação	vermelho	C32E14

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 será referido como um KPI agregado. 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 (os KPIs sem filhos) são definidos como KPIs agregados. Os KPIs de nível superior (KPIs com filhos) são definidos como KPIs de expressão.

Valores de KPI agregados são calculados de métricas preenchidas com dados enviados em mensagens de alerta CAP enviadas para o servidor do IBM WebSphere 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 de IBM Intelligent Operations Center, os KPIs pais possuem cálculos que fazem o KPI avaliar para um valor de 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 agregado. 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 agregados do IBM Intelligent Operations Center de amostra possuem filtros de tempo definidos.
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 WebSphere Business Monitor e ocorrências de saída do IBM Intelligent Operations Center.
20. Teste o KPI. O kit de ferramentas de desenvolvimento do IBM WebSphere Business Monitor possui um ambiente de teste para testar os KPIs antes da implementação; para obter detalhes, consulte o link no final do tópico.
21. Implemente o aplicativo de modelo de monitor.

Conceitos relacionados:

“Definindo Hierarquias de KPI”

É possível definir relacionamentos pai-filho entre KPIs e designar como os KPIs são exibidos no IBM Intelligent Operations Center. Projete suas próprias hierarquias de KPI para que possa consultar os KPIs de forma que isso se ajuste ao processo de negócios.

“KPIs de Amostra” na página 121

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

“Comunicação de Evento de KPI Entre o IBM WebSphere Business Monitor e o IBM Intelligent Operations Center” na página 116

O IBM WebSphere Business Monitor pode enviar eventos de saída de um contexto de monitoramento ou de principal indicador de desempenho (KPI) para o IBM Intelligent Operations Center.

Tarefas relacionadas:

“Implementando Modelos de Monitor” na página 119

Após definir os principais indicadores de desempenho (KPIs) e seus modelos de monitor, os modelos de monitor precisam ser implementados para o IBM WebSphere Business Monitor em execução no IBM Intelligent Operations Center servidor de aplicativos.

Referências relacionadas:


“Instalando Ferramentas Fornecidas com a Solução” na página 64

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 Rational Application Developer

 Centro de Informações do IBM Business Monitor

 XML Path Language (XPath) 2.0 (Segunda Edição)

Definindo Hierarquias de KPI

É possível definir relacionamentos pai-filho entre KPIs e designar como os KPIs são exibidos no IBM Intelligent Operations Center. Projete suas próprias hierarquias de KPI para que possa consultar os KPIs de forma que isso se ajuste ao processo de negócios.

Enquanto o IBM WebSphere Business Monitor permite um KPI baseado no valor de outro KPI, ele não permite a definição de um relacionamento pai-filho entre KPIs. Para simplificar essa tarefa, o IBM Intelligent Operations Center fornece um portlet Principais Indicadores de Desempenho para o administrador. Para obter informações sobre este portlet, consulte o link no final deste tópico.

Os KPIs de amostra do IBM Intelligent Operations Center definem uma série de KPIs do Departamento de Polícia com um design hierárquico, conforme segue:

```
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 no modelo de KPI como KPIs agregados. 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.

O IBM Intelligent Operations Center suporta uma alternativa para o uso do portlet Principais Indicadores de Desempenho para definição de relacionamentos de KPI. O portlet Principais Indicadores de Desempenho é o método padrão com o parâmetro **UseDBModelReader** definido para true no tabela de propriedades de sistema. Para obter informações sobre mudança de configuração no tabela de propriedades de sistema, consulte o link no final desse tópico. Para obter informações sobre o método alternativo para definir relacionamentos de KPI, clique no link no final do tópico.

Conceitos relacionados:

“Principais Indicadores de Desempenho” na página 168

Use o portlet Principais Indicadores de Desempenho para customizar o Key Performance Indicators (KPIs) e sua exibição hierárquica no IBM Intelligent Operations Center.

“Especificando Dados de Configuração para Todo o Sistema” na página 178

A tabela de propriedades de sistema do IBM Intelligent Operations Center armazena dados de configuração do IBM Intelligent Operations Center.

“Definindo Hierarquias do KPI com OWL”

O IBM Intelligent Operations Center suporta o uso de OWL (Web Ontology Language), como uma alternativa ao uso do portlet Principais Indicadores de Desempenho, para definir relacionamentos pai-filho de KPI.

Definindo Hierarquias do KPI com OWL

O IBM Intelligent Operations Center suporta o uso de OWL (Web Ontology Language), como uma alternativa ao uso do portlet Principais Indicadores de Desempenho, para definir relacionamentos pai-filho de KPI.

Os relacionamentos pai-filho KPI podem ser definidos em OWL que é lida e processada pelo IBM Intelligent Operations Center. As definições são armazenadas em um arquivo RDF (Resource Description Framework).

É possível especificar se o modelo de banco de dados do KPI deve ou não ser lido a partir de um arquivo RDF. Para obter informações adicionais sobre como alterar essa propriedade no tabela de propriedades de sistema, consulte o link no final desse tópico.

Um exemplo de definições OWL para o KPI Departamento de Polícia de amostra configurado é o seguinte:

```
<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 >
```

Nota: OWL é uma linguagem construída em RDF. OWL e RDF são semelhantes, mas OWL é uma linguagem mais forte. OWL fornece um vocabulário maior, sintaxe mais forte e maior interpretabilidade de máquina do que RDF.

Conceitos relacionados:

“Definindo Hierarquias de KPI” na página 114

É possível definir relacionamentos pai-filho entre KPIs e designar como os KPIs são exibidos no IBM Intelligent Operations Center. Projete suas próprias hierarquias de KPI para que possa consultar os KPIs de forma que isso se ajuste ao processo de negócios.

“Principais Indicadores de Desempenho” na página 168

Use o portlet Principais Indicadores de Desempenho para customizar o Key Performance Indicators (KPIs) e sua exibição hierárquica no IBM Intelligent Operations Center.

“Especificando Dados de Configuração para Todo o Sistema” na página 178

A tabela de propriedades de sistema do IBM Intelligent Operations Center armazena dados de configuração do IBM Intelligent Operations Center.

Comunicação de Evento de KPI Entre o IBM WebSphere Business Monitor e o IBM Intelligent Operations Center

O IBM WebSphere Business Monitor pode enviar eventos de saída de um contexto de monitoramento ou de principal indicador de desempenho (KPI) para o IBM Intelligent Operations Center.

Ocorrências de saída do servidor do IBM WebSphere 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.

Nota: É possível especificar se a conexão para o IBM WebSphere Business Monitor vai utilizar ou não o SSL para conexão segura. Para obter mais informações sobre como alterar essa propriedade na tabela de propriedades do sistema, consulte o link no final deste tópico.

Conceitos relacionados:

“Especificando Dados de Configuração para Todo o Sistema” na página 178

A tabela de propriedades de sistema do IBM Intelligent Operations Center armazena dados de configuração do IBM Intelligent Operations Center.

“Usando a Fila de Ocorrências de Entrada Definida para o IBM Intelligent Operations Center” na página 100

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 WebSphere 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 WebSphere 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 abordarem 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 WebSphere 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

Eventos de entrada são definidos usando o Rational Application Developer ou o WebSphere Integration Developer com o Kit de ferramentas de desenvolvimento do IBM WebSphere Business Monitor. 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 seja repetido, assim ele irá disparar toda vez que a origem do acionador for atualizada e a condição acionadora for atendida.
8. Selecione a fonte acionadora.
9. Defina a condição acionadora. Quando a condição acionadora for atendida, o acionador disparará.

Exemplo

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

Tarefas relacionadas:

“Modelando KPIs” na página 111

Modele KPIs com o Rational Application Developer ou o WebSphere Integration Developer, com o kit de ferramentas de desenvolvimento do IBM WebSphere Business Monitor instalado. O Rational Application Developer e o kit de ferramentas de desenvolvimento do IBM WebSphere Business Monitor estão 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 WebSphere 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 WebSphere 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 WebSphere Business Monitor, atualiza as informações de cache do KPI e atualiza os dados do IBM Intelligent Operations Center.

Eventos de saída são definidos usando o Rational Application Developer ou o WebSphere Integration Developer com o Kit de ferramentas de desenvolvimento do IBM WebSphere Business Monitor. 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 111

Modele KPIs com o Rational Application Developer ou o WebSphere Integration Developer, com o kit de ferramentas de desenvolvimento do IBM WebSphere Business Monitor instalado. O Rational Application Developer e o kit de ferramentas de desenvolvimento do IBM WebSphere Business Monitor estão 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 os principais indicadores de desempenho (KPIs) e seus modelos de monitor, os modelos de monitor precisam ser implementados para o IBM WebSphere Business Monitor em execução no IBM Intelligent Operations Center servidor de aplicativos.

Sobre Esta Tarefa

Para implementar um modelo de monitor que será usado pelo IBM WebSphere 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 WebSphere Business Monitor em execução no IBM Intelligent Operations Center servidor de aplicativos.

Procedimento

1. No Rational Application Developer ou WebSphere Integration Developer com o Kit de ferramentas de desenvolvimento do IBM WebSphere Business Monitor instalado, dê um clique direito o modelo de monitor que requer a 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 WebSphere Business Monitor.
5. Implemente o arquivo EAR no servidor do IBM WebSphere Business Monitor usando as instruções no centro de informações do IBM WebSphere 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 do valores fornecidos pelos modelos do IBM WebSphere Business Monitor.

Os nomes de exibição de KPI e nomes de intervalos são definidos nos modelos de amostra do IBM WebSphere 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 WebSphere 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 WebSphere Business Monitor é usado.

Os valores de exibição de KPI são localizados pelo IBM WebSphere Business Monitor usando os códigos ISO de idioma e país do servidor do IBM WebSphere Business Monitor. Por exemplo, um valor percentual de KPI seria exibido no formato 12,61% quando o código de idioma fosse en_US e 12.61% quando o código de idioma fosse 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 WebSphere Business Monitor retornam um valor nulo. Por

exemplo, o KPI Lago da Cidade do Nível das Águas é definido com um período de tempo diário de repetição baseado no último período completo. 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 WebSphere 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. Os KPIs de amostra são projetados para fornecer orientação para a implementação de diferentes tipos de KPI usando o Kit de Ferramentas de Desenvolvimento do IBM WebSphere Business Monitor. Modelos de monitor de amostra são fornecidos para água, transporte e segurança pública.

Armazenamento em Cache de KPIs

As definições de configuração do IBM Intelligent Operations Center são afetadas quando valores KPI são recuperados do IBM WebSphere Business Monitor.

O IBM Intelligent Operations Center mantém valores de KPI em um cache. Por padrão, os KPIs são carregados a partir do IBM WebSphere Business Monitor para o cache, e o cache é atualizado de acordo com o intervalo de tempo especificado pela propriedade `KpiCacheRefreshInterval` na tabela de propriedades do sistema. Esse período de atualização pode ser alterado, dependendo das solicitações para fornecer KPIs atualizados para o IBM Intelligent Operations Center. Para obter informações adicionais sobre mudança das propriedades na tabela de propriedades de sistema, consulte o link no final do tópico.

Note que ao criar um KPI no portlet Principais Indicadores de Desempenho, as atualizações para o KPI dependem exclusivamente da atualização do cache. Quando um KPI é definido no IBM WebSphere Business Monitor, um mecanismo acionador pode ser definido para implementar um processamento adicional, em resposta às mudanças nesse KPI.

Conceitos relacionados:

“Especificando Dados de Configuração para Todo o Sistema” na página 178

A tabela de propriedades de sistema do IBM Intelligent Operations Center armazena dados de configuração do IBM Intelligent Operations Center.

KPIs de Amostra

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

Os KPIs de nível mais baixo são definidos como KPIs agregados. KPIs agregados são calculados de valores contidos em mensagens de alerta de CAP recebidas e de uma função de agregação como média, máximo, mínimo, soma, número de ocorrências ou desvio padrão. Seus valores são expressos em medidas quantificáveis. Valores de KPI de nível inferior são localizados no formato apropriado com base no código do idioma do servidor do IBM WebSphere Business Monitor. Os KPIs de nível mais alto são mapeados para valores baseados no mapeamento definido quando o KPI de amostra foi criado.

O valor do KPI de amostra de nível mais alto é um número que se equipara à cor e ao nível de resposta recomendados. Um valor de 0 é aceitável, um valor de 1 é cuidado e um valor de 2 é execução. 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 WebSphere Business Monitor Toolkit instalado. O archive pode ser modificado para alterar, incluir ou excluir definições de KPI. As definições podem ser geradas novamente e reimplimentadas no IBM Intelligent Operations Center.

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

- `icoc_sample_public_safety_monitor_model`
- `icoc_sample_transportation_monitor_model`
- `icoc_sample_water_monitor_model`

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 290

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

“Drill Down de Key Performance Indicator” na página 275

Use o portlet Drill Down de Key Performance Indicator para consultar informações adicionais sobre a categoria de KPI e o status de seus KPIs subjacentes.

“Criando e Integrando KPIs” na página 109

Modelos de principais indicadores de desempenho (KPI) podem, ser criados e modificados usando um kit de ferramentas de desenvolvimento de monitoramento de negócios e um portlet de gerenciamento de KPI.

“Customizando KPIs” na página 167

No IBM Intelligent Operations Center é possível customizar os modelos do Principal Indicador de Desempenho (KPI), a fim de se adequarem aos processos de negócios.

Tarefas relacionadas:

“Implementando Modelos de Monitor” na página 119

Após definir os principais indicadores de desempenho (KPIs) e seus modelos de monitor, os modelos de monitor precisam ser implementados para o IBM WebSphere Business Monitor em execução no IBM Intelligent Operations Center servidor de aplicativos.

“Visualizando Eventos de Amostra e Eventos de KPI notabela de eventos de amostra” na página 108

O portlet do Script do Evento publica eventos de amostra a partir do tabela de eventos de amostra no Banco de dados do IBM Intelligent Operations Center. Utilize o procedimento a seguir para visualizar os eventos no tabela de eventos de amostra.

Configurando o Tivoli Service Request Manager

Na interface com o usuário do Tivoli Service Request Manager, é possível gerenciar o procedimentos padrão de operação, fluxos de trabalho e os recursos.

Se você incluir um prefixo comum nos nomes de procedimentos padrão de operação, fluxos de trabalho e recursos, será mais fácil filtrar os dados em uma procura. Por exemplo, para projetos do cliente, use o prefixo comum CX.

É possível especificar se a conexão com o Tivoli Service Request Manager utiliza SSL ao configurar a propriedade **TSRMServerSecurityEnabled**. Para obter mais informações sobre esta propriedade e sobre outras do Tivoli Service Request Manager acesse o link no final do tópico.

Conceitos relacionados:

“Servidor de eventos” na página 208

“Especificando Dados de Configuração para Todo o Sistema” na página 178

A tabela de propriedades de sistema do IBM Intelligent Operations Center armazena dados de configuração do IBM Intelligent Operations Center.

Utilizando a Interface com o Usuário do Tivoli Service Request Manager

Saiba como acessar a interface com o usuário do Tivoli Service Request Manager . Torne o Tivoli Service Request Manager Start Center mais fácil e rápido de usar, customizando-o com links para os recursos mais utilizados.

Abrindo Aplicativos do Tivoli Service Request Manager

É possível abrir os aplicativos do Tivoli Service Request Manager por meio da interface de Administrador do WebSphere Portal, ou por meio das Ferramentas de Administração da Solução ou por meio do portlet do Procedimentos Padrão de Operação. Também é possível visualizar um recurso no Tivoli Service Request Manager por meio da interface do IBM Intelligent Operations Center.

Antes de Iniciar

Para poder visualizar um recurso no Tivoli Service Request Manager por meio da interface do IBM Intelligent Operations Center, uma conexão única deve ser configurada.

Procedimento

- Para abrir o Tivoli Service Request Manager Start Center por meio da interface de Administração do WebSphere Portal, utilize as seguintes subetapas:
 1. Clique em **Intelligent Operations > Ferramentas de Administração > Consoles de Administração**.
 2. Clique em **Standard Operating Procedure Administração**.
 3. Efetue login no Tivoli Service Request Manager Start Center como um administrador.
- Para abrir aplicativos do Tivoli Service Request Manager relacionados ao procedimentos padrão de operação, utilize o portlet do Procedimentos Padrão de Operação:
 1. Para abrir o portlet do Procedimentos Padrão de Operação, na interface de Administração do WebSphere Portal, clique em **Intelligent Operations > Ferramentas de Customização > Procedimentos Padrão de Operação**.
 2. Escolha uma das opções a seguir:
 - Para abrir o aplicativo Standard Operating Procedure, clique em **Standard Operating Procedures**.
 - Para abrir o aplicativo Matriz de Seleção do Standard Operating Procedure, clique em **Matriz de Seleção do Standard Operating Procedures**.
 - Para abrir o aplicativo do designer de fluxo de trabalho, clique em **Designer de Fluxo de Trabalho**.
- Para visualizar um recurso na interface com o usuário do Tivoli Service Request Manager por meio da interface do IBM Intelligent Operations Center, execute as seguintes etapas:
 1. No portlet do Detalhes, na guia **Eventos e Incidentes**, clique com o botão direito do mouse em uma linha na lista de eventos.
 2. Para visualizar uma lista de recursos na proximidade do evento, clique em **Visualizar Recursos Próximos** e selecione o raio da área em que deseja manter o foco. Uma lista de recursos é exibida na guia **Recursos**.
 3. Na guia **Recursos**, clique com o botão direito do mouse em uma linha na lista de recursos, e em seguida clique em **Propriedades**. O recurso será exibido no Tivoli Service Request Manager, na guia **Recursos**.

Nota: Para desconectar-se completamente do Tivoli Service Request Manager, é preciso fechar a janela do navegador da Web da interface com o usuário do Tivoli Service Request Manager.

Tarefas relacionadas:

“Configurando Conexão Única para Serviços de Colaboração” na página 52

Importe o token SSO LTPA do WebSphere Portal para o , a fim de permitir que usuários acessem os serviços de colaboração sem precisar inserir novamente suas credenciais.

Configurando Aplicativos Favoritos no Tivoli Service Request Manager Start Center

Atualize seus aplicativos favoritos no Tivoli Service Request Manager Start Center para que eles sejam acessados com mais facilidade.

Sobre Esta Tarefa

Cada usuário do Tivoli Service Request Manager Start Center tem seu Tivoli Service Request Manager com a lista customizada do próprio do usuário em Aplicativos Favoritos.

Procedimento

1. Para visualizar o Tivoli Service Request Manager Start Center, na parte superior da interface com o usuário do Tivoli Service Request Manager, clique em **Centro de Início**.
2. No Tivoli Service Request Manager Start Center, clique no ícone **Editar Portlet** ao lado de Aplicativos Favoritos.
3. Na janela Configuração de Aplicativos Favoritos, clique em **Selecionar Aplicativos**.
4. Na janela Selecionar Aplicativos, selecione os aplicativos que deseja que sejam exibidos em Aplicativos Favoritos. A lista a seguir mostra aplicativos úteis para usuários do IBM Intelligent Operations Center:

CRONTASK

Configuração da Tarefa Cron

DOMAINADM

Domínios

PESSOA

Membros

PERSONGR

Grupos de Membros

PLUSIMTRIX

Matriz de Seleção SOP

PLUSIRES

Recursos

PLUSIWO

Atividades SOP

USER

Usuários

WFDESIGN

Designer de Fluxo de Trabalho (Workflow Designer)

5. Para definir a posição em que os aplicativos serão listados em Aplicativos Favoritos, execute as seguintes etapas:
 - a. Na janela Configuração de Aplicativos Favoritos, selecione um aplicativo.
 - b. No campo **Ordem**, insira um número.
6. Para salvar as atualizações, clique em **Concluído**.

Configurando Novos Usuários no Tivoli Service Request Manager

Ao incluir um usuário no IBM Intelligent Operations Center, designe permissões e grupos de pessoas para o usuário no Tivoli Service Request Manager.

Configurar Site de Inserção Padrão

Para que um novo usuário consiga incluir novos recursos e aplicar o procedimento padrão de operação, é preciso configurar o Site de Inserção Padrão para o usuário.

Procedimento

1. Efetue login no Tivoli Service Request Manager Start Center como um administrador.
2. Clique em **Acessar > Segurança > Usuários**.
3. Para procurar o usuário, na guia **Lista**, no campo **Usuário**, insira algumas ou todas as letras no nome do usuário.
4. Na lista, clique no nome do usuário, e em seguida clique na guia **Usuário**.
5. Em Configurações do Usuário, próximo ao campo **Site de Inserção Padrão** clique no ícone **Selecionar Valor**.
6. Na janela Selecionar Valor, procure e clique no nome do Site de Inserção Padrão; por exemplo, **PMSCRTTP**. PMSCRTTP é um site de amostra que é instalado com o IBM Intelligent Operations Center.
7. Clique no ícone **Salvar Usuário**.

Designando um Usuário para um Grupo de Segurança

Inclua usuários aos grupos de segurança apropriados, de forma que eles tenham acesso aos aplicativos apropriados no Tivoli Service Request Manager.

Sobre Esta Tarefa

Para incluir um usuário a um grupo, utilize o procedimento a seguir.

Procedimento

1. Efetue login no Tivoli Service Request Manager Start Center como um administrador.
2. Clique em **Acessar > Segurança > Usuários**.
3. Para procurar o usuário, na guia **Lista**, no campo **Usuário**, insira algumas ou todas as letras no nome do usuário.
4. Na lista, clique no nome do usuário, e em seguida clique na guia **Grupos**.
5. Para procurar o grupo no qual deseja incluir o usuário, no campo **Grupo**, insira algumas ou todas as letras no nome do grupo.
6. Se o nome do grupo requerido não estiver listado, clique em **Nova Linha**.
7. Em Detalhes, próximo ao campo **Grupo**, clique no ícone **Menu Detalhe**, e em seguida clique em **Selecionar Valor**.
8. Na janela Selecionar Valor, procure e clique no nome do grupo requerido.
9. Clique no ícone **Salvar Usuário**.

Designando um Usuário para um grupo de pessoas

Em um procedimento padrão de operação, as tarefas podem ser designadas para grupos de membros predefinidos. Um usuário deve ser um membro de um determinado grupo de pessoas para verificar as tarefas designadas para esse grupo de pessoas.

Antes de Iniciar

É possível utilizar grupos de membros de amostra fornecido durante a instalação do IBM Intelligent Operations Center ou é possível criar seu próprio grupos de membros. Para obter informações sobre como criar um grupo de pessoas em Tivoli Service Request Manager, consulte o centro de informações do Maximo Asset Management.

Nota: Certifique-se de que os nomes de todos os grupos de membros sejam do mesmo tamanho. Isso garante que os usuários sejam designados somente para tarefas alocadas para o grupos de membros, dos quais eles são membros.


Sobre Esta Tarefa

Para designar um usuário para um grupo de pessoas, utilize o procedimento a seguir.

Procedimento

1. Efetue login no Tivoli Service Request Manager Start Center como um administrador.
2. Clique em **Acessar > Administração > Recursos > Grupos de Pessoas**.
3. Para procurar pelo grupo de pessoas requerido, na guia **Lista**, no campo **Grupos de Pessoas** insira algumas ou todas as letras no nome do grupo de pessoas.
4. Na lista, clique no nome do grupo de pessoas.
5. Na guia **Grupo de Pessoas**, em **Pessoas**, clique em **Nova Linha**.
6. Em **Detalhes**, próximo ao campo **Pessoa**, clique no ícone **Menu Detalhe**, e em seguida clique em **Selecionar Valor**.
7. Na janela **Selecionar Valor**, procure e clique no nome do usuário que deseja incluir no grupo de pessoas.
8. No campo **Seqüência**, insira o próximo número incremental disponível.
9. Clique no ícone **Salvar Grupo de Pessoas**.

Informações relacionadas:

 Centro de Informações do Maximo Asset Management

Procedimentos Padrão de Operação

É possível definir o procedimentos padrão de operação e atividades para gerenciar eventos que chegam ao IBM Intelligent Operations Center. Use o portlet **Procedimentos Padrão de Operação** para acessar os aplicativos procedimento padrão de operação, matriz de seleção de procedimento padrão de operação e designer de fluxo de trabalho no Tivoli Service Request Manager.

Para ativar o portlet **Procedimentos Padrão de Operação**, na interface de administração do WebSphere Portal, clique em **Intelligent Operations > Ferramentas de Customização > Procedimentos Padrão de Operação**.

Um procedimento padrão de operação define uma sequência de atividades que são acionadas em resposta a um evento cujos parâmetros atendem a determinadas condições predefinidas, em que cada atividade corresponde a uma tarefa manual ou automatizada. É possível designar um fluxo de trabalho a uma tarefa automatizada. Cada atividade é designada a um grupo de proprietários e os usuários são designados a um grupo de proprietários por meio de sua associação a um grupo de pessoas. Todos os usuários que estão designados ao grupo de proprietários podem gerenciar as atividades por meio do portlet **Minhas Atividades**.

É possível especificar a ordem na qual algumas ou todas as atividades em um procedimento padrão de operação são executadas. Por exemplo, é possível especificar que uma atividade específica não seja iniciada até que a atividade anterior seja concluída ou ignorada.

Para abrir o aplicativo procedimento padrão de operação, no portlet Procedimentos Padrão de Operação, clique em **Procedimentos Padrão de Operação**.

Matriz de Seleção de Procedimento Padrão de Operação

No matriz de seleção de procedimento padrão de operação, defina os parâmetros de evento que determinem se um procedimento padrão de operação foi iniciado para um determinado evento. Cada procedimento padrão de operação pode ter um ou mais conjuntos de critérios de seleção. Porém, cada conjunto de critérios de seleção deve ser exclusivo.

Para abrir o aplicativo matriz de seleção de procedimento padrão de operação, no portlet Procedimentos Padrão de Operação, clique em **Matriz de Seleção de Procedimentos Padrão de Operação**.

Designer de fluxo de trabalho

Utilize o designer de fluxo de trabalho para projetar o fluxos de trabalho que pode ser designado para as atividades do procedimento padrão de operação como tarefas automatizadas.

Para abrir o aplicativo designer de fluxo de trabalho, no portlet Procedimentos Padrão de Operação, clique em **Designer de Fluxo de Trabalho**.

Customizando o Portlet Procedimentos Padrão de Operação

É possível customizar este portlet. Clique no botão no canto superior direito do portlet para ver as opções de customização do menu de portlet. As configurações compartilhadas afetam o conteúdo desse portlet para todos os usuários, mas apenas para esta ocorrência do portlet.

Conceitos relacionados:

“Minhas Atividades” na página 284

O portlet Minhas Atividades exibe uma lista dinâmica de atividades pertencentes ao grupo do qual o usuário que está conectado à interface é membro.

Referências relacionadas:

“Configurações do Portlet do Procedimentos Padrão de Operação” na página 164

Customize o portlet do Procedimentos Padrão de Operação alterando as configurações nos campos da janela **Configurações Compartilhadas**.

Criando fluxos de trabalho

No Tivoli Service Request Manager, é possível criar o fluxos de trabalho que pode ser incluído como tarefas automatizadas nas atividades do procedimento padrão de operação.


Sobre Esta Tarefa

Para obter informações detalhadas sobre como criar fluxos, consulte o link para o centro de informações do Maximo Asset Management no final do tópico.

Procedimento

1. Para abrir o portlet do Procedimentos Padrão de Operação, na interface de Administração do WebSphere Portal, clique em **Intelligent Operations > Ferramentas de Customização > Procedimentos Padrão de Operação**.
2. Para abrir o aplicativo do designer de fluxo de trabalho, clique em **Designer de Fluxo de Trabalho**.
3. Na janela Designer de Fluxo de Trabalho, clique na guia **Tela**.
4. Na guia **Tela**, clique nos ícones para inserir os nós necessários e setas para o fluxo de trabalho.

Informações relacionadas:

 Centro de Informações do Maximo Asset Management

Criando procedimentos padrão de operação

Crie um procedimento padrão de operação e designe-o a um grupo de proprietários. Os usuários são designados a um grupo de proprietários por meio da associação de um grupo de pessoas.

Procedimento

1. Para abrir o portlet Procedimentos Padrão de Operação na interface de Administração do WebSphere Portal, clique em **Intelligent Operations > Ferramentas de Customização > Procedimentos Padrão de Operação**.
2. Para abrir o aplicativo procedimento padrão de operação, clique em **Procedimentos Operacionais Padrão**.
3. Na janela Procedimento Padrão de Operação, na guia **Lista**, clique no ícone **Novo SOP**. Um procedimento padrão de operação em branco é exibido na guia **Procedimento Padrão de Operação**.
4. Para **Nome SOP**, insira um nome e no campo ao lado do **Nome SOP**, insira uma descrição. Para os nomes do procedimentos padrão de operação, use um formato consistente similar aos nomes do procedimentos padrão de operação de amostra; por exemplo, Preparar para evacuação de clima severo (Preparar). Também, se o último caractere do nome for um parênteses de fechamento, anexe o caractere de marcação da esquerda para a direita (LRM) para evitar potenciais problemas relacionados à renderização de texto bidirecional. Por exemplo, insira o nome usado no exemplo anterior como Preparar para evacuação de clima severo (Preparar)‎. O caractere LRM não é exibido na interface com o usuário depois de você salvar o procedimento padrão de operação. Além disso, se você incluir um prefixo comum nos nomes de todos os procedimentos padrão de operação, será mais fácil filtrar o procedimentos padrão de operação em uma procura. Por exemplo, para projetos do cliente, use o prefixo comum CX.
5. Para inserir uma descrição mais longa, clique no ícone ao lado do campo da descrição e insira uma descrição na janela que for exibida.
6. Em Detalhes, na lista **Tipo de Modelo**, selecione **Atividade**.
7. Em Detalhes, designe um grupo de proprietários ao procedimento padrão de operação:
 - a. Clique no ícone ao lado do campo **Grupo de Proprietários**.
 - b. Na janela Selecionar Valor, clique em um valor na lista para selecioná-lo.
8. Opcional: Para **Duração**, informe um limite de tempo no qual o procedimento padrão de operação deve ser concluído. O formato do limite de tempo é *hh:mm*, em que *hh* é o número de horas e *mm* é o número de minutos. A data de vencimento é calculada com base na duração.
9. Inclua tarefas no procedimento padrão de operação, conforme necessário:
 - a. Perto do lado direito inferior da interface com o usuário do Tivoli Service Request Manager, clique em **Nova Linha**. Em Etapas do SOP, uma nova linha de tarefa é anexada à lista de sequências de tarefas.
 - b. Para **Sequência** e **Tarefa**, insira o mesmo número. Número de tarefas com o seguinte padrão: 10, 20, 30 e assim por diante. Se usar esse padrão, posteriormente você terá mais flexibilidade para incluir e remover tarefas.
 - c. Para **Instrução**, insira uma descrição de tarefa. Para selecionar entre as descrições inseridas anteriormente, clique no ícone ao lado do campo de descrição.
 - d. Opcional: Designe um fluxo de trabalho:
 - 1) Para **Nome do Fluxo de Trabalho**, clique no ícone **Selecionar Valor**.
 - 2) Na janela **Selecionar Valor**, clique em um valor na lista para selecioná-lo. Para reduzir a lista, no campo de filtro que é exibido no início da lista, insira as primeiras letras do nome de um fluxo de trabalho que você deseja usar.
 - 3) Expanda a linha da tarefa e, em Detalhes, insira mais detalhes, conforme necessário. Se desejar, é possível especificar configurações de um grupo de proprietários e de controle de

fluxo. Se não especificar as configurações de um grupo de proprietários e de controle de fluxo para a tarefa, ela herdará as configurações do procedimento padrão de operação pai.

10. Para salvar o procedimento padrão de operação, perto da parte superior da interface com o usuário do Tivoli Service Request Manager, clique no ícone **Salvar SOP**.
11. Para que o procedimento padrão de operação seja aplicado aos eventos especificados no matriz de seleção de procedimento padrão de operação, assegure-se de alterar o status de DRAFT para ACTIVE:
 - a. Clique no ícone **Status da Mudança**.
 - b. Na janela Alterar Status, na lista **Novo Status**, selecione **Ativo**.
 - c. Opcional: Informe valores para **A Partir da Data** e **Memorando**.
 - d. Clique em **OK**.
12. Para revisar os procedimentos padrão de operação disponíveis, execute as etapas a seguir:
 - a. Clique na guia **Lista**.
 - b. Em Planos de Tarefa do SOP, escolha uma das opções a seguir:
 - No campo de filtro, pressione Enter para visualizar todos os procedimentos padrão de operação disponíveis.
 - No campo de filtro, informe as primeiras letras do nome de um procedimento padrão de operação.
 - c. Para visualizar os detalhes de um procedimento padrão de operação, clique no nome do procedimento padrão de operação na lista. Os detalhes são exibidos na guia **Standard Operating Procedure**.

O que Fazer Depois

Se você desejar poder especificar a ordem na qual algumas ou todas as atividades em um procedimento padrão de operação são executadas, em Detalhes, marque a caixa de seleção **Fluxo Controlado?**. Para obter mais informações sobre como ordenar as atividades designadas aos usuários ou grupos com base nos procedimentos padrão de operação, consulte o centro de informações do Maximo Asset Management e procure *controle de fluxo*.

Na matriz de seleção de procedimento padrão de operação, defina os parâmetros de evento que determinam para quais eventos o procedimento padrão de operação é selecionado.

Tarefas relacionadas:

“Designando um Usuário para um grupo de pessoas” na página 126

Em um procedimento padrão de operação, as tarefas podem ser designadas para grupos de membros predefinidos. Um usuário deve ser um membro de um determinado grupo de pessoas para verificar as tarefas designadas para esse grupo de pessoas.

Informações relacionadas:



Centro de Informações do Maximo Asset Management

Revisando Entradas na matriz de seleção de procedimento padrão de operação

Na matriz de seleção de procedimento padrão de operação, revise os critérios de seleção para cada procedimento padrão de operação. Os critérios de seleção são baseados nos parâmetros de evento.

Procedimento

1. Para abrir o portlet Procedimentos Padrão de Operação na interface de Administração do WebSphere Portal, clique em **Intelligent Operations > Ferramentas de Customização > Procedimentos Padrão de Operação**.
2. Para abrir o aplicativo Matriz de Seleção de Procedimento Padrão de Operação, clique em **Matriz de Seleção de Procedimentos Padrão de Operação**.
3. Na janela Matriz de Seleção de Procedimento Padrão de Operação, para exibir a primeira linha, clique no ícone **Filtro**.

4. Determine qual campo de filtro a ser utilizado:
 - Categoria
 - Severidade
 - Urgência
 - Certeza
 - Nome do SOP
5. Escolha uma das opções a seguir:
 - No campo de filtro, pressione Enter para visualizar todas as entradas existentes relacionadas ao parâmetro escolhido ou ao nome do procedimento padrão de operação.
 - No campo de filtro, informe as primeiras letras de um valor a ser filtrado.
 - Se você estiver filtrando um valor de parâmetro, insira valores por meio da janela Selecionar Valor:
 - a. Ao lado do campo de filtro, clique no ícone **Selecionar Valor**.
 - b. Na janela Selecionar Valor, clique em um valor na lista para selecioná-lo.
 - Para selecionar o nome de um procedimento padrão de operação a ser filtrado na janela Procedimento Padrão de Operação:
 - a. Ao lado do campo de filtro **NOME DO SOP**, clique no ícone **Menu Detalhe** e, em seguida, clique em **Acessar Procedimento Padrão de Operação**.
 - b. Na janela Standard Operating Procedure, clique na guia **Lista**.
 - c. Em Planos de Tarefas SOP, no campo de filtro, insira as primeiras letras do nome de um procedimento padrão de operação.
 - d. Para visualizar os detalhes de um procedimento padrão de operação, clique no nome do procedimento padrão de operação na lista. Os detalhes são exibidos na guia **Standard Operating Procedure**.
 - e. Para retornar o nome do procedimento padrão de operação exibida na guia **Standard Operating Procedure**, no canto superior direito, clique em **Retornar Com Valor**. O nome é exibido no campo de filtro **Nome do SOP** na matriz de seleção.
6. Para refinar mais a lista de entradas de critérios de seleção exibida, repita a Etapa 5 usando um dos outros campos de filtro listados na Etapa 4.

Definindo Parâmetros na matriz de seleção de procedimento padrão de operação

Na matriz de seleção de procedimento padrão de operação, defina os parâmetros de evento que determinam se um procedimento padrão de operação é selecionado para um evento específico.

Sobre Esta Tarefa

Não é possível salvar uma matriz de seleção de procedimento padrão de operação que contenha duas linhas de critérios de seleção idênticos. Se apropriado, uma mensagem de validação será exibida informando que você deve definir um conjunto exclusivo de critérios de seleção para um procedimento padrão de operação.

Procedimento

1. Para abrir o portlet Procedimentos Padrão de Operação na interface de Administração do WebSphere Portal, clique em **Intelligent Operations > Ferramentas de Customização > Procedimentos Padrão de Operação**.
2. Para abrir o aplicativo Matriz de Seleção de Procedimento Padrão de Operação, clique em **Matriz de Seleção de Procedimentos Padrão de Operação**.
3. Na janela Matriz de Seleção de Procedimento Padrão de Operação, para exibir a primeira linha, clique no ícone **Filtro**.
4. Na janela **Matriz de Seleção de SOP**, no canto inferior direito, clique em **Nova Linha**. Uma nova linha é anexada à matriz de seleção.

5. Informe valores para cada um dos parâmetros a seguir:

- Categoria
- Severidade
- Urgência
- Certeza

Use uma das opções a seguir para inserir valores para cada parâmetro:

- Para inserir valores por meio da janela Selecionar Valor:
 - a. Ao lado do campo de parâmetro, clique no ícone **Selecionar Valor**.
 - b. Na janela Selecionar Valor, clique em um valor na lista para selecioná-lo.
- Para inserir o nome do parâmetro manualmente:
 - a. Insira as primeiras letras do valor do parâmetro no campo.
 - b. Pressione a guia TAB para mover o cursor para o próximo campo e o valor do parâmetro será preenchido automaticamente.

6. Para inserir o nome do procedimento padrão de operação no campo **Nome do SOP**, escolha uma das opções a seguir:

- Para inserir o nome do procedimento padrão de operação por meio da janela Procedimento Padrão de Operação:
 - a. Ao lado do campo **NOME DO SOP**, clique no ícone **Menu Detalhe** e, em seguida, clique em **Acessar Procedimento Padrão de Operação**.
 - b. Na janela Procedimento Padrão de Operação, clique na guia **Lista**.
 - c. Em Planos de Tarefa do SOP, no campo de filtro, insira as primeiras letras do nome de um procedimento padrão de operação.
 - d. Para visualizar os detalhes de um procedimento padrão de operação, clique no nome do procedimento padrão de operação na lista. Os detalhes são exibidos na guia **Procedimento Padrão de Operação**.
 - e. Para retornar o nome do procedimento padrão de operação que é exibido na guia **Procedimento Padrão de Operação**, no canto superior direito, clique em **Retornar Com Valor**. O nome é exibido no campo **Nome do SOP** da nova linha na matriz de seleção.
- Informe o nome do procedimento padrão de operação manualmente.

7. Clique no ícone **Salvar matriz**.

Gerenciamento de recursos

Gerenciar Recursos no Tivoli Service Request Manager.

Sincronizando os Recursos de Amostra para o Banco de Dados do IBM Intelligent Operations Center

Se quiser utilizar os recursos de amostra instalados com o IBM Intelligent Operations Center, você deve sincronizá-los com o banco de dados do IBM Intelligent Operations Center manualmente.

Procedimento

1. Efetue logon no Tivoli Service Request Manager Start Center como um administrador.
2. Clique em **Acessar > Ativos > Recursos IOC(IntOpCtr)**.
3. Para visualizar todos os recursos do IBM Intelligent Operations Center de amostra, na janela Recursos (IntOpCtr), na guia **Lista**, clique no campo **Recurso** e pressione a tecla Enter.
4. Para cada recurso que deseja sincronizar com o banco de dados do IBM Intelligent Operations Center, atualize o recurso. Por exemplo, modifique o **Descrição** e salve a mudança.
5. Verifique se os recursos sincronizados estão listados nas seguintes tabelas de banco de dados do IBM Intelligent Operations Center:
 - IOC.RESOURCE

- IOC.RESOURCE_X_CAPABILITY

O que Fazer Depois

Se os recursos de amostra não são corretamente sincronizados para o banco de dados do IBM Intelligent Operations Center, revise o arquivo de log da análise do Tivoli Netcool/Impact. Insira o seguinte comando:

```
tail -f /opt/IBM/netcool/omnibus/log/ioc_xml.log
```

Também, revise o arquivo de log de política do Tivoli Netcool/Impact em `/opt/IBM/netcool/impact/log/NCI_policylogger.log`. Para ativar o arquivo de log de política do Tivoli Netcool/Impact, execute as seguintes etapas:

1. Efetue logon no console administrativo do Tivoli Netcool/Impact em `http://event_server:9080/nci`. Efetue logon como o usuário `admin` com a senha `netcool`.
2. Clique em **Projeto IOC**.
3. Na guia **Serviços**, clique em **Criador de Logs de Política**.
4. Para **Log de Nível Mais Alto**, mude o valor de `0` para `3`.
5. Salve as mudanças.
6. Execute o teste.

Para obter mais informações sobre arquivos de log de resolução de problemas, consulte o link no final do tópico.

Conceitos relacionados:

“Arquivos de Log do Servidor de eventos” na página 296

Utilize os procedimentos a seguir para ativar os rastreios e visualizar logs para alguns dos sistemas no .

Criando ou Modificando as Categoria de Evento para Mapeamento de Capacidade

Os recursos são exibidos no portlet do Mapa, dependendo da categoria do evento selecionado e das capacidades de recursos mapeados. Antes de criar um recurso, mapeie a capacidade do recurso para a categoria de evento apropriada.

Antes de Iniciar

Para garantir que as capacidade do recurso são atualizadas, você deve configurar o valor da senha para o usuário administrativo do Tivoli Service Request Manager, por exemplo, `maxadmin`, para `maxadmin`.

Sobre Esta Tarefa

Mapear uma capacidade de recurso para uma categoria de evento garante que, ao visualizar recursos adjacentes no portlet IBM Intelligent Operations Center Detalhes, os recursos apropriados são exibidos no portlet Mapa. Por exemplo, se você visualizar recursos adjacentes para uma categoria de evento meteorológico, um warehouse que armazena sacos de areia é exibido, no qual o warehouse é o tipo de recurso e os sacos de areia são uma capacidade mapeada do warehouse.

Procedimento

1. Efetue logon no Tivoli Service Request Manager Start Center como um administrador.
2. Clique em **Acessar > Configuração do Sistema > Configuração de Plataforma > Domínios**.
3. Escolha a opção adequada:
 - Para criar uma categoria de evento para mapeamento de capacidade, clique em **Nova Linha** e insira os detalhes apropriados nos campos.
 - Para modificar uma categoria de evento existente para mapeamento de capacidade, use o campo de filtro para exibir os mapeamentos de categoria de evento apropriados, depois clique na linha da qual deseja editar e modificar os detalhes.

- Para excluir uma categoria de evento existente para mapeamento de capacidade, use o campo de filtro para exibir os mapeamentos de categoria de evento apropriados, depois clique no ícone **Marcar Linha para Exclusão** no final da linha que deseja excluir.
4. Clique no ícone **Salvar Domínio**.
 5. Verifique se os recursos sincronizados estão listados nas seguintes tabelas de banco de dados do IBM Intelligent Operations Center:
 - IOC.RESOURCE
 - IOC.RESOURCE_X_CAPABILITY

Resultados

Novos recursos cuja capacidade seja mapeada para a categoria de evento do evento atualmente selecionado são exibidos no portlet IBM Intelligent Operations Center Mapa imediatamente. Recursos atualizados cuja capacidade seja mapeada para a categoria de evento do evento atualmente selecionado são exibidos somente após a página que contém o portlet IBM Intelligent Operations Center Mapa ser recarregada.

O que Fazer Depois

- Se os recursos mapeados não estiverem atualmente listados no banco de dados do IBM Intelligent Operations Center, revise o arquivo de log do Tivoli Netcool/Impact. Insira o seguinte comando:

```
tail -f /opt/IBM/netcool/omnibus/log/ioc_xml.log
```

Para obter mais informações sobre arquivos de log de resolução de problemas, consulte o link no final do tópico.

- Se desejar mapear mais de duas categorias de evento para uma capacidade, use um comando do DB2 para fazer o mapeamento. Utilize as seguintes etapas:
 1. Para efetuar logon no servidor de dados como um usuário do banco de dados do Tivoli Service Request Manager, insira o seguinte comando: `su-db2inst6`
 2. Para conectar-se ao banco de dados do IBM Intelligent Operations Center, insira o seguinte comando: `db2 connect to maximo`
 3. Para mapear uma categoria de evento para uma capacidade, insira o seguinte comando:

```
insert into synonymdomain
(domainid, maxvalue, value, description, defaults, synonymdomainid, valueid) values
('PLUSICATCPLMAP', 'category_name', 'capability_name',
'mapping_description', 0, NEXTVAL FOR synonymdomainseq,
'PLUSICATCPLMAP|mapping_key');
```

No comando anterior, substitua as variáveis *category_name*, *capability_name*, *mapping_description* e *mapping_key* com valores apropriados. Para *mapping_key*, crie um valor apropriado. Por exemplo, o seguinte comando mapeia a categoria de evento Met para a capacidade COT, e designa o valor METCOT para *mapping_key*.

```
insert into synonymdomain
(domainid, maxvalue, value, description, defaults, synonymdomainid, valueid) values
('PLUSICATCPLMAP', 'Met', 'COT', 'Has cots', 0, NEXTVAL FOR synonymdomainseq,
'PLUSICATCPLMAP|METCOT');
```

4. Para concluir a gravação para o banco de dados, insira o seguinte comando: `db2 commit;`

Criando um Recurso

Crie um recurso na interface com o usuário no Tivoli Service Request Manager.

Antes de Iniciar

Certifique-se de que a capacidade do novo recurso seja mapeada para uma categoria, para que o recurso seja exibido no portlet do Mapa na interface com o usuário do IBM Intelligent Operations Center.

Procedimento

1. Efetue login no Tivoli Service Request Manager Start Center como um administrador.
2. Clique em **Acessar > Ativos > Recursos (IntOpCtr)**.
3. Na janela Recursos IOC, clique no ícone **Novo Recurso**.
4. Na guia **Recurso**, insira os seguintes detalhes:

Recurso

Um ID exclusivo para o recurso.

Descrição Longa

O nome do recurso exibido na interface com o usuário do IBM Intelligent Operations Center, no portlet do Detalhes, na guia **Recursos**.

Descrição Resumida

Uma breve descrição do recurso exibido como ajuda instantânea se passar o mouse sobre o recurso no portlet do Mapa na interface com o usuário do IBM Intelligent Operations Center.

Latitude

A posição latitudinal do local do recurso.

Longitude

A posição longitudinal do local do recurso.

5. Clique na guia **Capacidades**.
6. Próximo ao campo **Classificação**, clique no ícone **Menu Detalhe**, e em seguida clique em **Classificar**.
7. Na janela Classificar, navegue pela árvore de navegação para localizar a classificação do recurso apropriado.
8. Clique em um nome de classificação; por exemplo, um armazém. Uma tabela de capacidades associadas à classificação é exibida na janela Recursos IOC.
9. Na tabela Capacidade, clique na capacidade e insira o **Valor Numérico**.
10. Clique no ícone **Salvar Recurso**.

O que Fazer Depois

Verifique se o recurso está listado nas seguintes tabelas de banco de dados do IBM Intelligent Operations Center:

- IOC.RESOURCE
- IOC.RESOURCE_X_CAPABILITY

Tarefas relacionadas:

“Criando ou Modificando as Categoria de Evento para Mapeamento de Capacidade” na página 133
Os recursos são exibidos no portlet do Mapa, dependendo da categoria do evento selecionado e das capacidades de recursos mapeados. Antes de criar um recurso, mapeie a capacidade do recurso para a categoria de evento apropriada.

Visualizando, Atualizando ou Excluindo um recurso

Acesse a interface com o usuário do Tivoli Service Request Manager por meio da interface com o usuário do IBM Intelligent Operations Center e visualize, atualize ou exclua os recursos.

Sobre Esta Tarefa

O procedimento a seguir descreve como acessar dados do recurso no Tivoli Service Request Manager por meio da interface com o usuário do IBM Intelligent Operations Center. Para acessar os dados de recurso diretamente por meio do Tivoli Service Request Manager, utilize as seguintes etapas:

1. Efetue login no Tivoli Service Request Manager Start Center.
2. Clique em **Acessar > Ativos > Recursos (IntOpCtr)**.

3. Para listar todos os recursos do IBM Intelligent Operations Center, na janela Recursos (IntOpCtr), na guia **Lista**, clique no campo **Recurso** e pressione a tecla Enter.
4. Na lista, clique na linha para o recurso que deseja modificar.
5. Clique na guia **Recurso** ou na guia **Capacidades**, conforme apropriado.

Procedimento

1. Abra a interface com o usuário do IBM Intelligent Operations Center.
2. No portlet Detalhes, na guia **Eventos e Incidentes**, identifique um evento na lista cujos recursos deseja visualizar, atualizar ou excluir.
3. Para visualizar uma lista de recursos na proximidade do evento, clique com o botão direito do mouse em **Visualizar Recursos Próximos** e selecione o raio da área em que deseja manter o foco. Uma lista de recursos é exibida na guia **Recursos**.
4. Na guia **Recursos**, clique com o botão direito do mouse em uma linha na lista de recursos e selecione uma opção do menu:
 - Para atualizar as informações sobre um recurso, clique em **Atualizar**.
 - Para remover um recurso da lista e do mapa, clique em **Excluir**.
 - Para visualizar as informações sobre um recurso, clique em **Propriedades**.

Qualquer que seja a opção, o recurso será exibido em Tivoli Service Request Manager, na guia **Recurso**.

5. Em Tivoli Service Request Manager, na guia **Recurso**, é possível escolher as seguintes ações sobre o recurso:
 - Atualize o nome do recurso, descrições, latitude e longitude.
 - Para excluir o recurso, selecione **Excluir Recurso** na lista **Selecionar Ação**.
6. Na guia **Capacidades**, é possível escolher as seguintes ações sobre as capacidades do recurso:
 - Clique nas capacidades apropriadas e modifique o **Valor Numérico**. Para uma capacidade a ser mapeada para o recurso, o valor deve ser 1 ou mais.
 - Selecione uma capacidade, e em seguida clique no ícone **Marcar Linha para Exclusão** no final da linha.
7. Ao concluir a atualização do recurso, clique no ícone **Salvar Recurso**.

O que Fazer Depois

Para conseguir visualizar os dados do recurso atualizado na interface com o usuário do IBM Intelligent Operations Center, reconfigure o Mapa. Em seguida, revise os recursos para um evento por meio do portlet do Detalhes.

Criando um Tipo de Recurso

Crie um tipo de recurso no Tivoli Service Request Manager.

Sobre Esta Tarefa

É possível definir uma hierarquia de tipos de recursos, assim, os tipos de recurso podem ter tipos de recurso filho e assim por diante.

Procedimento

1. Efetue logon no Tivoli Service Request Manager Start Center como um administrador.
2. Clique em **Acessar > Administração > Classificações**.
3. Para visualizar todos os tipos de recurso existentes do IBM Intelligent Operations Center, na guia **Lista**, no campo **Descrição**, insira RESOURCE. Todos os tipos de recurso na hierarquia serão exibidos.
4. Clique no tipo de recurso, ou tipo de recurso filho, para o qual deseja criar um tipo de recurso filho. Os detalhes da classificação para o pai do novo tipo de recurso são exibidos na guia **Classificações**.

5. Na guia **Classificações**, em Filhos, clique em **Nova Linha**.
6. Na linha em branco que é anexada à lista, insira os seguintes valores para o novo tipo de recurso:
 - a. Na coluna **Classificação**, insira um nome.
 - b. Na coluna **Classificação Desc.**, insira uma descrição.
 - c. Para evitar que o nome do tipo de recurso seja mudado quando o tipo de recurso for salvo, limpe a caixa de seleção **Gerar Descrição**.
7. Clique no ícone **Salvar Classificação**.
8. Para incluir um gráfico para o novo tipo de recurso, execute as seguintes subetapas:
 - a. Salve cópias do gráfico em dois tamanhos em formato PNG. O ícone gráfico maior é exibido no portlet Mapa, e o ícone gráfico menor é exibido na lista de eventos no portlet Detalhes.

Tamanho 24 pixels x 24 pixels
Por exemplo, *new_resource_24.png*

Tamanho 16 pixels x 16 pixels
Por exemplo, *new_resource_16.png*
 - b. Copie cada arquivo PNG para o diretório apropriado no servidor de aplicativos:
 - /opt/IBM/WebSphere/wp_profile/installedApps/ICPWPSNode/iss_portal_ear.ear/iss_common_widgets_web.war/images/resource_icons/PNG-24x24/Normal_State
 - /opt/IBM/WebSphere/wp_profile/installedApps/ICPWPSNode/iss_portal_ear.ear/iss_common_widgets_web.war/images/resource_icons/PNG-16x16/Normal_State
 - c. Verifique se cada ícone é exibido corretamente no link do navegador da web apropriado:
 - http://appserver/ibm/iss/common/widgets/images/resource_icons/PNG-24x24/Normal_State/new_resource_24.png
 - http://appserver/ibm/iss/common/widgets/images/resource_icons/PNG-16x16/Normal_State/new_resource_16.png

Incluindo uma Capacidade a um Tipo de Recurso

Crie uma capacidade no Tivoli Service Request Manager.

Procedimento

1. Efetue logon no Tivoli Service Request Manager Start Center como um administrador.
2. Clique em **Acessar > Administração > Classificações**.
3. Para visualizar todas as classificações existentes IBM Intelligent Operations Center, na guia **Lista**, filtre por RECURSO.
4. Clique na guia **Classificações**.
5. Em Filhos, na lista, clique no tipo de recurso para o qual deseja incluir uma capacidade.
6. Para evitar que o nome do tipo de recurso seja mudado quando o tipo de recurso for salvo, limpe a caixa de seleção **Gerar Descrição**.
7. Em Atributos, clique em **Nova Linha**.
8. Insira os detalhes para a nova capacidade:
 - a. Para **Atributo**, insira um nome.
 - b. No campo à direita do campo **Atributo**, insira uma descrição.
 - c. Para inserir um valor para o **Tipo de Dados**, clique no ícone Selecionar Valor e escolha um valor na janela Selecionar Valor.
 - d. Para especificar que recursos filhos herdam essa capacidade, selecione **Aplicar Hierarquia Descendente?**
9. Clique no ícone **Salvar Classificação**.

procedimentos padrão de operação, fluxos de trabalho de Amostra e Recursos

Os procedimentos padrão de operação, fluxos de trabalho de amostra e recursos são fornecidos ao instalar o IBM Intelligent Operations Center Versão 1.5.

Procedimentos Padrão de Operação

Os três procedimentos padrão de operação seguintes são fornecidos:

PLUSIMITIG: Preparação inicial para tempo severo (mitigar)

PLUSIMITIG contém as seguintes etapas:

1. Validar a severidade do tempo. Etapa manual não associada ao fluxos de trabalho.
2. Aumentar a classificação de severidade se necessário. Etapa manual não associada ao fluxos de trabalho.

PLUSIPREPA: Preparar para retirada do clima severo (Preparar)

PLUSIPREPA contém as seguintes etapas:

1. Preparar abrigos de retirada. Etapa manual associada ao PLUSISOP00 do fluxo de trabalho.
2. Identificar recursos de suporte de retirada. Etapa manual associada ao PLUSISOP00 do fluxo de trabalho.
3. Avaliar a disponibilidade de recursos de suporte. Etapa manual associada ao PLUSISOP00 do fluxo de trabalho.

PLUSIRESPO: Evacuar áreas de afetadas (Responder e Recuperar)

PLUSIRESPO contém as seguintes etapas:

1. Aprovar retirada diretiva. Etapa manual não associada ao fluxos de trabalho.
2. Certifique-se de que rotas de saída estejam limpas. Etapa manual não associada ao fluxos de trabalho.

O matriz de seleção de procedimento padrão de operação é preenchido com dados que acionam a seleção dos três procedimentos padrão de operação, conforme mostrado na seguinte tabela:

Tabela 35. Matriz de Seleção de Procedimento Padrão de Operação data de amostra

Categoria	Gravidade	Urgência	Certeza	Nome do Procedimento Padrão de Operação
Met	Grave	Futura	Observada	PLUSIMITIG
Met	Grave	Futura	Provável	PLUSIMITIG
Met	Extrema	Futura	Observada	PLUSIPREPA
Met	Extrema	Futura	Provável	PLUSIPREPA
Met	Extrema	Imediato	Observada	PLUSIRESPO

Sample fluxo de trabalho

Há um fluxo de trabalho de amostra:

PLUSISOP00: Conclua a ação da atividade

O PLUSISOP00 fluxo de trabalho aciona uma ação para mudar o status de uma atividade paraCOMP (concluída).

O PLUSISOP00 fluxo de trabalho está associado a cada uma das etapas do PLUSIPREPA de amostra do procedimento padrão de operação. Se iniciar uma das etapas, o status da etapa será automaticamente marcado como concluído.

Recursos de Amostra

A tabela a seguir lista os recursos de amostra, fornecidas no domínio: PLUSICATCPLMAP:

Tabela 36. Recursos de Amostra

Recurso	Descrição	Tipo de recurso
BASCOMEYE	Bascombe Eye Institute	RESOURCES\HOSPITAL
BLUEFISHW	Blue Fish Warehouse	RESOURCES\WAREHOUSE
DOCTORSH	Doctor's Hospital	RESOURCES\HOSPITAL
MERYCYH	Mercy Hospital	RESOURCES\HOSPITAL
MAMICHILD	Miami Children's Hospital	RESOURCES\HOSPITAL
SFFOODDIST	South Florida Food Distribution	RESOURCES\WAREHOUSE
TITLEASING	Tropical Trailer Leasing Corporation	RESOURCES\WAREHOUSE
UNIMIAMI	University of Miami Hospital	RESOURCES\HOSPITAL
WTDCDIST	WTDC Distribution Center Miami	RESOURCES\WAREHOUSE

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 7

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 no seu fuso horário no formato especificado na tabela de banco de dados de propriedades do sistema. 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 178

A tabela de propriedades de sistema do IBM Intelligent Operations Center armazena dados de configuração do IBM Intelligent Operations Center.

“Utilizando CAP para Ocorrências KPI” na página 96

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).

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 estão listados nas seções a seguir.

Portlets do Usuário

A tabela a seguir lista os portlets do usuário inclusos no IBM Intelligent Operations Center. A tabela também indica em quais visualizações de página de amostra cada portlet está disponível.

É possível customizar os portlets. Para obter informações adicionais, consulte o link no final do tópico.

Tabela 37. Portlets do Usuário no IBM Intelligent Operations Center

Portlet	Descrição	Visualizações de páginas de amostra
“Contatos” na página 271	O portlet Contatos pode exibir uma lista de seus contatos organizados por categoria. É possível organizar os contatos em categorias baseadas nas pessoas com as quais você precisa se comunicar. Por exemplo, é possível ter uma categoria para contatos de trabalho geral e outra categoria para contatos de trabalho do projeto. Com o portlet Contatos, é possível comunicar-se com pessoas e modificar seu status online, contatos ou grupos.	<ul style="list-style-type: none"> • “Visualização Supervisor: Status” na página 267 • “Visualização Supervisor: Operações” na página 268 • “Visualização Operator: Operações” na página 269
“Detalhes” na página 272	O portlet Detalhes é um portlet de lista interativo. Todos os eventos que você está autorizado a visualizar estão visíveis na lista de eventos e em qualquer portlet de mapa vinculado ao portlet Detalhes.	<ul style="list-style-type: none"> • “Visualização Supervisor: Operações” na página 268 • “Visualização Operator: Operações” na página 269 • “Visualização Mapa de Localização” na página 270
“Drill Down de Key Performance Indicator” na página 275	Para focar em uma categoria de KPI específica no portlet Drill Down de Key Performance Indicator, clique na categoria no portlet Status. Esta categoria é então exibida por si própria no portlet Drill Down de Key Performance Indicator. É possível usar a lista para inspecionar os KPIs subjacentes até acessar os detalhes do KPI que causaram a mudança de status.	<ul style="list-style-type: none"> • “Visualização Supervisor: Status” na página 267
“Mapa de Localização” na página 276	Utilize o portlet do Mapa de Localização para ver os eventos marcados em um mapa de localização. Um mapa de localização no IBM Intelligent Operations Center é um mapa ou plano com áreas pré-definidas para interação, por exemplo, áreas de assentos em um grande estádio esportivo.	<ul style="list-style-type: none"> • “Visualização Mapa de Localização” na página 270

Tabela 37. Portlets do Usuário no IBM Intelligent Operations Center (continuação)

Portlet	Descrição	Visualizações de páginas de amostra
“Mapa” na página 279	<p>No portlet Mapa:</p> <p>Um mapa da região geográfica, com marcadores de eventos e de recursos.</p> <p>Um formulário de filtro para selecionar as categorias dos eventos a serem mostrados no mapa e nos portlets vinculados ao portlet Mapa.</p> <p>Um formulário de filtro para selecionar as capacidades dos recursos a serem mostrados no mapa e na guia Recursos no portlet vinculado Detalhes. Para visualizar este formulário, primeiro selecione Visualizar Recursos Próximos no portlet Detalhes.</p>	<ul style="list-style-type: none"> • “Visualização Supervisor: Operações” na página 268 • “Visualização Operator: Operações” na página 269
“Minhas Atividades” na página 284	<p>Um usuário que está conectado pode visualizar as atividades designadas a ele no portlet Minhas Atividades. No portlet Minhas Atividades, as atividades são agrupadas pelos procedimentos padrão de operação pai. Cada procedimento padrão de operação corresponde a um evento individual.</p>	<ul style="list-style-type: none"> • “Visualização Supervisor: Status” na página 267 • “Visualização Supervisor: Operações” na página 268 • “Visualização Operator: Operações” na página 269
“Notificações” na página 286	<p>O portlet Notificações 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>	<ul style="list-style-type: none"> • “Visualização Supervisor: Status” na página 267 • “Visualização Supervisor: Operações” na página 268 • “Visualização Operator: Operações” na página 269
“Relatórios” na página 288	<p>Use o portlet Relatórios para visualizar um relatório de eventos como um gráfico. O portlet fornece opções para agrupar eventos e é possível escolher eventos por uma data ou intervalo de data específico. Estes relatórios ajudam a planejar respostas a eventos atuais e futuros.</p>	<ul style="list-style-type: none"> • “Supervisor: Relatórios ” na página 270 • “Operator: Relatórios” na página 270
“Status” na página 290	<p>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.</p>	<ul style="list-style-type: none"> • “Visualização Supervisor: Status” na página 267

Tarefas relacionadas:

“Customizando os portlets” na página 145

Como administrador, é possível alterar as configurações de portlet para customizar um portlet.

Miniportais Administrative

A tabela a seguir lista os portlets administrativos inclusos no no IBM Intelligent Operations Center. Os portlets administrativos estão na página de Administração.

Tabela 38. Portlets Administrativos no IBM Intelligent Operations Center

Portlet	Descrição
“Sobre” na página 195	Use o portlet Sobre para visualizar detalhes da versão do IBM Intelligent Operations Center e IBM Smarter Cities Software Solutions integrado que você instalou. Também é possível visualizar detalhes de quaisquer atualizações aplicadas desde sua instalação.
“Consoles de Administração” na página 203	Utilize o portlet do Consoles de Administração para administrar os serviços fornecidos pela solução.
“Verificando os Componentes” na página 210	A ferramenta Verificação do Sistema testa componentes dentro do IBM Intelligent Operations Center para determinar se eles estão acessíveis e operacionais.
“Resumo de Permissões do Usuário” na página 79	O portlet Resumo de Permissões do Usuário exibe detalhes de uma associação ao grupo e permissões concedidas a usuários.
“Principais Indicadores de Desempenho” na página 168	No portlet do Principais Indicadores de Desempenho é possível visualizar, alterar, copiar, criar e excluir KPIs. Também é possível customizar as hierarquias de KPI exibidos no Status e nos portlets do Drill Down de Key Performance Indicator.
“Gerenciador de Mapa de Localização” na página 176	Use o portlet Gerenciador de Mapa de Localização para customizar o portlet Mapa de Localização.
“Procedimentos Padrão de Operação” na página 127	É possível definir o procedimentos padrão de operação e atividades para gerenciar eventos que chegam ao IBM Intelligent Operations Center. Use o portlet Procedimentos Padrão de Operação para acessar os aplicativos procedimento padrão de operação, matriz de seleção de procedimento padrão de operação e designer de fluxo de trabalho no Tivoli Service Request Manager.
“Script do Evento” na página 107	Use o portlet Script do Evento para gravar um script para criar uma lista sequencial de eventos a serem publicados em intervalos de tempo predefinidos.
“Publicador de Amostra” na página 103	O portlet Publicador de Amostra é uma ferramenta de teste automatizada destinada a um administrador que gerencia ou verifica a solução. Um administrador pode usar o portlet Publicador de Amostra como um aplicativo cliente para testar a publicação de mensagens do CAP no IBM Intelligent Operations Center. O portlet Publicador de Amostra pode eliminar o requisito para criar manualmente um aplicativo cliente de teste.

Tarefas relacionadas:

“Customizando os portlets”

Como administrador, é possível alterar as configurações de portlet para customizar um portlet.

Criando ou Customizando uma Página

É possível criar novas páginas para que sejam incluídas no IBM Intelligent Operations Center e especificar quais portlets exibir nessas páginas. É possível customizar a aparência e o layout dos portlets incluídos em cada página.

Sobre Esta Tarefa

Use a interface com o usuário do WebSphere Portal para customizar páginas e portlets.

Nota: Ao criar ou editar um layout da página, certifique-se de que os portlets estejam operando corretamente, aderindo às seguintes regras:

- Os portlets Mapa e Detalhes devem estar no mesmo grupo e na mesma página para permitir a inclusão de um evento a partir do portlet Mapa.
- Os portlets Minhas Atividades e Detalhes devem estar no mesmo grupo e na mesma página para permitir a solicitação de detalhes do evento a partir do portlet Minhas Atividades ou a solicitação de detalhes do Procedimento Padrão de Operação a partir do portlet Detalhes.

Procedimento

1. Para abrir o WebSphere Portal, clique na guia **Administração**.
2. No WebSphere Portal, clique em **Interface com o Usuário do Portal**.
3. Clique na opção necessária:
 - Para trabalhar com as páginas ou criar novas, clique em **Gerenciar Páginas**.
 - 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 7

Customizando os portlets

Como administrador, é possível alterar as configurações de portlet para customizar um portlet.

Sobre Esta Tarefa

Há dois modos possíveis de customização, cada um alterando as configurações de portlet para todos os usuários:

- **Editar Configurações Compartilhadas** altera o portlet apenas para a instância do portlet em que você está ao alterar as configurações.
- **Configurar** altera as configurações globais do portlet para todas as instâncias do portlet sempre que elas ocorrem.

Os modos de customização que estão disponíveis dependem das permissões associadas ao seu ID do usuário. As configurações globais são substituídas por configurações compartilhadas.

Procedimento

1. Efetue login no portal de soluções como administrador.
2. Clique no canto superior direito do portlet para visualizar o menu do portlet.
3. Clique em **Editar Configurações Compartilhadas** ou em **Configurar**.
4. Insira as configurações nos campos fornecidos.
5. Para fechar a janela de configurações, clique em um dos botões:
 - **Salvar** para salvar as mudanças.
 - **Cancelar** para cancelar as mudanças.
 - **Reconfigurar para Padrões** para reverter para as configurações globais padrão.

Resultados

Todas as novas configurações salvas entrarão em vigor na próxima vez que o portlet for atualizado. Os valores da configuração global padrão fornecidos com o IBM Intelligent Operations Center serão utilizados para qualquer parâmetro que não foi reconfigurado.

Configurações do Portlet do Sobre

Customize o portlet do Sobre alterando as configurações nos campos da janela **Configurações Compartilhadas**.

Parâmetros de Customização

Os campos da janela **Configurações Compartilhadas** contêm os valores dos parâmetros de customização para o portlet do Sobre. Os parâmetros de customização são descritos na tabela a seguir.

Tabela 39. Parâmetros de Customização do Portlet do Sobre

Parâmetro	Descrição	Valor Padrão
Altura do portlet	Número de pixels indicando a altura padrão do portlet.	400
Altura máxima do portlet	Número de pixels indicando a altura máxima do portlet.	600

Conceitos relacionados:

“Sobre” na página 195

Use o portlet Sobre para visualizar detalhes da versão do IBM Intelligent Operations Center e IBM Smarter Cities Software Solutions integrado que você instalou. Também é possível visualizar detalhes de quaisquer atualizações aplicadas desde sua instalação.

Configurações do Portlet do Consoles de Administração

Customize o portlet do Consoles de Administração alterando as configurações nos campos da janela **Configurações Compartilhadas**.

Parâmetros de Customização

Os campos da janela **Configurações Compartilhadas** contêm os valores dos parâmetros de customização para o portlet do Consoles de Administração. Os parâmetros de customização são descritos na tabela a seguir.

Tabela 40. Parâmetros de Customização do Consoles de Administração

Parâmetro	Descrição	Valor Padrão
JSP de ajuda padrão	Nome do arquivo de ajuda JSP a ser mostrado quando a ajuda for selecionada no menu do portlet.	AdministrationConsolePortletHelp

Tabela 40. Parâmetros de Customização do Consoles de Administração (continuação)

Altura do portlet	Número de pixels indicando a altura padrão do portlet.	400
Altura máxima do portlet	Número de pixels indicando a altura máxima do portlet.	450
Título do Portlet	Título para substituir o título fornecido com a solução.	Se você não inserir um valor para esse parâmetro, o título fornecido pela solução será exibido, que é Consoles de Administração.
Pacote de Recursos	Local do pacote configurável de recursos que você fornece como uma origem para o valor de propriedades, por exemplo, título do portlet. Esse local é necessário se você deseja especificar o título como uma chave da propriedade em um pacote configurável de recursos que você fornece. Se nenhum pacote configurável for especificado, então a chave não será procurada e o título será exibido conforme fornecido pela solução.	Não há nenhum pacote configurável de recursos padrão.

Conceitos relacionados:

“Consoles de Administração” na página 203

Utilize o portlet do Consoles de Administração para administrar os serviços fornecidos pela solução.

Configurações do Portlet do Contatos

Customize o portlet do Contatos alterando as configurações nos campos da janela **Configurações Compartilhadas**.

Parâmetros de Customização

Os campos da janela **Configurações Compartilhadas** contêm os valores dos parâmetros de customização para o portlet do Contatos. Os parâmetros de customização são descritos na tabela a seguir.

Tabela 41. Parâmetros de Customização do Contatos

Parâmetro	Descrição	Valor Padrão
JSP de ajuda padrão	Nome do arquivo de ajuda JSP a ser mostrado quando a ajuda for selecionada no menu do portlet.	SametimeWebClientPortletHelp
Altura do portlet	Número de pixels indicando a altura padrão do portlet.	250
Altura máxima do portlet	Número de pixels indicando a altura máxima do portlet.	600
Título do Portlet	Título para substituir o título fornecido com a solução.	Se você não inserir um valor para esse parâmetro, o título fornecido pela solução será exibido será: Contatos.

Tabela 41. Parâmetros de Customização do Contatos (continuação)

Pacote de Recursos	Local do pacote configurável de recursos que você fornece como uma origem para o valor de propriedades, por exemplo, título do portlet. Esse local é necessário se você deseja especificar o título como uma chave da propriedade em um pacote configurável de recursos que você fornece. Se nenhum pacote configurável for especificado, então a chave não será procurada e o título será exibido conforme fornecido pela solução.	Não há nenhum pacote configurável de recursos padrão.
--------------------	---	---

Conceitos relacionados:

“Contatos” na página 271

Use o portlet Contatos para enviar mensagens instantâneas na solução.

Configurações do Portlet do Detalhes

Customize o portlet do Detalhes alterando as configurações nos campos da janela **Configurações Compartilhadas**.

Parâmetros de Customização

Os campos da janela **Configurações Compartilhadas** contêm os valores dos parâmetros de customização para o portlet do Detalhes. Os parâmetros de customização são descritos na tabela a seguir.

Tabela 42. Parâmetros de Customização para o Portlet do Detalhes

Nome do parâmetro	Descrição	Valor Padrão
Colunas	Especificações e ordem das colunas a serem exibidas na lista.	[{"id": "commonevents.headline", "width": "20"}, {"id": "commonevents.eventType", "width": "7"}, {"id": "commonevents.category", "width": "10"}, {"id": "commonevents.severity", "width": "10"}, {"id": "commonevents.certainty", "width": "10"}, {"id": "commonevents.urgency", "width": "10"}, {"id": "commonevents.sent", "width": "12", "sortPriority": "1", "sortAscending": "false"}]
Condições	Condições adicionais para a exibição de eventos ou recursos, as condições adicionais não podem ser substituídas usando a barra de ferramentas ou filtro de mapa. O padrão é que nenhuma condição adicional seja aplicada.	[]
JSP de ajuda padrão	Nome do arquivo de ajuda JSP a ser mostrado quando a ajuda for selecionada no menu do portlet.	CommonEventsPortletHelp
Ocultar Evento Incluir	Configuração true ou false para ocultar ou exibir o botão e opção de menu pop-up Incluir Eventos .	true
Ocultar Recurso Incluir	Configuração true ou false para ocultar ou exibir o botão Incluir Recursos na guia Recursos .	true

Tabela 42. Parâmetros de Customização para o Portlet do Detalhes (continuação)

Ocultar Eventos	Configuração true ou false para ocultar ou exibir a guia Eventos e Incidentes .	false
Ocultar Recursos	Configuração true ou false para ocultar ou exibir a guia Recursos .	false
Ocultar Barra de ferramentas	Configuração true ou false para ocultar ou exibir a barra de ferramentas no topo da lista.	true
Ignorar e Cancelar o Modo de Recurso	True ou false para reconhecer ou ignorar mensagem de cancelamento de modo de recurso de entrada do portlet Mapa.	false
Ignorar Criação de Evento	Configuração true ou false para reconhecer ou ignorar eventos criados no portlet do Mapa pelo usuário.	false
Ignorar Mudanças do Filtro de Eventos	Configuração true ou false para reconhecer ou ignorar seleções de filtro de eventos feitas no portlet do Mapa pelo usuário.	false
Ignorar de Seleção de Eventos	Configuração true ou false para reconhecer ou ignorar seleção de eventos recebidos feita no portlet do Mapa pelo usuário.	false
Ignorar Tarefas de Eventos	Configuração true ou false para reconhecer ou ignorar todas as seleções de menu pop-up.	false
Ignorar Reconfiguração de Mapa	Configuração true ou false para reconhecer ou ignorar um clique do botão Recursos no portlet.	false
Ignorar Filtro de Recursos Alterado	Configuração true ou false para reconhecer ou ignorar seleções do filtro de recursos feitas no portlet do Mapa pelo usuário.	false
Ignorar Tarefas de Recursos	Configuração true ou false para reconhecer ou ignorar todos os recursos das seleções de menu pop-up.	false
Identificador de grupo de portlet	Nome do grupo ao qual este portlet pertence. Um nome comum configura a comunicação entre os portlets Mapa, Detalhes e Mapa de Localização na mesma página.	default
Altura do portlet	Número de pixels indicando a altura padrão do portlet.	350
Altura máxima do portlet	Número de pixels indicando a altura máxima do portlet.	600
Título do Portlet	Título para substituir o título fornecido com a solução.	Se você não inserir um valor para esse parâmetro, o título fornecido pela solução e exibido será: Detalhes.

Tabela 42. Parâmetros de Customização para o Portlet do Detalhes (continuação)

Pacote de Recursos	Local do pacote configurável de recursos que você fornece como uma origem para o valor de propriedades, por exemplo, título do portlet. Esse local é necessário se você deseja especificar o título como uma chave da propriedade em um pacote configurável de recursos que você fornece. Se nenhum pacote configurável for especificado, então a chave não será procurada e o título será exibido conforme fornecido pela solução.	Não há nenhum pacote configurável de recursos padrão.
--------------------	---	---

Nota: A explicação do quê ocorre com o título do portlet quando você fornece um pacote configurável se aplica também ao título da coluna que se origina do mesmo pacote configurável de recursos.

Parâmetros de Colunas

O valor do parâmetro **colunas** é uma matriz de objetos JSON que podem ser configurados, conforme explicado no Tabela 43.

Tabela 43. Objetos no Valor dos Parâmetros de Colunas do Portlet do Detalhes

Objeto	Contém
ID	O identificador da coluna para indicar que a coluna deve ser exibida
mín.	Número de pixels indicando a largura da coluna
format	Sequência que representa o formato a ser usado para colunas de data e hora, a entrada substitui a configuração na tabela sysprop
sortAscending	<ul style="list-style-type: none"> • Valor de true para usar uma ordem de classificação ascendente nos itens da coluna • Valor de false para usar uma ordem de classificação descendente nos itens da coluna
sortPriority	<ul style="list-style-type: none"> • Número para indicar a prioridade de classificação dessa coluna entre todas as colunas; quando mais baixo o número, mais alta a prioridade • Nenhum valor, deixe em branco para usar a prioridade de classificação padrão das colunas • Valor -1 para desativar a prioridade de classificação padrão das colunas
título	Título da coluna, deixe em branco para usar o título de coluna padrão

As colunas são exibidas no portlet na mesma ordem que a fornecida nos objetos JSON que compõem o valor do parâmetro **colunas**. Somente as colunas com os identificadores da coluna especificados no valor serão exibidas, todas as outras estarão ocultas. Se o valor do parâmetro **colunas** for omitido, as colunas serão exibidas conforme indicado na configuração padrão, exibida na primeira linha do Tabela 42 na página 148.

Os valores possíveis para os identificadores da coluna estão descritos no Tabela 44 na página 151.

Tabela 44. Identificadores de Coluna Válidos para o Portlet Detalhes

Identificador de coluna	Descrição
commonevents.id	UUID fornecido para o evento no tabela de eventos comum
commonevents.externalEventId	Identificador de evento designado pelo requisitante do evento
commonevents.specification	Especificação de formato seguida pelo evento, por exemplo, CAP
commonevents.eventType	Valor não convertido para o código específico do sistema que indica se um evento foi escalado ou não: Evento ou Incidente
commonevents.sent	Horário enviado conforme fornecido pelo requisitante do evento
commonevents.headline	Texto do título descrevendo o evento
commonevents.hover text	Texto da ajuda instantânea descrevendo o evento
commonevents.category	Valor de categoria não convertido
commonevents.certainty	Valor de certeza não convertido
commonevents.severity	Valor de severidade não convertido
commonevents.urgency	Valor de urgência não convertido
commonevents.url	Endereço da web da URL para obter informações adicionais sobre o evento
commonevents.externalWorkOrderId	Identificador de ordem de serviço associado, geralmente o ID do Tivoli Service Request Manager procedimento padrão de operação
commonevents.areaId	Identificador de área do mapa de localização se o evento estiver vinculado a um mapa de localização
commonevents.largeIcon	Ícone usado para representar o evento no mapa
commonevents.largeHiliteIcon	Ícone usado quando o evento está destacado no mapa
commonevents.largeGreyIcon	Ícone usado quando o evento está desativado no mapa
commonevents.smallIcon	Ícone usado para o evento na lista
commonevents.user1	Valor configurado dentro da política do Tivoli Netcool/Impact
commonevents.user2	Valor configurado pelo usuário dentro da política do Tivoli Netcool/Impact
commonevents.user3	Valor configurado pelo usuário dentro da política do Tivoli Netcool/Impact
commonevents.user4	Valor configurado pelo usuário dentro da política do Tivoli Netcool/Impact
commonevents.user5	Valor configurado pelo usuário dentro da política do Tivoli Netcool/Impact

Parâmetro Condições

O valor do parâmetro **condições** é uma matriz de objetos JSON que podem ser configurados, conforme descrito no Tabela 45 na página 152.

Tabela 45. Objetos Dentro do Valor dos Parâmetros de Condições do Portlet do Detalhes

Tipo de objeto	Contém
seletor	Identificador da coluna à qual o operador se aplica
Operador	Operador SQL que é aplicado para os valores do seletor; as opções são: <ul style="list-style-type: none"> contains quando a coluna do seletor contém o valor, essa opção é o padrão equals quando a coluna do seletor é igual ao valor notEquals a coluna do seletor não é igual ao valor startsWith quando a coluna do seletor inicia com o valor endsWith quando a coluna do seletor termina com o valor
valores	Valor da coluna exibido, o valor deve ser o valor da chave não convertido conforme especificado na tabela anterior

Nota:

O parâmetro **conditions** define critérios além daqueles critérios fornecidos no filtro do portlet Mapa. Esses critérios substituem as condições especificadas no filtro do mapa ou na barra de ferramentas.

Nota: A barra de ferramentas é oculta por padrão.

Por exemplo, você precisa da seguinte mudança para as colunas:

- Exiba apenas as colunas **Enviado**, **Título**, **Categoria** e **URL**.
- Mude a largura da coluna **Enviado** para 12.
- Mude o formato da coluna **Enviado** para d-**MMM**-yyyy.
- Mude a prioridade da ordem de classificação da coluna **Enviado** para 2 e a coluna **Categoria** para 1.

Estas mudanças serão exibidas ao inserir o seguinte no campo **Colunas** e salvar suas preferências:

```
[{"id": "commonevents.sent", "width": "10", "format": "d-MMM-yyyy HH:mm", "sortPriority": "2"}, {"id": "commonevents.headline"}, {"id": "commonevents.category", "sortPriority": "1"}, {"id": "commonevents.url"}]
```

Por exemplo, você deseja exibir somente eventos que preenchem ambas as seguintes condições:

- Uma **Severidade** de Extremo ou Severa
- Um **Tipo de evento** de Incidente

Estas mudanças serão exibidas ao inserir o seguinte no campo **Condições** e salvar suas preferências:

```
[{"selector": "commonevents.severity", "operator": "equals", "values": ["Extreme", "Severe"]}, {"selector": "commonevents.eventType", "operator": "equals", "values": ["Incident"]}]
```

Conceitos relacionados:

“Detalhes” na página 272

Use o portlet Detalhes para visualizar, monitorar e gerenciar eventos no IBM Intelligent Operations Center.

Configurações do Portlet do Drill Down de Key Performance Indicator

Customize o portlet do Drill Down de Key Performance Indicator alterando as configurações nos campos da janela **Configurações Compartilhadas**.

Parâmetros de Customização

Os campos da janela **Configurações Compartilhadas** contêm os valores dos parâmetros de customização para o portlet do Drill Down de Key Performance Indicator. Os parâmetros de customização são descritos na tabela a seguir.

Tabela 46. Parâmetros de Customização do Drill Down de Key Performance Indicator

Parâmetro	Descrição	Valor Padrão
Colunas	Especificações e ordem das colunas a serem exibidas na lista.	[{"sortPriority": "1", "sortAscending": "true", "id": "kpi.NAME"}]
Customizar Cores de KPI	Cores usadas no portlet para indicar o status de KPIs, por exemplo, é possível inserir: <pre>{"acceptable": "#7f7f7f", "take_action": "#34333"}</pre> As cores que você inserir aqui substituirão as cores fornecidas pela solução.	{}
JSP de ajuda padrão	Nome do arquivo de ajuda JSP a ser mostrado quando a ajuda for selecionada no menu do portlet.	KpiDrillDownPortletHelp
Ativar Filtro de KPI	Configuração true ou false para ativar ou desativar um filtro de KPI de acordo com as informações na configuração do parâmetro filtro de KPI .	false
Ocultar barra de ferramentas	Configuração verdadeira ou falsa para ocultar ou exibir a barra de ferramentas na parte superior do portlet.	true
Filtro de KPI	IDs de KPIs a serem exibidos quando Ativar filtro de KPI estiver configurado para true para o portlet, por exemplo, é possível inserir : ["Transportation", "Airports", "Roads_and_Traffic", "Public_Safety", "Fire_Department", "Water", "Delayed_Flights", "Delayed_Flights_Airport_Two"]	[]
Identificador de grupo de portlet	Nome do grupo ao qual este portlet pertence. Um nome comum configura a comunicação entre os portlets Drill Down de Key Performance Indicator e Status na mesma página.	default
Altura do portlet	Número de pixels indicando a altura padrão do portlet.	350
Altura máxima do portlet	Número de pixels indicando a altura máxima do portlet.	600
Título do Portlet	Título para substituir o título fornecido com a solução.	Se você não inserir um valor para esse parâmetro, o título fornecido pela solução e exibido será: Drill Down de Key Performance Indicator.

Tabela 46. Parâmetros de Customização do Drill Down de Key Performance Indicator (continuação)

Pacote de Recursos	Local do pacote configurável de recursos que você fornece como uma origem para o valor de propriedades, por exemplo, título do portlet. Esse local é necessário se você deseja especificar o título como uma chave da propriedade em um pacote configurável de recursos que você fornece. Se nenhum pacote configurável for especificado, então a chave não será procurada e o título será exibido conforme fornecido pela solução.	Não há nenhum pacote configurável de recursos padrão.
--------------------	---	---

Nota: A explicação do quê ocorre com o título do portlet quando você fornece um pacote configurável se aplica também ao título da coluna que se origina do mesmo pacote configurável de recursos.

Parâmetros de Colunas

O valor do parâmetro **colunas** é uma matriz de objetos JSON que podem ser configurados, conforme explicado na tabela a seguir.

Tabela 47. Objetos no Valor dos Parâmetros de Colunas do Portlet do Drill Down de Key Performance Indicator

Objeto	Contém
sortPriority	<ul style="list-style-type: none"> Número para indicar a prioridade de classificação dessa coluna entre todas as colunas; quando mais baixo o número, mais alta a prioridade Nenhum valor, deixe em branco para usar a prioridade de classificação padrão da coluna -1 para desativar a prioridade de classificação padrão da coluna
sortAscending	<ul style="list-style-type: none"> true para usar uma ordem de classificação ascendente nos itens da coluna false para usar uma ordem de classificação descendente nos itens da coluna
ID	O identificador da coluna para indicar que a coluna deve ser exibida

As colunas são exibidas no portlet na mesma ordem que a fornecida nos objetos JSON que compõem o valor do parâmetro **colunas**. Somente as colunas com os identificadores da coluna especificados no valor serão exibidas, todas as outras estarão ocultas. Se o valor do parâmetro **colunas** for omitido, as colunas serão exibidas conforme indicado na configuração padrão, exibida na primeira linha do Tabela 46 na página 153.

Os valores possíveis para os identificadores da coluna estão descritos na tabela a seguir.

Tabela 48. Identificadores de Coluna Válidos para o Portlet Drill Down de Key Performance Indicator

Identificador de coluna	Descrição
kpi.NAME	Nome do KPI
kpi.CURRENT.VALUE	Valor atual do KPI
kpi.CURRENT.STATUS	Status atual do KPI
kpi.CALCULATION.TIME	Horário em que o KPI foi calculado

Conceitos relacionados:

“Drill Down de Key Performance Indicator” na página 275

Use o portlet Drill Down de Key Performance Indicator para consultar informações adicionais sobre a categoria de KPI e o status de seus KPIs subjacentes.

Configurações do Portlet do Principais Indicadores de Desempenho

Customize o portlet do Principais Indicadores de Desempenho alterando as configurações nos campos da janela **Configurações Compartilhadas**.

Parâmetros de Customização

Os campos da janela **Configurações Compartilhadas** contêm os valores dos parâmetros de customização para o portlet do Principais Indicadores de Desempenho. Os parâmetros de customização são descritos na tabela a seguir.

Tabela 49. Parâmetros de Customização do Principais Indicadores de Desempenho

Parâmetro	Descrição	Valor Padrão
JSP de ajuda padrão	Nome do arquivo de ajuda JSP a ser mostrado quando a ajuda for selecionada no menu do portlet.	KpiManagerPortletHelp
Altura do portlet	Número de pixels indicando a altura padrão do portlet.	500
Altura máxima do portlet	Número de pixels indicando a altura máxima do portlet.	600
Título do Portlet	Título para substituir o título fornecido com a solução.	Se você não inserir um valor para esse parâmetro, o título fornecido pela solução e exibido será: Principais Indicadores de Desempenho.
Pacote de Recursos	Local do pacote configurável de recursos que você fornece como uma origem para o valor de propriedades, por exemplo, título do portlet. Esse local é necessário se você deseja especificar o título como uma chave da propriedade em um pacote configurável de recursos que você fornece. Se nenhum pacote configurável for especificado, então a chave não será procurada e o título será exibido conforme fornecido pela solução.	Não há nenhum pacote configurável de recursos padrão.

Conceitos relacionados:

“Principais Indicadores de Desempenho” na página 168

Use o portlet Principais Indicadores de Desempenho para customizar o Key Performance Indicators (KPIs) e sua exibição hierárquica no IBM Intelligent Operations Center.

Configurações do Portlet do Mapa de Localização

Customize o portlet do Mapa de Localização alterando as configurações nos campos da janela **Configurações Compartilhadas**.

Parâmetros de Customização

Os campos da janela **Configurações Compartilhadas** contêm os valores dos parâmetros da customização para o portlet. Os parâmetros de customização são descritos na tabela a seguir.

Tabela 50. Valores do Parâmetro de Customização do Portlet do Mapa de Localização

Parâmetro	Descrição	Valor Padrão
-----------	-----------	--------------

Seleções de filtro padrão	Categorias de evento padrão a serem exibidas no mapa. Insira o nome ou nomes separados por ponto e vírgula e sem espaços.	CBRNE;Env;Fire;Geo;Health;Infra;Met;Rescue;Safety;Security;Transport;Other
Cor de destaque da área padrão	Cor padrão de uma área destacada ao passar o mouse sobre a área utilizando o cursor.	#808080
JSP de ajuda padrão	Nome do arquivo de ajuda JSP a ser mostrado quando a ajuda for selecionada no menu do portlet.	LocationMapPortletHelp
Seleção do mapa padrão	Nome do mapa de localização a ser exibido no portlet.	Miami SunLife Stadium
Altura máxima do portlet	Número de pixels indicando a altura máxima do portlet.	600
Altura do portlet	Número de pixels indicando a altura padrão do portlet.	400
Identificador de grupo de portlet	Nome do grupo ao qual este portlet pertence. Um nome comum configura a comunicação entre os portlets Mapa, Detalhes e Mapa de Localização na mesma página.	default
Título do Portlet	Título para substituir o título fornecido com a solução.	Se você não inserir um valor para esse parâmetro, o título fornecido pela solução e exibido será: Mapa de Localização.
Pacote de Recursos	Local do pacote configurável de recursos que você fornece como uma origem para o valor de propriedades, por exemplo, título do portlet. Esse local é necessário se você deseja especificar o título como uma chave da propriedade em um pacote configurável de recursos que você fornece. Se nenhum pacote configurável for especificado, então a chave não será procurada e o título será exibido conforme fornecido pela solução.	Não há nenhum pacote configurável de recursos padrão.

Conceitos relacionados:

“Mapa de Localização” na página 276

Utilize o portlet do Mapa de Localização para ver os eventos marcados em um mapa de localização. Um mapa de localização no IBM Intelligent Operations Center é um mapa ou plano com áreas pré-definidas para interação, por exemplo, áreas de assentos em um grande estádio esportivo.

Configurações do Portlet do Gerenciador de Mapa de Localização

Customize o portlet do Gerenciador de Mapa de Localização alterando as configurações nos campos da janela **Configurações Compartilhadas**.

Parâmetros de Customização

Os campos da janela **Configurações Compartilhadas** contêm os valores dos parâmetros da customização para o portlet. Os parâmetros de customização são descritos na tabela a seguir.

Tabela 51. Valores do Parâmetro de Customização do Portlet do Gerenciador de Mapa de Localização

Parâmetro	Descrição	Valor Padrão
Cor padrão para a nova área selecionada	Cor padrão de uma área desenhada no mapa e selecionada.	#4AA02C
Cor padrão para a área salva selecionada	Cor padrão de uma área no mapa salva e selecionada.	#808080
Cor padrão para a nova área	Cor padrão de uma área desenhada no mapa.	#009900
Cor padrão para a área salva	Cor padrão de uma área salva no mapa.	#808080
JSP de ajuda padrão	Nome do arquivo de ajuda JSP a ser mostrado quando a ajuda for selecionada no menu do portlet.	LocationMapManagerPortletHelp
Altura do portlet	Número de pixels indicando a altura padrão do portlet.	400
Título do Portlet	Título para substituir o título fornecido com a solução.	Se você não inserir um valor para esse parâmetro, o título fornecido pela solução e exibido será: Gerenciador de Mapa de Localização.
Pacote de Recursos	Local do pacote configurável de recursos que você fornece como uma origem para o valor de propriedades, por exemplo, título do portlet. Esse local é necessário se você deseja especificar o título como uma chave da propriedade em um pacote configurável de recursos que você fornece. Se nenhum pacote configurável for especificado, então a chave não será procurada e o título será exibido conforme fornecido pela solução.	Não há nenhum pacote configurável de recursos padrão.

Conceitos relacionados:

“Gerenciador de Mapa de Localização” na página 176

Use o portlet Gerenciador de Mapa de Localização para customizar o portlet Mapa de Localização.

Configurações do Portlet do Mapa

Customize o portlet do Mapa alterando as configurações nos campos da janela **Configurações Compartilhadas**.

Parâmetros de Customização

Os campos da janela **Configurações Compartilhadas** contêm os valores dos parâmetros de customização para o portlet do Mapa. Os parâmetros de customização são descritos na tabela a seguir.

Tabela 52. Valores do Parâmetro de Customização

Parâmetro	Descrição	Valor Padrão
-----------	-----------	--------------

Tabela 52. Valores do Parâmetro de Customização (continuação)

Latitude do centro	Coordenadas específicas para configurar o ponto central do mapa. O local atual do mapa é exibido à direita dos campos. É possível aplicar o zoom e panoramizar no mapa para o local necessário, em seguida recorte e cole os valores mostrados nos campos correspondentes.	25.780416
Longitude do centro		-80.203629
Nível de Zoom	Nível de ampliação padrão para o mapa. O intervalo de níveis de zoom válidos disponíveis é dependente do mapa de base. Em geral, a faixa é de 1 para cima. O valor 1 é o menor nível de zoom que exibe o mapa em sua menor ampliação. Por exemplo, o mapa de base ArcGIS padrão fornecido com a solução exibe o detalhe geográfico até o máximo de zoom, nível 12.	11
Tipo de camada de base	Valor para o tipo do mapa de base.	ARC_GIS_REST
URL da camada de base	URL do mapa de base. A URL deve conter, na ordem correta, os marcadores que representam as coordenadas x, y e z do mapa. É possível selecionar um mapa do seu servidor Esri GIS instalado ou em um serviço GIS publicamente disponível.	http://services.arcgisonline.com/ArcGIS/rest/services/World_Street_Map/MapServer/tile/{z}/{y}/{x}
Alimentação de KML ou URL do arquivo	URL para exibir os dados KML. Insira uma URL de um local no mesmo servidor do portlet com o mesmo domínio e porta. Para garantir que esta condição seja implementada, insira somente URLs que comecem com '/' ou caractere de barra, para que o navegador selecione o domínio e a porta atuais. Para diversas sequências de URL, use um ponto e vírgula e nenhum espaço entre as URLs. Se o web site requerido não for local, utilize um servidor proxy no portal de seu servidor para acessar o site. Nota: Utilize esta opção para pequenos ajustes locais, mas considere a quantidade de dados envolvidos, para não sobrecarregar a exibição ou afetar o desempenho.	Não há nenhum valor padrão fornecido com a solução.

Tabela 52. Valores do Parâmetro de Customização (continuação)

A quantidade de itens a serem exibidos	Limite para o número de marcadores exibidos em uma visualização. Insira o número máximo de marcadores que puderem ser exibidos. Se o número de marcadores na área do mapa na visualização exceder seu limite, nenhum marcador será mostrado e será exibida uma mensagem de aviso. O usuário poderá então escolher entre carregar os marcadores ou alterar a visualização.	250
Seleções de filtro padrão	Categorias de evento padrão a serem exibidas no mapa. Insira o nome ou nomes separados por ponto e vírgula e sem espaços.	CBRNE;Env;Fire;Geo;Health;Infra;Met;Rescue;Safety;Security;Transport;Outro
Altura máxima do portlet	Número de pixels indicando a altura máxima do portlet.	600
Identificador de grupo de portlet	Nome do grupo ao qual este portlet pertence. Um nome comum configura a comunicação entre os portlets Mapa, Detalhes e Mapa de Localização na mesma página.	default
Título do Portlet	Título para substituir o título fornecido com a solução.	Se você não inserir um valor para esse parâmetro, o título fornecido pela solução e exibido será: Mapa.
JSP de ajuda padrão	Nome do arquivo de ajuda JSP a ser mostrado quando a ajuda for selecionada no menu do portlet.	NavigatorPortletHelp
Pacote de Recursos	Local do pacote configurável de recursos que você fornece como uma origem para o valor de propriedades, por exemplo, título do portlet. Esse local é necessário se você deseja especificar o título como uma chave da propriedade em um pacote configurável de recursos que você fornece. Se nenhum pacote configurável for especificado, então a chave não será procurada e o título será exibido conforme fornecido pela solução.	Não há nenhum pacote configurável de recursos padrão.

Conceitos relacionados:

“Mapa” na página 279

Use o portlet Mapa para ver eventos e recursos em um mapa.

Configurações do Portlet do Minhas Atividades

Customize o portlet do Minhas Atividades alterando as configurações nos campos da janela

Configurações Compartilhadas.

Parâmetros de Customização

Os campos da janela **Configurações Compartilhadas** contêm os valores dos parâmetros de customização para o portlet do Minhas Atividades. Os parâmetros de customização são descritos na tabela a seguir.

Tabela 53. Parâmetros de Customização do Minhas Atividades

Parâmetro	Descrição	Valor Padrão
JSP de ajuda padrão	Nome do arquivo de ajuda JSP a ser mostrado quando a ajuda for selecionada no menu do portlet.	ActivitiesPortletHelp
Identificador de grupo de portlet	Nome do grupo ao qual este portlet pertence. Um nome comum configura a comunicação entre portlets na mesma página. Por exemplo, um nome comum configura a comunicação entre os portlets Minhas Atividades e Detalhes.	default
Altura do portlet	Número de pixels indicando a altura padrão do portlet.	200
Altura máxima do portlet	Número de pixels indicando a altura máxima do portlet.	600
Título do Portlet	Título para substituir o título fornecido com a solução.	Se você não inserir um valor para esse parâmetro, o título fornecido pela solução e exibido será: Minhas Atividades.
Pacote de Recursos	Local do pacote configurável de recursos que você fornece como uma origem para o valor de propriedades, por exemplo, título do portlet. Esse local é necessário se você deseja especificar o título como uma chave da propriedade em um pacote configurável de recursos que você fornece. Se nenhum pacote configurável for especificado, então a chave não será procurada e o título será exibido conforme fornecido pela solução.	Não há nenhum pacote configurável de recursos padrão.

Conceitos relacionados:

“Minhas Atividades” na página 284

O portlet Minhas Atividades exibe uma lista dinâmica de atividades pertencentes ao grupo do qual o usuário que está conectado à interface é membro.

Configurações do Portlet do Notificações

Customize o portlet do Notificações alterando as configurações nos campos da janela **Configurações Compartilhadas**.

Parâmetros de Customização

Os campos da janela **Configurações Compartilhadas** contêm os valores dos parâmetros de customização para o portlet do Notificações. Os parâmetros de customização são descritos na tabela a seguir.

Tabela 54. Parâmetros de Customização do Notificações

Parâmetro	Descrição	Valor Padrão
Colunas	Especificações e ordem das colunas a serem exibidas na lista.	[{"id": "notifications.HEADLINE"}, {"id": "notifications.SENTFROM"}, {"id": "notifications.SENTTIME", "width" : "10", "format": "yyyy-MM-dd HH:mm:ss"}]
JSP de ajuda padrão	Nome do arquivo de ajuda JSP a ser mostrado quando a ajuda for selecionada no menu do portlet.	CityCoordinatorPortletHelp

Tabela 54. Parâmetros de Customização do Notificações (continuação)

Ocultar barra de ferramentas	Configuração verdadeira ou falsa para ocultar ou exibir a barra de ferramentas na parte superior do portlet.	true
Altura do portlet	Número de pixels indicando a altura padrão do portlet.	200
Altura máxima do portlet	Número de pixels indicando a altura máxima do portlet.	600
Título do Portlet	Título para substituir o título fornecido com a solução.	Se você não inserir um valor para esse parâmetro, o título fornecido pela solução e exibido será: Notificações.
Pacote de Recursos	Local do pacote configurável de recursos que você fornece como uma origem para o valor de propriedades, por exemplo, título do portlet. Esse local é necessário se você deseja especificar o título como uma chave da propriedade em um pacote configurável de recursos que você fornece. Se nenhum pacote configurável for especificado, então a chave não será procurada e o título será exibido conforme fornecido pela solução.	Não há nenhum pacote configurável de recursos padrão.

Nota: A explicação do que ocorre com o título do portlet quando você fornece um pacote configurável se aplica também ao título da coluna que se origina do mesmo pacote configurável de recursos.

Parâmetros de Colunas

O valor do parâmetro **colunas** é uma matriz de objetos JSON que podem ser configurados, conforme explicado no Tabela 55.

Tabela 55. Objetos no Valor dos Parâmetros de Colunas do Portlet do Notificações

Objeto	Contém
ID	O identificador da coluna para indicar que a coluna deve ser exibida
mín.	Número de pixels indicando a largura da coluna
format	Sequência que representa o formato a ser usado para colunas de data e hora, a entrada substitui a configuração na tabela sysprop
sortAscending	<ul style="list-style-type: none"> true para usar uma ordem de classificação ascendente nos itens da coluna false para usar uma ordem de classificação descendente nos itens da coluna
sortPriority	<ul style="list-style-type: none"> Número para indicar a prioridade de classificação dessa coluna entre todas as colunas; quando mais baixo o número, mais alta a prioridade Nenhum valor, deixe em branco para usar a prioridade de classificação padrão das colunas -1 para desativar a prioridade de classificação padrão das colunas
título	Título da coluna, deixe em branco para usar o título de coluna padrão

As colunas são exibidas no portlet na mesma ordem que a fornecida nos objetos JSON que compõem o valor do parâmetro **colunas**. Somente as colunas com os identificadores da coluna especificados no valor serão exibidas, todas as outras estarão ocultas. Se o valor do parâmetro **colunas** for omitido, as colunas serão exibidas conforme indicado na configuração padrão, exibida na primeira linha do Tabela 54 na página 160.

Os valores possíveis para os identificadores da coluna estão descritos no Tabela 56.

Tabela 56. Identificadores de Coluna Válidos para o Portlet Notificações

Identificador de coluna	Descrição
notifications.ID	UUID fornecido para a notificação na tabela de notificações
notifications.CATEGORY	Valor não convertido da categoria do evento ou KPI relacionado à notificação
notifications.SENTFROM	Serviço que gerou a notificação
notifications.SENTTOGROUP	Lista de grupos que podem acessar a notificação
notifications.SENTTIME	Tempo gerado pelo serviço que enviou a notificação
notifications.HEADLINE	Texto curto descrevendo a notificação
notifications.DESCRPTION	Texto detalhado descrevendo a notificação
notifications.ALERTLINK	Lista de alertas de CAP relacionados à notificação
notifications.KPILINK	KPI relacionado à notificação

Conceitos relacionados:

“Notificações” na página 286

Use o portlet Notificações para visualizar as mensagens de alerta e os seus detalhes.

Configurações do Portlet do Relatórios

Customize o portlet do Relatórios alterando as configurações nos campos da janela **Configurações Compartilhadas**.

Parâmetros de Customização

Os campos da janela **Configurações Compartilhadas** contêm os valores dos parâmetros da customização para o portlet. Os parâmetros de customização são descritos na tabela a seguir.

Tabela 57. Valores do Parâmetro de Customização do Portlet do Relatórios

Parâmetro	Descrição	Valores Padrão
JSP de ajuda padrão	Nome do arquivo de ajuda JSP a ser mostrado quando a ajuda for selecionada no menu do portlet.	ReportsIntegrationPortletHelp
Altura do portlet	Número de pixels indicando a altura padrão do portlet.	600
Altura máxima do portlet	Número de pixels indicando a altura máxima do portlet.	800
Título do Portlet	Título do portlet Relatórios.	Relatório Customizado

Tabela 57. Valores do Parâmetro de Customização do Portlet do Relatórios (continuação)

URL do relatório	Especifica a URL do relatório que é exibido.	<code>http://ioc1bvtlite1.rtp.raleigh.ibm.com/cognos/ServletGateway/servlet/Gateway?b_action=cognosViewer&ui.action=run&ui.object=%2fcontent%2fpackage%5b%40name%3d%27ioc_cap_model%27%5d%2ffolder%5b%40name%3d%27reports%27%5d%2ffolder%5b%40name%3d%27User_defined_reports%27%5d%2freport%5b%40name%3d%27User_defined_report%27%5d&ui.name=User_defined_report&run.outputFormat=&run.prompt=true&cv.toolbar=false&cv.header=false</code>
Pacote de Recursos	Local do pacote configurável de recursos que você fornece como uma origem para o valor de propriedades, por exemplo, título do portlet. Esse local é necessário se você deseja especificar o título como uma chave da propriedade em um pacote configurável de recursos que você fornece. Se nenhum pacote configurável for especificado, então a chave não será procurada e o título será exibido conforme mostrado no campo do Título do Portlet da janela Configurações Compartilhadas .	Não há nenhum pacote configurável de recursos padrão.
Mostrar campo URL na página	Selecione True para incluir o botão URL do relatório na página do portlet Relatórios. Esse botão permite que todos os usuários, não apenas os administradores, criem um relatório customizado e configurem a URL do relatório. Selecione False para omitir o botão URL do relatório da página do portlet Relatórios.	False

Conceitos relacionados:

“Relatórios” na página 288

Use o portlet Relatórios para visualizar um relatório de eventos como um gráfico. O portlet fornece opções para agrupar eventos e é possível escolher eventos por uma data ou intervalo de data específico. Estes relatórios ajudam a planejar respostas a eventos atuais e futuros.

Configurações do Portlet do Publicador de Amostra

Customize o portlet do Publicador de Amostra alterando as configurações nos campos da janela **Configurações Compartilhadas**.

Parâmetros de Customização

Os campos da janela **Configurações Compartilhadas** contêm os valores dos parâmetros de customização para o portlet do Publicador de Amostra. Os parâmetros de customização são descritos na tabela a seguir.

Tabela 58. Parâmetros de Customização do Publicador de Amostra

Parâmetro	Descrição	Valor Padrão
-----------	-----------	--------------

Tabela 58. Parâmetros de Customização do Publicador de Amostra (continuação)

JSP de ajuda padrão	Nome do arquivo de ajuda JSP a ser mostrado quando a ajuda for selecionada no menu do portlet.	SamplePublisherPortletHelp
Título do Portlet	Título para substituir o título fornecido com a solução.	Se você não inserir um valor para esse parâmetro, o título fornecido pela solução e exibido será: Publicador de Amostra.
Pacote de Recursos	Local do pacote configurável de recursos que você fornece como uma origem para o valor de propriedades, por exemplo, título do portlet. Esse local é necessário se você deseja especificar o título como uma chave da propriedade em um pacote configurável de recursos que você fornece. Se nenhum pacote configurável for especificado, então a chave não será procurada e o título será exibido conforme fornecido pela solução.	Não há nenhum pacote configurável de recursos padrão.

Conceitos relacionados:

“Publicador de Amostra” na página 103

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

Configurações do Portlet do Procedimentos Padrão de Operação

Customize o portlet do Procedimentos Padrão de Operação alterando as configurações nos campos da janela **Configurações Compartilhadas**.

Parâmetros de Customização

Os campos da janela **Configurações Compartilhadas** contêm os valores dos parâmetros de customização para o portlet do Procedimentos Padrão de Operação. Os parâmetros de customização são descritos na tabela a seguir.

Tabela 59. Parâmetros de Customização do Procedimentos Padrão de Operação

Parâmetro	Descrição	Valor Padrão
JSP de ajuda padrão	Nome do arquivo de ajuda JSP a ser mostrado quando a ajuda for selecionada no menu do portlet.	SOPManagerPortletHelp
Altura do portlet	Número de pixels indicando a altura padrão do portlet.	440

Conceitos relacionados:

“Procedimentos Padrão de Operação” na página 127

É possível definir o procedimentos padrão de operação e atividades para gerenciar eventos que chegam ao IBM Intelligent Operations Center. Use o portlet Procedimentos Padrão de Operação para acessar os aplicativos procedimento padrão de operação, matriz de seleção de procedimento padrão de operação e designer de fluxo de trabalho no Tivoli Service Request Manager.

Configurações do Portlet do Status

Customize o portlet do Status alterando as configurações nos campos da janela **Configurações Compartilhadas**.

Parâmetros de Customização

Os campos da janela **Configurações Compartilhadas** contêm os valores dos parâmetros de customização para o portlet do Status. Os parâmetros de customização são descritos na tabela a seguir.

Tabela 60. Parâmetros de Customização do Status

Parâmetro	Descrição	Valor Padrão
Customizar Cores de KPI	<p>Cores a serem usadas no portlet para indicar o status de KPIs, por exemplo, é possível inserir:</p> <pre>{"acceptable": "#7f7f7f", "take_action": "#34333"}</pre> <p>As cores que você inserir aqui substituirão as cores fornecidas pela solução.</p>	{ }
JSP de ajuda padrão	Nome do arquivo de ajuda JSP a ser mostrado quando a ajuda for selecionada no menu do portlet.	KpiStatusPortletHelp
Ativar Filtro de KPI	Configuração true ou false para ativar ou desativar um filtro KPI adicional para o portlet, de acordo com as informações no valor do parâmetro Filtro do KPI .	false
Filtro de KPI	IDs de KPIs a serem exibidos quando 'Ativar filtro do KPI' está configurado para true para o portlet, por exemplo:	[]
Identificador de grupo de portlet	Nome do grupo ao qual este portlet pertence. Um nome comum configura a comunicação entre os portlets Drill Down de Key Performance Indicator e Status na mesma página.	default
Altura do portlet	Número de pixels indicando a altura padrão do portlet.	200
Altura máxima do portlet	Número de pixels indicando a altura máxima do portlet.	600
Título do Portlet	Título para substituir o título fornecido com a solução.	Se você não inserir um valor para esse parâmetro, o título fornecido pela solução e exibido será: Status.
Pacote de Recursos	Local do pacote configurável de recursos que você fornece como uma origem para o valor de propriedades, por exemplo, título do portlet. Esse local é necessário se você deseja especificar o título como uma chave da propriedade em um pacote configurável de recursos que você fornece. Se nenhum pacote configurável for especificado, então a chave não será procurada e o título será exibido conforme fornecido pela solução.	Não há nenhum pacote configurável de recursos padrão.
Mostrar legenda	Configuração verdadeira ou falsa para ocultar ou exibir a legenda no portlet.	true
Ordem de Classificação	Propriedade do KPI pelo qual a lista de KPIs está classificada. O padrão é classificar em ordem alfabética ascendente, por nome de KPI. Outras opções são kpi.CURRENT.VALUE, kpi.CURRENT.STATUS, e kpi.CALCULATION.TIME	+kpi.NAME

Conceitos relacionados:

“Status” na página 290

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

Customizando a Ajuda do Portlet

É possível implementar ajuda alternativa para um portlet do IBM Intelligent Operations Center.

Sobre Esta Tarefa

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

Se você mudar o layout ou os dados exibidos em um portlet, pode também desejar mudar a ajuda exibida.

Procedimento

1. Crie a ajuda alternativa como um arquivo JSP.
2. É possível dar ao arquivo qualquer nome que você queira, mas é necessário usar o sufixo correto para o seu idioma. A configuração do idioma se baseia no idioma do seu navegador. Use o identificador do código de idioma padrão para o seu idioma, por exemplo:

Opção	Descrição
<code>_pt_BR</code>	Português do Brasil
<code>_en</code>	Inglês
<code>_fr</code>	Francês
<code>_de</code>	Alemão
<code>_es</code>	Espanhol

3. Use a janela **Configurações Compartilhadas** do portlet para configurar o parâmetro **DefaultHelpJSP** com o nome o arquivo de ajuda alternativo. Não inclua o sufixo de idioma ou a extensão de arquivo `.jsp`.
4. Copie o arquivo JSP de ajuda alternativo para o local correto: `/opt/IBM/WebSphere/wp_profile/installedApps/cell1/ioc_portal_ear.ear/portlet_war/portlet_root/jsp/html/help`. Os valores para cada portlet das variáveis `portlet_war` e `portlet_root` estão listados em um tópico separado. Consulte o link no final desse tópico para uma lista desses valores.

Nota: Ao mudar o arquivo de ajuda do Resumo de Permissões do Usuário, substitua `ioc_portal_ear.ear` por `iss_portal_ear.ear` no caminho fornecido nessa etapa.

O que Fazer Depois

Forneça conversões para o arquivo de ajuda alternativo para todos os idiomas suportados, incluindo um idioma padrão.

Informações relacionadas:

 [Documentação do Produto IBM WebSphere Portal 7](#)

Locais do Arquivo de Ajuda do Portlet

Valores de locais são necessários para cada portlet ao substituir a ajuda do portlet padrão por seu arquivo de ajuda JSP alternativo.

As Tabelas 1 e 2 fornecem valores para o local dos arquivos de ajuda do portlet do usuário e do administrador.

Tabela 61. Valores do Portlet do Usuário para Localização de um Arquivo de Ajuda Alternativo

Portlet	<code>portlet_war</code>	<code>portlet_root</code>
Detalhes	<code>icoc_ui_common_events_portlet.war</code>	<code>_icoc_ui_common_events_portlet</code>
Drill Down de Key Performance Indicator	<code>icoc_ui_kpi_drilldown_portlet.war</code>	<code>_icoc_ui_kpi_drilldown_portlet</code>

Tabela 61. Valores do Portlet do Usuário para Localização de um Arquivo de Ajuda Alternativo (continuação)

Portlet	<i>portlet_war</i>	<i>portlet_root</i>
Mapa de Localização	icoc_ui_location_map_portlet.war	_icoc_ui_location_map_portlet
Mapa	icoc_ui_navigator_portlet.war	_icoc_ui_navigator_portlet
Minhas Atividades	icoc_ui_activities_portlet.war	_icoc_ui_activities_portlet
Notificações	icoc_ui_city_coordinator_portlet.war	_icoc_ui_city_coordinator_portlet
Relatórios	icoc_ui_reports_portlet.war	_icoc_ui_reports_portlet
Status	icoc_ui_kpi_status_portlet.war	_icoc_ui_kpi_status_portlet

Tabela 62. Valores do Portlet de Administração para Localização de um Arquivo de Ajuda Alternativo

Portlet	<i>portlet_war</i>	<i>portlet_root</i>
Consoles de Administração	icoc_ui_administration_console_portlet.war	_icoc_ui_administration_console_portlet
Script do Evento	icoc_ui_event_scripting_portlet.war	_icoc_ui_event_scripting_portlet
Principais Indicadores de Desempenho	icoc_ui_kpi_manager_portlet.war	_icoc_ui_kpi_manager_portlet
Gerenciador de Mapa de Localização	icoc_ui_location_map_manager_portlet.war	_icoc_ui_location_map_manager_portlet
Publicador de Amostra	icoc_ui_sample_publisher_portlet.war	_icoc_ui_sample_publisher_portlet
Procedimentos Padrão de Operação	icoc_ui_sop_manager_portlet.war	_icoc_ui_sop_manager_portlet
Resumo de Permissões do Usuário	iss_ui_security_portlet.war	_iss_ui_security_portlet

Customizando KPIs

No IBM Intelligent Operations Center é possível customizar os modelos do Principal Indicador de Desempenho (KPI), a fim de se adequarem aos processos de negócios.

Os KPIs são projetados para fornecer dados estatísticos que podem ser utilizados para analisar tendências ou para indicar áreas problemáticas. Os dados do KPI são atualizados por eventos dentro do IBM Intelligent Operations Center.

O IBM Intelligent Operations Center fornece um conjunto de KPIs e ocorrências de amostra que podem ser usados para atualizar status de KPI. Existem três modelos de KPI de amostra fornecidos com o IBM Intelligent Operations Center baseados em monitoramento e processos de negócios de água, transporte e segurança públicos de amostra. Para obter mais informações sobre os KPIs de amostra fornecidos com o IBM Intelligent Operations Center, siga o link no final do tópico.

Cada solução do IBM Intelligent Operations Center segue um processo de criação e de integração do KPI para configurar os KPIs necessários para o ambiente de negócios específico. É possível criar seus próprios modelos de KPI com o IBM WebSphere Business Monitor. Para obter mais informações sobre a criação e a integração de KPIs com o IBM Intelligent Operations Center, siga o link no final do tópico.

Utilize o portlet do Principais Indicadores de Desempenho para customizar os KPIs no IBM Intelligent Operations Center. O portlet do Principais Indicadores de Desempenho é fornecido para o administrador como uma das opções das **Ferramentas de Customização da Solução**.

Ao utilizar o portlet, é possível visualizar as propriedades do KPI; criar, copiar ou modificar KPIs; e visualizar ou alterar as exibições hierárquicas para modelos do KPI.

Utilize a guia **Definição de KPI** para definir as KPIs associadas a um modelo de KPI específico no IBM Intelligent Operations Center:

- Visualize a lista atual de KPIs pertencentes a um modelo de KPI.
- Visualize as propriedades de um KPI existente.
- Atualize as propriedades de um KPI existente.
- Crie um novo KPI para um modelo de KPI:
 - Agregue o KPI calculado usando uma métrica definida
 - Valor do KPI de expressão baseado em outros KPIs
- Exclua um KPI.

Suas atualizações serão salvas nos modelos do IBM WebSphere Business Monitor armazenados no banco de dados do IBM Intelligent Operations Center. As atualizações também serão refletidas na próxima atualização do Status e dos portlets do Drill Down de Key Performance Indicator.

Use a guia **Hierarquia de Exibição do KPI** para atualizar as hierarquias do KPI exibidas no Status e nos portlets do Drill Down de Key Performance Indicator.

- Visualize as hierarquias KPI existentes.
- Visualize as propriedades principais de um KPI.
- Altere a estrutura em árvore movendo ou removendo itens de uma hierarquia do KPI.
- Inclua KPIs predefinidos a uma hierarquia.

As atualizações serão refletidas na próxima atualização do Status e dos portlets do Drill Down de Key Performance Indicator.

Nota: Quaisquer alterações na hierarquia de exibição são independentes do modelo do KPI e um entendimento do modelo KPI é necessário para assegurar que as atualizações respeitem a lógica do modelo KPI.

Conceitos relacionados:

“Criando e Integrando KPIs” na página 109

Modelos de principais indicadores de desempenho (KPI) podem, ser criados e modificados usando um kit de ferramentas de desenvolvimento de monitoramento de negócios e um portlet de gerenciamento de KPI.

“KPIs de Amostra” na página 121

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

Principais Indicadores de Desempenho

Use o portlet Principais Indicadores de Desempenho para customizar o Key Performance Indicators (KPIs) e sua exibição hierárquica no IBM Intelligent Operations Center.

No portlet do Principais Indicadores de Desempenho é possível visualizar, alterar, copiar, criar e excluir KPIs. Também é possível customizar as hierarquias de KPI exibidos no Status e nos portlets do Drill Down de Key Performance Indicator.

Para acessar o portlet do Principais Indicadores de Desempenho, na interface de Administração do WebSphere Portal, clique em **Intelligent Operations > Ferramentas de Customização > Principais Indicadores de Desempenho**.

Visualizando Hierarquias de KPI

Use a guia **Relacionamentos e Exibição** para visualizar modelos de KPI conforme eles são exibidos no Status e nos portlets do Drill Down de Key Performance Indicator.

Sobre Esta Tarefa

À esquerda da janela **Relacionamentos e Exibição**, você verá listado os nós de nível raiz para as hierarquias de KPI que você está autorizado a visualizar. Estes nós representam os modelos KPI conforme são exibidos no Status e nos portlets do Drill Down de Key Performance Indicator.

Procedimento

1. Expanda um nó de nível raiz para ver os níveis mais baixos da árvore de modelo que deseja visualizar.
2. Clique em um título do nó de nível raiz para visualizar seus detalhes à direita da janela. As informações são exibidas conforme descrito na tabela a seguir:

Opção	Descrição
Nome	título do nó de nível raiz
Tipo	tipo de nó de nível raiz
ID de Modelo	identificador para o modelo de KPI correspondente
Categoria	classificação do modelo
Ícone	ícone que representa o nó de nível raiz

3. Clique em um KPI para visualizar os detalhes à direita da janela **Relacionamentos e Exibição**.

Alterando uma Hierarquia de KPI

Use a guia **Relacionamentos e Exibição** para alterar ou remover um modelo de KPI conforme ele é exibidos no Status e nos portlets do Drill Down de Key Performance Indicator.

Procedimento

1. À esquerda da janela **Relacionamentos e Exibição**, clique no nó do nível de raiz e subitens para expandir a árvore hierárquica para o nível que deseja.
2. É possível mover, incluir, alterar ou remover os itens existentes, conforme segue:
 - Para mover subitens dentro de uma árvore, arraste um item para a posição que desejar. Indicadores verdes ou vermelhos indicam se uma movimentação é permitida ou não.
 - Para incluir em uma árvore a partir da lista de subitens existente para um modelo de KPI, clique com o botão direito do mouse no item para conter o subitem e clique em **Incluir KPI**.
 - Para acessar a janela **Propriedades do KPI** e alterar um subitem, clique com o botão direito do mouse no item e clique em **Editar**.
 - Para remover um nó de nível raiz ou um subitem de uma árvore, clique com o botão direito do mouse no item e clique em **Remover**. Remover um item do nó raiz removerá todos os subitens que ele contém.
3. Clique em **Salvar** para salvar as atualizações.

Nota: Não é possível aqui editar o nome de uma organização proprietária ou nó de nível raiz. Se deseja alterar uma organização proprietária, remova-a e substitua por outro nome.

Incluindo uma Organização Proprietária

Utilize a guia **Relacionamentos e Exibição** para incluir um nó de nível raiz a ser exibido no Status e nos portlets do Drill Down de Key Performance Indicator.

Procedimento

1. Na parte superior esquerda da janela **Relacionamentos e Exibição**, clique em **Incluir Organização Proprietária**.
2. Tipo em um nome de exibição.
3. Na lista suspensa do campo **Modelo**, selecione o nó de nível raiz a ser incluído.
4. Na lista suspensa do campo **Categoria**, selecione uma categoria para o nó de nível raiz.
5. Na lista suspensa do campo **Ícone**, selecione o nome do arquivo para o ícone para representar o nó de nível raiz.
6. Clique em **OK** para incluir o novo nó à esquerda da janela **Relacionamentos e Exibição**.
7. Clique em **Salvar** para atualizar a exibição no Status e nos portlets do Drill Down de Key Performance Indicator.

Alterando a Legenda do KPI

Utilize a guia **Relacionamentos e Exibição** para alterar a legenda do KPI no portlet do Status.

Procedimento

1. Na parte superior esquerda da janela **Relacionamentos e Exibição**, clique em **Legenda KPI**.
2. Altere a exibição para a legenda do KPI conforme segue:
 - Para incluir um intervalo, clique em **Incluir Linha**.
 - Para alterar um intervalo, edite os campos em **Nome do Intervalo**, **Cor**, **Ícone**.
 - Para excluir um intervalo, clique em **Excluir**.
3. Clique em **OK** para atualizar a exibição no Status e nos portlets do Drill Down de Key Performance Indicator.

Visualizando um Modelo de KPI

Utilize a guia **Definição de KPI** para visualizar KPIs pertencentes aos modelos de KPI dentro do IBM Intelligent Operations Center.

Procedimento

O campo **Filtrar por Modelo** contém uma lista suspensa de modelos de processos de negócios que você está autorizado a visualizar. Selecione todos os modelos ou o modelo para o qual deseja ver os KPIs. As informações são exibidas conforme descrito na tabela a seguir:

Opção	Descrição
Nome do KPI	Título do KPI. É possível clicar no nome do KPI para ver as propriedades.
Modelo	Nome do modelo a que pertence o KPI.
Criado	Método de criação do KPI: <ul style="list-style-type: none">• Um KPI modelado é um KPI criado no nível de modelo utilizando o IBM WebSphere Business Monitor.• Um Painel KPI for um KPI criado usando o portlet do Principais Indicadores de Desempenho.
Tipo	Tipo de KPI: <ul style="list-style-type: none">• Um KPI agregado possui um valor baseado no método de métrica e de agregação selecionado.• Um KPI de expressão possui um valor baseado em outros KPIs ou funções definidas pelo usuário, utilizando uma expressão XPath definida.

Opção	Descrição
Acesso	Nível de acesso de um KPI: <ul style="list-style-type: none"> Um KPI compartilhado é um KPI que outros usuários têm acesso para visualização. Um KPI particular é um KPI que não pode ser compartilhado com usuários que não sejam o proprietário.

Visualizando ou alterando um KPI

Utilize a guia **Definição de KPI** para visualizar ou alterar um KPI existente pertencente a um modelo no IBM Intelligent Operations Center.

Procedimento

1. Selecione um KPI. Na parte superior esquerda da janela **Definição de KPI**, clique em **Editar**. A janela **Propriedades do KPI** se abre.
2. Para alterar o KPI, edite os campos nas guias da janela de propriedades. Para obter mais detalhes sobre como editar esses campos para criar um KPI agregado ou expressão, clique no link no final do tópico.

Nota: Não é possível alterar a definição de um KPI modelado aqui.

3. Para salvar e sair da janela atualizada **Propriedades KPI**, clique em **OK**. Para salvar e continuar a alterar o KPI copiado, clique em **Aplicar**. Para sair sem salvar, clique em **Cancelar**.

Copiando um KPI

Utilize a guia **Definição de KPI** para fazer cópia de um KPI existente para um modelo no IBM Intelligent Operations Center.

Procedimento

1. Selecione um KPI. Na parte superior esquerda da janela **Definição de KPI**, clique em **Mais Ações > Copiar**. A janela **Propriedades de KPI** é aberta.
2. Digite um novo nome de KPI no campo **Nome de KPI**.
3. Edite as propriedades do KPI copiado de acordo com as etapas 3 e 4 do procedimento para alterar um KPI.

Criando um KPI

Utilize a guia **Definição de KPI** para criar um KPI para um modelo no IBM Intelligent Operations Center.

Procedimento

1. Na parte superior esquerda da janela **Definição de KPI**, clique em **Criar**.
2. Clique em **Novo KPI Agregado** ou **Novo KPI de Expressão**. A janela **Propriedades do KPI** se abre.
3. Edite as propriedades do KPI novo de acordo com as etapas 3 e 4 do procedimento para alterar um KPI.

O que Fazer Depois

Para obter informações adicionais sobre como criar KPIs, acesse o link da documentação do IBM Websphere Business Monitor no final do tópico.

KPIs de Amostra

Um conjunto de KPIs de amostra é fornecido com a solução. 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.

Customizando o Portlet do Principais Indicadores de Desempenho

É possível customizar este portlet. Clique no botão no canto superior direito do portlet para ver as opções de customização do menu de portlet. As configurações compartilhadas afetam o conteúdo desse portlet para todos os usuários, mas apenas para esta ocorrência do portlet.

Conceitos relacionados:

“Status” na página 290

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

“Drill Down de Key Performance Indicator” na página 275

Use o portlet Drill Down de Key Performance Indicator para consultar informações adicionais sobre a categoria de KPI e o status de seus KPIs subjacentes.

Referências relacionadas:

“Configurações do Portlet do Principais Indicadores de Desempenho” na página 155

Customize o portlet do Principais Indicadores de Desempenho alterando as configurações nos campos da janela **Configurações Compartilhadas**.

Informações relacionadas:

 Centro de Informações do IBM WebSphere Business Process Management Versão 7.0

Faça Backup Antes de Customizar KPIs

Faça backup e restaure KPIs que foram criadas ou modificadas com o IBM WebSphere Business Monitor, ou com o portlet Principais Indicadores de Desempenho.

Sobre Esta Tarefa

Antes de customizar modelos de KPI e modificar KPIs, você pode querer fazer backup de modelos existentes. O procedimento nesse tópico exporta todos os KPIs do modelo especificado para o arquivo especificado, e importa KPIs do arquivo especificado para o modelo especificado.

Procedimento

1. Efetue logon no servidor de aplicativos.
2. Mude o diretório bin do perfil do IBM WebSphere Business Monitor: `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin`
3. Para exportar KPIs, execute o comando: `./wsadmin.sh -wsadmin_classpath "../../../../plugins/com.ibm.wbimonitor.lifecycle.spi.jar:../../../../plugins/com.ibm.wbimonitor.repository.jar" -lang jython -f "../../../../scripts/wbm/kpi/exportKpis.jy" "xml_file_path" model_ID model_version ALL`
xml_file_path é o nome e caminho do arquivo XML para o qual você está exportando os KPIs.
model_ID e *model_version* são o ID e versão do modelo de KPI do qual você está exportando os KPIs.
4. Para importar KPIs, execute o comando: `./wsadmin.sh -wsadmin_classpath "../../../../plugins/com.ibm.wbimonitor.lifecycle.spi.jar:../../../../plugins/com.ibm.wbimonitor.repository.jar" -lang jython -f "../../../../scripts/wbm/kpi/importKpis.jy" "xml_file_path"`
xml_file_path é o nome e caminho do arquivo XML do qual você está importando os KPIs.

Exemplo

Para exportar todos os KPIs do modelo, `icoc_sample_public_safety_monitor_model`, para `/tmp/kpis.xml`, execute o seguinte comando. No comando, o valor de `xml_file_path` é `/tmp/kpis.xml`, o valor de `model_ID` é `icoc_sample_public_safety_monitor_model`, e o valor de `model_version` é `2011-02-18T10:49:46`.

```
./wsadmin.sh -wsadmin_classpath "../../plugins/com.ibm.wbimonitor.lifecycle.spi.jar:  
../../plugins/com.ibm.wbimonitor.repository.jar" -lang jython -f "../../scripts.wbm  
/kpi/exportKpis.jy" "/tmp/kpis.xml" icoc_sample_public_safety_monitor_model  
2011-02-18T10:49:46 ALL
```

Para obter informações adicionais, consulte o link para o centro de informações do WebSphere Business Monitor no final desse tópico.

Referências relacionadas:

“Fazendo Backup de Dados” na página 259

Para evitar a perda de dados importantes no IBM Intelligent Operations Center, faça backup de certos arquivos, diretórios e bancos de dados em intervalos regulares.

Informações relacionadas:



Redbooks do IBM Smarter Cities Software Solutions

Customizando a Correlação de Evento

Essa seção explica a correlação de evento e descreve como mudar e criar novas tabelas de decisão. Também explica o aplicativo de regra.

Correlação de Evento e o Aplicativo de Regra

Esse tópico fornece uma visão geral do processo de correlação de evento e explica brevemente o aplicativo de regra.

O aplicativo de regras de correlação de evento baseado no WebSphere Operational Decision Management possibilita modificar e estender regras de correlação sem conhecimento técnico avançado de IBM Intelligent Operations Center ou WebSphere Operational Decision Management. Porém, conhecimento básico de eventos do Protocolo de Alerta Comum e do WebSphere Operational Decision Management é requerido.

As variáveis determinam como os eventos se correlacionam: o evento de origem, o evento de destino e a tabela de decisão.

Para cada evento do Protocolo de Alerta Comum recebido, o aplicativo de regras é chamado para determinar se algum dos eventos existentes se correlaciona com o evento recebido. O evento de origem sempre é o novo evento recebido e ele aciona a correlação. O processo de correlação verifica o evento de origem em relação aos eventos no banco de dados. Quando um evento localizado no banco de dados se correlaciona com o evento de origem, esse evento é chamado evento de destino. Sempre que uma correlação possível é localizada, o portlet de Notificações envia um alerta.

A determinação é unilateral. Esse conceito é importante porque as regras que determinam a correlação não precisam ser simétricas. Por exemplo, se o evento A se correlaciona com o evento B, isso não significa que o evento B se correlaciona com o evento A.

O aplicativo de regras fornece uma tabela de correlação de amostra que se adequa à maioria dos requisitos. Consulte o “Customizando Configurações de Correlação de Evento” na página 174 para diferentes maneiras de customizar as regras de correlação.

Customizando Configurações de Correlação de Evento

Essa seção explica como customizar configurações de correlação de evento.

A tabela de decisão, que pode ser editada no Centro de Decisão, tem dois tipos de colunas. Colunas à esquerda são chamadas de colunas de decisão. Elas determinam qual coluna de ação, à direita, usar. As tabelas de decisão são verificadas da esquerda para a direita e, dependendo dos valores das diferentes linhas, levam a uma coluna de ação à direita. A coluna de ação define o que é executado quando uma linha específica é atingida.

A maneira recomendada para expandir e modificar configurações de correlação de evento é editar uma tabela de decisão existente. Os seguintes itens descrevem como as tabelas de decisão são formatadas:

- No lado esquerdo da tabela de decisão (plano de fundo branco) estão as colunas de decisão. Elas determinam quais linhas nas colunas de ação (plano de fundo cinza) são executadas.
- A última coluna de ação na tabela chama o serviço de consulta e publicação. Se houver uma linha de ação que você não queira como uma consulta e publicação de correlação, desative a entrada nessa última coluna.
- A coluna Configurar Consulta SQL nas colunas de ação podem substituir os parâmetros de consulta. Substituir parâmetros de consulta é incômodo e desnecessário para a maioria dos aplicativos. O requisito para essa consulta é que haja três colunas nomeadas no resultado da consulta:
 - event_headline - O título a ser usado na descrição da correlação. Esse texto se torna a descrição da notificação.
 - event_external_id - O ID externo, como CAP-ID, do evento
 - event_internal_id - O ID interno, como CapAlertId, a ser usado pelo portlet de Notificações para mapear para títulos no campo **Refere-se a Alertas** das propriedades de notificação.

Essa seção contém os seguintes tópicos:

Mudando as Propriedades de Decisão

Use a interface com o usuário do Centro de Decisão no WebSphere Operational Decision Management para mudar as configurações de correlação de evento. Esse tópico explica mais informações sobre a mudança de propriedades de decisão nas tabelas de decisão. Ele também fornece um link para a documentação do WebSphere Operational Decision Management.

Sobre Esta Tarefa

A interface com o usuário está localizada no nó 1 da instalação do servidor de portal nessa URL: http://app_server:9084/teamserver. Efetue logon como waswebadmin.

A maioria das mudanças que você faz podem ser feitas dentro do aplicativo de regra, conforme descrito em “Editando a Tabela de Decisão” na página 175. Outras modificações podem envolver mudanças no seguinte:

- As políticas do Tivoli Netcool/Impact
- O nó de cálculo do WebSphere Message Broker Java que transforma as mensagens de políticas de impacto em formato bean orientado para mensagem
- O Modelo de Objeto Executável (XOM) e o Modelo de Objeto de Negócios (BOM) de consulta

Para obter informações e instruções adicionais para modificar o XOM e o BOM, informações para o nó do broker de mensagem e informações sobre o Centro de Decisão, consulte os Centros de Informações do WebSphere Operational Decision Management e do WebSphere Message Broker usando os links abaixo.

Informações relacionadas:

 [Centro de Informações do IBM WebSphere Operational Decision Management](#)

 [Documentação do WebSphere Message Broker](#)

Editando a Tabela de Decisão

Esse tópico fornece uma breve explicação da tabela de decisão, e fornece as etapas para mudar as propriedades da tabela de decisão.

No aplicativo de regras IBM Intelligent Operations Center WebSphere Operational Decision Management, existe uma tabela de correlação básica definida que usa a categoria e o tipo do evento para determinar qual linha de ação executar.

Atualmente, as linhas de ação são idênticas, mas podem ser usadas para se ajustarem aos seus requisitos. Por exemplo, é possível definir que os eventos de fogo sejam tratados diferentemente de outros eventos e somente se correlacionem com eventos de água e outros eventos de fogo. Para mudar valores para que se ajustem aos seus requisitos, ative a célula da coluna Categorias para a linha e insira "Fogo, Água" na célula. Se desejar que a regra faça distinção entre Eventos e Incidentes, inclua uma linha nessa coluna de decisão e na coluna de ação, de acordo.

Para mudar o raio da procura para eventos correlatos, mude o valor de **Configurar raio de procura**. O número inteiro inserido é interpretado como metros a partir do centro do evento de origem. Assim, se você digitar 2000, ele se correlacionará somente com eventos que são inferiores a 2000 metros do evento de origem.

Mudando as Propriedades da Tabela de Decisão Procedimento

1. Efetue logon no http://app_server:9084/teamserver como rtsadmin.
2. Acesse o explorador do seu navegador.
3. Clique em **capCorrelationRules**.
4. Clique em **simpleCorrelationPolicy**.
5. Clique em **Editar**. A página de propriedades é exibida.
6. Clique em **Avançar** na página de propriedades.
7. Edite a tabela. Para exemplos de colunas que você pode incluir no tabela de decisão, consulte o modelo fornecido na pasta de modelos.
8. Ao concluir as alterações das propriedades para a tabela, clique em **Concluir**.

O que Fazer Depois

Exporte o aplicativo de regra do Centro de Decisão usando o link relacionado abaixo.

Tarefas relacionadas:

“Implementando o Conjunto de Regras Modificado para o Fluxo do IBM Intelligent Operations Center”
Use esse tópico para implementar o conjunto de regras modificado para o Rule Execution Server.

Implementando o Conjunto de Regras Modificado para o Fluxo do IBM Intelligent Operations Center

Use esse tópico para implementar o conjunto de regras modificado para o Rule Execution Server.

Sobre Esta Tarefa

Ao modificar quaisquer propriedades ou itens na tabela de decisão, você deve implementar o conjunto de regras modificado para o fluxo de evento no IBM Intelligent Operations Center. Após implementar o

conjunto de regras modificado para o Rule Execution Server, as regras de correlação funcionam diferentemente dependendo das suas mudanças. O Rule Execution Server verifica os eventos recebidos para possíveis correlações.

Para implementar o conjunto de regras modificado, conclua as seguintes etapas.

Procedimento

1. Exporte o aplicativo de regra do Centro de Decisão:
 - a. Acesse `app_server:9084/teamsrver/`.
 - b. Efetue logon como `rtsadmin`.
 - c. Navegue para **Projeto > Gerar Conjunto de Regras**.
 - d. Clique em **Avançar**, selecione nada e faça o download do arquivo jar RuleApp.
2. Importe o aplicativo de regra no Rule Execution Server:
 - a. Acesse `app_server:9083/res`.
 - b. Clique na guia Explorer.
 - c. Clique em `emicoc_wodm_correlation_ruleApp > Incluir Conjunto de Regras`.
 - d. Nomeie o conjunto de regras e anote o caminho do novo conjunto de regras:
`/icoc_wodm_correlation_ruleApp/1.0/yourChosenName/version`.
Onde
 - `yourChosenName` é o nome que você escolhe para o conjunto de regras
 - `version` é a versão do conjunto de regras
3. Configure o novo caminho do conjunto de regras configurado na política de impacto:
 - a. Acesse `event_server:9080/nci/login_main.jsp`.
 - b. No menu suspenso à esquerda, selecione IBM Intelligent Operations Center.
 - c. Clique em **Políticas**, e selecione a política **IOC_Event_Correlation**.
 - d. Mude o valor do campo: `JMSProps.ilog_rules_bres_mdb_rulesetPath` para o novo caminho:
`/icoc_wodm_correlation_ruleApp/1.0/yourChosenName/version`.
Onde
 - `yourChosenName` é o nome que você escolhe para o conjunto de regras
 - `version` é a versão do conjunto de regras
 - e. Clique em **Salvar**.

Tarefas relacionadas:

“Mudando as Propriedades da Tabela de Decisão” na página 175

Gerenciador de Mapa de Localização

Use o portlet Gerenciador de Mapa de Localização para customizar o portlet Mapa de Localização.

É possível customizar os seguintes aspectos do portlet Mapa de Localização:

- Nome de classificação a ser exibido no menu à esquerda do portlet.
- Mapa a ser exibido no portlet.
- Áreas em um mapa.

Áreas dentro de um mapa são identificadas por um código identificador de área. Todo evento com um código identificador de área aparece em todos os mapas de local com a área definida.

Há também uma opção para fornecer a uma área um identificador pai. É possível usar o identificador pai para criar uma hierarquia de área. Por exemplo, crie áreas para representar os assentos no primeiro piso de um estádio esportivo. Cada assento é definido no mapa de localização detalhado do primeiro piso do

estádio. Além disso, forneça a cada assento um identificador pai para indicar que está no primeiro piso do estádio. Um evento com um identificador de área para um dos assentos aparece no mapa de assento detalhado do primeiro piso. Esse evento também aparece em mapa da visão geral do estádio porque o primeiro piso tem o mesmo identificador de área que o usado como identificador pai para assentos.

Para acessar o portlet Gerenciador de Mapa de Localização, na interface de administração do WebSphere Portal, clique em **Intelligent Operations > Ferramentas de Customização > Gerenciador de Mapa de Localização**.

Incluindo uma Classificação no Menu do Mapa

Use a guia **Classificações** para incluir uma classificação para exibição no menu do mapa do portlet Mapa de Localização.

Procedimento

1. Insira um nome no campo **Nome da Classificação**. Você tem a opção de incluir uma descrição.
2. Para incluir sua classificação no portlet, clique em **Enviar**.

Resultados

Sua nova classificação aparecerá no portlet Mapa de Localização quando você atualizar a página de portlet.

Incluindo um Mapa no Portlet

Use a guia **Mapas de Localização** para incluir um mapa de localização para exibição no portlet Mapa de Localização.

Procedimento

1. Insira um nome no campo **Nome da Classificação**. É possível selecionar da lista suspensa.
2. Insira um nome do mapa de localização no campo **Nome do Mapa**. Você tem a opção de incluir uma descrição do mapa.
3. Insira uma URL para o mapa de localização no campo **Imagem**.
4. Para incluir seu mapa no menu, clique em **Enviar**.

Resultados

Seu mapa aparece no menu do portlet Mapa de Localização quando você atualiza a página do portlet. É possível selecionar e visualizar o mapa.

Incluindo ou Alterando Áreas em um Mapa de Localização

Use a guia **Áreas** para criar novas áreas, alterar áreas ou remover áreas para exibir em um mapa de localização no portlet Mapa de Localização.

Procedimento

1. Insira um nome de mapa no campo **Nome do Mapa**. É possível selecionar da lista suspensa de mapas.
2. Para arrastar uma nova área no mapa, clique no símbolo de polígono no canto superior direito da caixa. Clique na posição necessária no mapa e, em seguida, clique em cada canto para arrastar um polígono. Clique duas vezes para concluir o polígono. Por padrão, as novas áreas aparecem em verde.
3. Para inserir detalhes para uma área, clique no símbolo de mão no canto superior direito da caixa. Clique na área a ser atualizada.
4. Insira um nome de mapa da área no campo **Nome da Área**. Você tem a opção de incluir uma descrição.

5. Insira um identificador de área no campo **Identificador de Área**. Você tem a opção de incluir um identificador de área-pai.
6. Para atualizar uma área no mapa, clique em **Atualizar Área**. Para remover uma área no mapa, clique em **Remover Área**.
7. Para incluir suas mudanças no mapa, clique em **Enviar**.

Resultados

Suas mudanças aparecerão no portlet Mapa de Localização quando você atualizar a página de portlet.

Customizando o Portlet Gerenciador de Mapa de Localização

É possível customizar este portlet. Clique no botão no canto superior direito do portlet para ver as opções de customização do menu de portlet. As configurações compartilhadas afetam o conteúdo desse portlet para todos os usuários, mas apenas para esta ocorrência do portlet.

Conceitos relacionados:

“Mapa de Localização” na página 276

Utilize o portlet do Mapa de Localização para ver os eventos marcados em um mapa de localização. Um mapa de localização no IBM Intelligent Operations Center é um mapa ou plano com áreas pré-definidas para interação, por exemplo, áreas de assentos em um grande estádio esportivo.

Referências relacionadas:

“Configurações do Portlet do Gerenciador de Mapa de Localização” na página 156

Customize o portlet do Gerenciador de Mapa de Localização alterando as configurações nos campos da janela **Configurações Compartilhadas**.

Especificando Dados de Configuração para Todo o Sistema

A tabela de propriedades de sistema do IBM Intelligent Operations Center armazena dados de configuração do IBM Intelligent Operations Center.

As seguintes propriedades são para todo o sistema, usadas pelo IBM Intelligent Operations Center.

Tabela 63. Valores para Todo o Sistema, Utilizados pelo IBM Intelligent Operations Center

Região	Assunto	Nome	Tipo	Valor
Sistema	*	ActivityCollectionRefreshInterval	Integer	A taxa de atualização da coleção no servidor em segundos. O padrão é 300 (5 minutos). Essa propriedade afeta a taxa de atualização de serviço de UI para atividades.
Sistema	*	ActivityProviderEJBNDIName	Sequência	O nome da ligação JNDI da interface remota do provedor da atividade. Por meio dessa interface, é possível implementar o seu próprio provedor de atividades para funcionar com o seu processo ou sistema de gerenciamento de fluxo de trabalho. O provedor de atividades é um EJB que implementa a interface da atividade no <code>iss_common.jar</code> .
Sistema	*	AppMonitorPort	Sequência	Porta da web utilizada pelo Tivoli Monitoring.
Sistema	*	ApplicationServerHostname	Sequência	O nome do host ou endereço IP utilizado pelo servidor de aplicativos.

Tabela 63. Valores para Todo o Sistema, Utilizados pelo IBM Intelligent Operations Center (continuação)

Região	Assunto	Nome	Tipo	Valor
Sistema	*	CollectionRefreshInterval	Integer	A taxa de atualização da coleção no servidor em segundos. O padrão é 15 segundos. Essa propriedade afeta a taxa de atualização de serviço de UI para eventos e notificações.
Sistema	*	DatabaseServerHostname	Sequência	O nome do host ou endereço IP utilizado pelo servidor de dados.
Sistema	*	DateFormat	Sequência	O formato usado quando o IBM Intelligent Operations Center exibe a data. O padrão é aaaa-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 aaaa-MM-dd HH:mm:ss. Qualquer padrão Java <code>java.text.SimpleDateFormat</code> válido de data e hora pode ser especificado.
Sistema	*	DisableTSRMSync	Booleano	Especifica se a sincronização do Tivoli Service Request Manager está desativada. O padrão é false. Configure para true se uma implementação não tiver a instalação do Tivoli Service Request Manager.
Sistema	*	EventContainerDeleteEvent	Sequência	Especifica se um evento é excluído do banco de dados do Servidor de Objeto do Tivoli Netcool/OMNIBus. A exclusão é implementada pela política do Tivoli Netcool/Impact quando o banco de dados do IBM Intelligent Operations Center é atualizado com um evento. O padrão é true. Se o valor for true, o evento é limpo do banco de dados do Servidor de Objeto. Se o valor for false, o evento não é limpo do banco de dados do Servidor de Objeto.
Sistema	*	EventRouterPollDelay	Integer	O atraso em milissegundos entre intervalo de pesquisa de UI. O atraso é o número de milissegundos antes do próximo intervalo de pesquisa. O padrão é 0.
Sistema	*	EventRouterPollErrorDelay	Integer	O atraso em milissegundos entre intervalos de pesquisa de UI após a ocorrência de um erro. O atraso é o número de milissegundos após um erro e antes do próximo intervalo de pesquisa. O padrão é 5000.
Sistema	*	EventRouterTimeout	Integer	O intervalo de pesquisa de UI em segundos. O intervalo de pesquisa é o intervalo de tempo durante o qual pesquisar eventos antes do tempo limite. O padrão é 20.

Tabela 63. Valores para Todo o Sistema, Utilizados pelo IBM Intelligent Operations Center (continuação)

Região	Assunto	Nome	Tipo	Valor
Sistema	*	EventServerHostname	Sequência	O nome do host ou endereço IP utilizado pelo .
Sistema	*	MgmtServerHostname	Sequência	O nome do host ou endereço IP utilizado pelo Servidor de Gerenciamento.
Sistema	*	ModelManagerServerEJBPort	Sequência	Porta EJB utilizada pelo serviços de modelo semântico.
Sistema	*	ModelManagerServerHostname	Sequência	Nome de host ou endereço IP utilizado pelo serviços de modelo semântico.
Sistema	*	MonitorServerHostname	Sequência	Nome de host ou endereço IP utilizado pelo IBM WebSphere Business Monitor.
Sistema	*	MonitorServerWebPort	Sequência	A porta da Web utilizada pelo Gateway de Serviços REST do IBM WebSphere Business Monitor.
Sistema	*	MonitorServerSecurityEnabled	Booleano	Especifica se a conexão como IBM WebSphere Business Monitor usa SSL para conexão HTTP segura. O padrão é true. Se o valor for true, a conexão usa SSL Se o valor for false, a conexão não usa SSL.
Sistema	*	PortalServerHostname	Sequência	Nome de host ou endereço IP usado pelo WebSphere Portal Server.
Sistema	*	PortalServerWebPort	Sequência	A porta da web usada pelo WebSphere Portal Server.
Sistema	*	RegExpEmail	Sistema	A expressão regular utilizada para validar um endereço de e-mail. O padrão é .+.
Sistema	*	RegExpTelephone	Sistema	Expressão regular usada para validar um número de telefone. O padrão é .+.
Sistema	*	SecurityUserPrefix	Sequência	O prefixo do ID do usuário utilizado para mapear o usuário ao nome distinto de LDAP. O padrão é uid.
Sistema	*	SecurityUserSuffix	Sequência	O sufixo do ID do usuário utilizado para mapear o usuário para um nome distinto LDAP ou para um nome distinto local. O padrão, utilizado ao executar um portal com a segurança LDAP, é ou=users,ou=SWG,o=IBM,c=US. Configure o valor para o=defaultWIMFileBasedRealm ao executar um portal local com segurança LDAP.
Sistema	*	TdsPort	Sequência	A porta da web usada pelo Tivoli Directory Server Web Administration Tool
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 java.text.SimpleDateFormat pode ser especificado.
Sistema	*	TSRMDirectServerHostname	Sequência	Nome de host ou endereço IP utilizado pelo Tivoli Service Request Manager.

Tabela 63. Valores para Todo o Sistema, Utilizados pelo IBM Intelligent Operations Center (continuação)

Região	Assunto	Nome	Tipo	Valor
Sistema	*	TSRMDirectServerWebPort	Sequência	Porta da web utilizada pelo Tivoli Service Request Manager.
Sistema	*	TSRMServerActivityUri	Sequência	A URI de atividade e de aplicativo de tarefas utilizadas por Tivoli Service Request Manager. O padrão é /tsrm/maximo/ui/maximo?event=loadapp&value=Activity&uniqueid={0}. O valor do ID de atividade é substituído por {0}.
Sistema	*	TSRMServerResourceAddUri		A URI do recurso de inclusão utilizada por Tivoli Service Request Manager. O padrão é /tsrm/maximo/ui/maximo?event=loadapp&value=plusires&additional=event=INSERT. O valor do ID do recurso externo é substituído por {0}.
Sistema	*	TSRMServerResourceDeleteUri		A URI do recurso de exclusão utilizada por Tivoli Service Request Manager. O padrão é /tsrm/maximo/ui/maximo?event=loadapp&value=plusires&additional=event=useqbe&additional=eventvalue=LOCATION={0}. O valor do ID do recurso externo é substituído por {0}.
Sistema	*	TSRMServerResourcePropertiesUri		A URI das propriedades de recursos utilizada por Tivoli Service Request Manager. O padrão é /tsrm/maximo/ui/maximo?event=loadapp&value=plusires&additional=event=useqbe&additional=eventvalue=LOCATION={0}. O valor do ID do recurso externo é substituído por {0}.
Sistema	*	TSRMServerResourceUpdateUri		A URI do recurso de atualização utilizada por Tivoli Service Request Manager. O padrão é /tsrm/maximo/ui/maximo?event=loadapp&value=plusires&additional=event=useqbe&additional=eventvalue=LOCATION={0}. O valor do ID do recurso externo é substituído por {0}.
Sistema	*	TSRMServerSecurityEnabled	Booleano	Especifica se a conexão HTTP com o Tivoli Service Request Manager usará SSL. O padrão é false. Se o valor for true, a conexão usa SSL Se o valor for false, a conexão não usa SSL.
Sistema	*	TSRMServerWorkflowUri	Sequência	URI do fluxo de trabalho usado pelo Tivoli Service Request Manager. O padrão é /maximo/ui/?event=loadapp&value=sr&&additional=event=useqbe&additional=eventvalue=TICKETID={0}. O valor do ID de incidente é substituído por {0}.

Tabela 63. Valores para Todo o Sistema, Utilizados pelo IBM Intelligent Operations Center (continuação)

Região	Assunto	Nome	Tipo	Valor
Sistema	*	UseDBModelReader	Booleano	Especifica se o modelo de banco de dados da KPI é lido a partir de um arquivo RDF. O padrão é true. Se o valor for true, o modelo KPI não é lido de um arquivo RDF. Se o valor for false, o modelo KPI é lido de um arquivo RDF.
Sistema	*	WebSEALServerHostname	Sequência	Nome de host ou endereço IP utilizado pelo Tivoli Access Manager WebSEAL.

As propriedades a seguir podem ser alteradas para configurar como os KPIs são processados.

Tabela 64. Propriedades que Afetam o Processamento do KPI

Região	Assunto	Nome	Tipo	Valor
KPI	*	CacheKpis	Booleano	Especifica se os KPIs recuperados do IBM WebSphere Business Monitor são armazenados em cache. O padrão é true. Se o valor for true, os KPIs são armazenados em cache para reutilização. Com que frequência o cache é atualizado é especificado por KpiCacheRefreshInterval. Se o valor for false, os KPIs são sempre recuperados a partir do IBM WebSphere Business Monitor quando o IBM Intelligent Operations Center solicita informações de KPI.
KPI	*	KpiCacheRefreshInterval	Integer	Especifica a frequência de atualização do cache de KPI. O intervalo é especificado em segundos. O padrão é 300 (5 minutos). KpiCacheRefreshInterval será ignorado se CacheKpis for especificado como false.
KPI	*	KpiSentToGroup	Sequência	Especifica os grupos que recebem notificações de KPI. Separe os nomes de grupo com ponto-e-vírgula (;). O valor padrão é CityWideExecutive;CityWideSupervisor.
KPI	*	PreLoadKpis	Booleano	Especifica se os KPIs são recuperados a partir do IBM WebSphere Business Monitor quando o IBM Intelligent Operations Center inicia. O padrão é true. Se true, todos os KPIs são recuperados do IBM WebSphere Business Monitor quando o IBM Intelligent Operations Center for iniciado. KPIs são armazenadas em cache para reuso. O KpiCacheRefreshInterval especifica com que frequência o cache é atualizado. Se false, KPIs são recuperadas a partir do IBM WebSphere Business Monitor apenas quando o IBM Intelligent Operations Center informações da KPI. Nota: Se o PreLoadKpis for true, então o CacheKpis será considerado true não importando seu valor especificado.

Atualizando a Tabela de Propriedades do Sistema

Para mudar os dados de configuração do IBM Intelligent Operations Center no sistema inteiro, atualize a tabela de propriedades do sistema.

Sobre Esta Tarefa

Use um cliente VNC para efetuar logon no servidor de banco e dados do servidor de dados e abra uma janela de comando. No procedimento a seguir, insira comandos na janela de comando.

Procedimento

1. Efetue logon no servidor de dados como raiz
2. Para abrir o Centro do Controle do DB2®, temporariamente desligue o controle de acesso; insira os comandos:

```
xhost +  
su - db2inst1  
db2cc
```
3. No Centro de Controle do DB2, abra a tabela de propriedades do sistema:
 - a. Para abrir o Centro de Controle do DB2, insira o seguinte comando: - db2cc
 - b. No Centro de Controle do DB2, clique em **Todos os Bancos de Dados > IOCCDB > Tabelas > SYSPROP**.
 - c. Clique com o botão direito do mouse na tabela **SYSPROP**, e depois clique em **Abrir**.
 - d. Modifique o campo necessário e clique em **Confirmar**
 - e. Feche a tabela.
4. Feche o Centro de Controle do DB2.
5. Para retornar para o usuário raiz, insira o comando: **exit**
6. Para ativar o controle de acesso novamente, insira o comando: **xhost-**

Nota: Para implementar as mudanças feitas, você deve reiniciar o servidor de portal. É possível reiniciar o servidor de portal com o script IOCCControl. Para obter informações sobre como iniciar os serviços, consulte o link no final deste tópico.

Tarefas relacionadas:

“Iniciando os Serviços” na página 195

O Ferramenta de Controle de Plataforma está disponível para iniciar os serviços em execução nos servidores IBM Intelligent Operations Center.

Configurando o IBM Cognos Business Intelligence para Criar Relatórios

O IBM Intelligent Operations Center fornece um subsistema de relatórios que utiliza o IBM Cognos Business Intelligence para criar e gerenciar relatórios. O IBM Intelligent Operations Center acompanha uma página de relatórios que pode exibir até seis relatórios. Também é possível criar uma página de relatórios manualmente e customizar o layout do portlet.

O subsistema de relatório é instalado noservidor de aplicativos e usa um modelo de dados analítico.

Criando um Portlet Relatórios

Use as informações nesse tópico para criar uma página de portlet Relatórios, copiando um portlet existente usando o console do IBM Intelligent Operations Center.

Sobre Esta Tarefa

Para copiar um portlet existente e configurar propriedades para criar uma nova página de relatório, conclua as seguintes etapas.

Procedimento

1. Efetue logon no IBM Intelligent Operations Center como um administrador.
2. Navegue para **Administração > Gerenciamento de Portlets > Portlets**.
3. No campo **Procurar**, insira **Relatórios** e clique em **Procurar**. A janela do portlet **Relatórios** é exibida.
4. Além do portlet que deseja copiar, clique no ícone **Copiar Portlet**. A janela do portlet **Copiar** é exibida.
5. Para o nome do novo portlet, insira **CognosReport**.
6. Clique em **OK**. O novo portlet é exibido na janela **Gerenciar Portlets**.
7. Navegue até **Administração > Interface com o Usuário do Portal > Gerenciar Páginas**.
8. Clique em **Raiz do Conteúdo > Cidade** e clique na guia **Nova Página**. A página **Propriedades da Página** é exibida.
9. Insira as propriedades a seguir para a nova página do relatório:
 - a. No campo **Título**, insira um título para a página do relatório. Um título de exemplo é **Operador: Relatórios**.
 - b. No campo **Nome Exclusivo**, insira um nome que identifique especificamente esta página do relatório. Um nome exclusivo de exemplo é `com.ibm.iss.ioc.citywide.OperatorReports`.
 - c. No campo **Nome Fácil da URL**, insira **relatório**.
 - d. No campo **Tema**, aceite o padrão **Herdar Tema Pai**.
 - e. No campo **Estilo do Tema**, aceite o padrão **Herdar Política do Tema Pai**.
 - f. Em **Modo de Renderizar Agregação**, selecione **Herdar Renderização Pai**.
 - g. Clique em **OK**.

A nova página de relatório é incluída na lista de páginas do portlet.

Editando o Layout do Portlet de Relatórios

Utilize estas etapas para formatar o layout da página do portlet de Relatórios.

Sobre Esta Tarefa

Para selecionar o layout da página do portlet de Relatórios utilizando o console do IBM Intelligent Operations Center, conclua as seguintes etapas.

Procedimento

1. Efetue logon no IBM Intelligent Operations Center como um administrador.
2. Navegue até **Administração > Interface com o Usuário do Portal > Gerenciar Páginas**.
3. Próximo à página que deseja editar, clique no ícone **Editar Layout da Página**. A página **Editar Layout** é exibida.
4. Selecione o ícone de layout que possui as páginas lado a lado com uma linha sob as páginas. Este é o quinto ícone a partir da esquerda.
5. No mesmo quadro onde deseja incluir o portlet, clique em **Incluir Portlets**.
6. Procure e marque a caixa de seleção **CognosPortlet** e clique em **OK** para incluir o portlet no layout da página. Uma mensagem é exibida confirmando que o portlet foi incluído.
7. Repita as etapas 5 e 6 para incluir portlets adicionais. É possível adicionar até seis portlets.
8. Clique em **Pronto**.

O que Fazer Depois

É possível editar as configurações compartilhadas para cada portlet. No canto superior direito do portlet que deseja editar, clique na seta e selecione **Editar Configurações Compartilhadas** no menu. Para obter informações adicionais, consulte “Customizando um Portlet para Exibir Relatórios” na página 185.

Customizando um Portlet para Exibir Relatórios

Utilize as informações deste tópico para customizar um portlet do IBM Intelligent Operations Center para exibir relatórios do IBM Cognos Business Intelligence.

Procedimento

1. Efetue logon no portal de soluções como administrador.
2. Selecione a visualização e o portlet que deseja customizar para exibir relatórios.
3. Navegue até o menu de exibição do portlet no canto superior direito do portlet.
4. Clique em **Editar Configurações Compartilhadas**.
5. Insira suas configurações nos campos fornecidos.
 - a. Insira um título para o relatório.
 - b. Insira a **URL** para o relatório. Localize a URL requerida, conforme descrito no tópico do “Localizando a URL do Relatório”.
Example: CAP_events_by_type_status_and_date:
`http://9.161.84.100:9082/ServletGateway/servlet/Gateway?b_action=cognosViewer&ui.action=run&ui.object=%2fcontent%2fpackage%5b%40name%3d%27ioc_model%27%5d%2ffolder%5b%40name%3d%27reports%27%5d%2freport%5b%40name%3d%27CAP_events_by_type_status_and_date%27%5d&ui.name=CAP_events_by_type_status_and_date&run.outputFormat=&run.prompt=true`
 - c. Configure o portal **Largura** para 600.
 - d. Configure o portal **Altura** para 600.
 - e. Clique em **Salvar**.
 - f. No menu de exibição do portlet, clique em **Voltar** para retornar à visualização do portlet principal.

Resultados

O portlet Relatórios é atualizado para exibir o relatório recém-selecionado.

Localizando a URL do Relatório

Este tópico fornece as etapas para localizar a URL de um relatório.

Procedimento

1. Efetue o logon no IBM Cognos Connection.
2. Navegue até **Pastas Públicas > ioc_model > relatórios**.
3. Selecione um relatório e clique no ícone **Configurar Propriedades**.
4. Na guia **Geral**, clique em **Visualizar o Caminho de Procura, ID e URL** para visualizar a URL do relatório.
5. Na seção **URL de Ação Padrão**, copie a URL e cole-a no portlet, conforme necessário.

Trabalhando com Modelo de Dados

O IBM Intelligent Operations Center fornece dois modelos de dados utilizados ao gerar relatórios. Um metamodelo define o idioma e os processos a partir dos quais formar um modelo.

Os relatórios do IBM Intelligent Operations Center são construídos sobre dois modelos de dados.

- Modelo de Dados de Esquema Comum
- Modelo de Dados de Esquema do Common Alerting Protocol (CAP)

Ambos os modelos de dados do IBM Intelligent Operations Center são organizados como camadas. Para os autores do relatório, a Visualização Apresentação ou camada é disponibilizada e consiste nos namespaces a seguir:

Business

Contém dicionários, filtros e dados.

Dimensional

Contém dimensões de evento para relatórios e análise.

Consulta Customizada

Contém assuntos de consulta que podem ser usados para a construção de consultas customizadas para relatórios relacionais.

Gerando os Relatórios de Modelos de Dados de Esquema Comuns

Esse tópico descreve como gerar os relatórios de modelos de dados de esquema comuns. Esses relatórios ajudam os gerentes e supervisores a monitorarem eventos atuais, reagirem a eventos que estão acontecendo e a se planejarem para eventos futuros.

Sobre Esta Tarefa

Usando o console do IBM Intelligent Operations Center, conclua essas etapas para gerar relatórios de modelos de dados de esquema comuns. Consulte os links de referência no final desse tópico para obter uma descrição das opções para gerar um relatório.

Procedimento

1. Na guia Administração do console do IBM Intelligent Operations Center, clique em **Intelligent Operations > Ferramentas de Administração > Consoles de Administração**. A página Consoles de Administração é exibida.
2. Em Servidor de Aplicativos, clique em **Administração de Relatório**. A página IBM Cognos Connection é exibida.
3. Clique em **modelo comum de ioc**. As pastas públicas do Cognos são exibidas.
4. Clique em **Relatórios**.
5. Selecione o tipo de relatório que deseja gerar:
 - Para gerar um relatório de gráfico de pizza, clique em **Gráficos de Pizza**. Os relatórios de gráficos de pizza de esquema comuns são exibidos.
 - Para gerar um relatório de gráfico de tabela, clique em **Gráficos de Tabelas**. Os relatórios de gráficos de tabela de esquema comum são exibidos.
6. Selecione o relatório que deseja gerar.

Opções de Gráficos de Pizza:

Esse tópico fornece as opções possíveis de selecionar para os relatórios de gráficos de pizza comuns.

Para acessar os relatórios de gráficos de pizza a partir da página IBM Cognos Connection, clique em **Pastas Públicas > ioc_common_model > relatórios > Gráficos de Pizza**.

Tabela 65. Opções de gráficos de pizza para os relatórios de modelos de dados de esquema comuns

Relatório	Descrição
Evento por Categoria	Exibe eventos com base na categoria de evento. Por exemplo, é possível visualizar todos os eventos ambientais, de incêndio ou de transporte.
Evento por Segurança	Exibe eventos com base na probabilidade de eles ocorrerem. Por exemplo, se ocorreu um acidente de trânsito, a certeza pode ser "observada."
Evento por Data de Envio	Esse relatório mostra eventos que foram enviados em uma data específica.

Tabela 65. Opções de gráficos de pizza para os relatórios de modelos de dados de esquema comuns (continuação)

Relatório	Descrição
Evento por Tipo de Evento	Exibe eventos com base no tipo. Por exemplo, o evento pode ser um tornado se aproximando ou um acidente de trânsito.
Evento por Título	Exibe eventos pela descrição inserida para o evento quando o evento foi criado. Portanto, o título é de fato a descrição do evento.
Evento por Severidade	Exibe eventos com base na severidade. Por exemplo, os eventos podem ser extremos ou graves.
Evento por Especificação	Exibe eventos por especificação. Por exemplo, um evento pode ser um evento Protocolo de Alerta Comum ou non-Common Alerting Protocol. Portanto, esse gráfico mostra a porcentagem de eventos Protocolo de Alerta Comum e non-Common Alerting Protocol.
Evento por Urgência	Exibe eventos com base em sua urgência. Por exemplo, o evento pode estar ocorrendo e pode ser descrito como "imediatos".
Evento por URL	Exibe eventos pela URL inserida para o evento quando o evento foi criado.

Opções de Gráficos de Tabela:

Esse tópico descreve as informações possíveis de gerar para os relatórios de gráficos de tabela comuns.

Para acessar relatórios de gráficos de tabela a partir da página IBM Cognos Connection, clique em **Pastas Públicas > ioc_common_model > relatórios > Gráficos de Pizza**.

A única opção de gráfico de tabela para relatórios de modelos de dados de esquema comuns é a Lista de Eventos. A lista de eventos fornece uma lista completa de eventos com informações detalhadas para cada evento. Alguns exemplos de informações sobre a lista de eventos são explicados a seguir.

Tabela 66. Informações da lista de eventos para gráficos de tabela comuns

Campo de relatório	Descrição
ID	Identifica o relatório
ID de evento externo	O ID de evento gerado quando o evento foi criado.
Especificação	Especifica se o evento é um evento Protocolo de Alerta Comum ou não Protocolo de Alerta Comum.
Tipo de evento	Exibe eventos com base no tipo. Por exemplo, o evento pode ser um tornado se aproximando ou um acidente de trânsito.
Enviado	A data e hora em que o evento foi enviado.
Título	A descrição do evento.
Categoria	Exibe eventos com base na categoria de evento. Por exemplo, é possível visualizar todos os eventos ambientais, de incêndio ou de transporte.
Certeza	Exibe eventos com base na probabilidade de eles ocorrerem. Por exemplo, se ocorreu um acidente de trânsito, a certeza pode ser "observada."
Severidade	Exibe eventos com base na severidade. Por exemplo, os eventos podem ser extremos ou graves.

Tabela 66. Informações da lista de eventos para gráficos de tabela comuns (continuação)

Campo de relatório	Descrição
Urgência	Exibe eventos com base em sua urgência. Por exemplo, o evento pode estar ocorrendo e pode ser descrito como "imediatos".
Url	A URL associada ao relatório.

Gerando os Relatórios de Modelos de Dados de Esquema do Protocolo de Alerta Comum

Esse tópico descreve como gerar os relatórios de modelos de dados de esquema do Protocolo de Alerta Comum. Esses relatórios ajudam os gerentes e supervisores a monitorarem eventos atuais, reagirem a eventos que estão acontecendo e a se planejarem para eventos futuros.

Sobre Esta Tarefa

Usando o console do IBM Intelligent Operations Center, conclua essas etapas para gerar relatórios de modelos de dados de esquema do Protocolo de Alerta Comum. Consulte os links de referência no final desse tópico para obter uma descrição das opções para gerar um relatório.

Procedimento

1. Na guia Administração do console do IBM Intelligent Operations Center, clique em **Intelligent Operations > Ferramentas de Administração > Consoles de Administração**. A página Consoles de Administração é exibida.
2. Em Servidor de Aplicativos, clique em **Administração de Relatório**. A página IBM Cognos Connection é exibida.
3. Clique em **modelo de ioc cap**. As pastas públicas do Cognos são exibidas.
4. Clique em **Relatórios**.
5. Selecione o tipo de relatório que deseja gerar:
 - Para gerar o relatório de modelo de dados listado nesta página, selecione o relatório.
 - Para gerar um relatório de gráfico de pizza, clique em **Gráficos de Pizza**. Os relatórios de gráficos de pizza de esquema comuns são exibidos. Selecione o relatório da lista.
 - Para gerar um relatório definido pelo usuário, clique em **Relatórios Definidos pelo Usuário**. A página Relatório Customizado do Cognos é exibida. Preencha os campos para o relatório customizado e clique em **Atualizar**.

Opções de Relatórios de Modelos de Dados:

Esse tópico descreve as opções possíveis de selecionar para gerar um relatório do Protocolo de Alerta Comum.

Para acessar essas opções de relatório a partir da página IBM Cognos Connection, clique em **Pastas Públicas > ioc_cap_model > relatórios**.

Tabela 67. Opções para informações sobre os relatórios do Protocolo de Alerta Comum

Relatório	Descrição
Eventos do Protocolo de Alerta Comum por tipo, status e data	Esse relatório mostra eventos do Protocolo de Alerta Comum por tipo de evento, status do evento e data do evento. Por exemplo, o tipo de evento pode ser acidente e o status pode ser urgente. A data pode ser a data de hoje.

Tabela 67. Opções para informações sobre os relatórios do Protocolo de Alerta Comum (continuação)

Relatório	Descrição
Métricas de KPI de eventos do Protocolo de Alerta Comum por data	Esse relatório mostra eventos do Protocolo de Alerta Comum baseados em métricas de KPI para uma determinada data ou intervalo de datas.
Métricas de KPI de eventos do Protocolo de Alerta Comum por departamento	Esse relatório mostra eventos do Protocolo de Alerta Comum baseados em métricas de KPI para um determinado departamento ou área. Por exemplo, o relatório pode mostrar métricas de KPI para o departamento de água ou para uma determinada área de uma cidade.
Detalhes completos do Protocolo de Alerta Comum	Esse relatório mostra detalhes completos sobre eventos do Protocolo de Alerta Comum. Por exemplo, os detalhes incluem o ID do Protocolo de Alerta Comum, o emissor, a data e hora de envio, status, tipo de mensagem, origem de outros.
Eventos do IBM Intelligent Operations Center por gravidade a qualquer momento	Esse relatório lista todos os eventos do IBM Intelligent Operations Center baseados em sua gravidade. Por exemplo, os eventos podem ser extremos.
Eventos do IBM Intelligent Operations Center por gravidade em andamento	Esse relatório lista todos os eventos do IBM Intelligent Operations Center que estão ocorrendo atualmente, por gravidade. Por exemplo, a gravidade em andamento pode ser uma condição climática extrema que está ocorrendo.

Opções de Gráficos de Pizza:

Esse tópico descreve as opções existentes para gerar relatórios de gráficos de pizza do Protocolo de Alerta Comum.

Para acessar os relatórios de gráficos de pizza a partir da página IBM Cognos Connection, clique em **Pastas Públicas > ioc_cap_model > relatórios > Gráficos de Pizza**.

Tabela 68. Opções para informações sobre relatórios de gráficos de pizza do Protocolo de Alerta Comum

Relatório	Descrição
Cap por categoria	Exibe Protocolo de Alerta Comum por uma categoria específica. Por exemplo, é possível visualizar todos os eventos ambientais, de incêndio ou de transporte.
Cap por certeza	Exibe eventos do Protocolo de Alerta Comum baseados em sua probabilidade de ocorrência. Por exemplo, se ocorreu um acidente de trânsito, a certeza pode ser "observada."
Cap por data de envio	Exibe eventos do Protocolo de Alerta Comum enviados em uma data específica.
Cap por tipo de evento	Exibe eventos do Protocolo de Alerta Comum baseados em tipo. Por exemplo, o evento pode ser um tornado se aproximando ou um acidente de trânsito.
Cap por código de manipulação	Exibe eventos do Protocolo de Alerta Comum por código de manipulação. Por exemplo, o código de manipulação pode ser "evento."
Cap por tipo de mensagem	Exibe eventos do Protocolo de Alerta Comum baseados em tipos de mensagens, tais como atualizações e alertas.

Tabela 68. Opções para informações sobre relatórios de gráficos de pizza do Protocolo de Alerta Comum (continuação)

Relatório	Descrição
Cap por escopo	Exibe eventos do Protocolo de Alerta Comum por escopo. Por exemplo, um evento por escopo pode ser "público".
Cap por emissor	Exibe eventos do Protocolo de Alerta Comum por nome do emissor.
Cap por gravidade	Exibe eventos do Protocolo de Alerta Comum baseados em gravidade. Por exemplo, os eventos podem ser extremos ou graves.
Cap por origem	Exibe Protocolo de Alerta Comum por uma origem específica. Por exemplo, a origem pode ser transporte.
Cap por status	Exibe eventos do Protocolo de Alerta Comum por status. Os status são: <ul style="list-style-type: none"> • Aceitável • Cuidado • Execute uma ação
Cap por urgência	Exibe eventos do Protocolo de Alerta Comum baseados em sua urgência. Por exemplo, o evento pode estar ocorrendo e ser descrito como "imediate".
Notificação por categoria	Exibe mensagens de alerta em formato de Protocolo de Alerta Comum por uma categoria específica. Por exemplo, é possível visualizar todos os eventos ambientais, de incêndio ou de transporte.
Notificação por tipo	Exibe notificações em formato de Protocolo de Alerta Comum por tipo. Por exemplo, o tipo pode ser atualizações e alertas.

Opções de Relatórios de Eventos Definidos pelo Usuário:

Esse tópico descreve as opções existentes para gerar relatórios definidos pelo usuário do Protocolo de Alerta Comum para eventos.

Para acessar os relatórios definidos pelo usuário a partir da página IBM Cognos Connection, clique em **Pastas Públicas > ioc_cap_model > relatórios > Relatórios Definidos pelo Usuário > Eventos**.

Tabela 69. Opções de eventos do Protocolo de Alerta Comum

Relatório	Descrição
Eventos por Categoria a Qualquer Momento	Exibe todos os eventos por categoria, independentemente da data. Por exemplo, é possível visualizar todos os eventos ambientais, de incêndio ou de transporte.
Eventos por Certeza a Qualquer Momento	Exibe todos os eventos por certeza, independentemente da data. Por exemplo, se ocorreu um acidente de trânsito, a certeza pode ser "observada."
Eventos por Tipo de Evento a Qualquer Momento	Exibe todos os eventos por tipo de evento, independentemente da data. Por exemplo, os eventos podem ser um tornado que se aproxima ou um acidente de trânsito que ocorreu em qualquer data.
Eventos por Gravidade a Qualquer Momento	Exibe todos os eventos por gravidade, independentemente da data. Por exemplo, são exibidos eventos extremos ou graves para qualquer data.

Tabela 69. Opções de eventos do Protocolo de Alerta Comum (continuação)

Relatório	Descrição
Eventos por Urgência a Qualquer Momento	Exibe todos os eventos por urgência, independentemente da data. Por exemplo, os eventos podem estar ocorrendo e serem descritos como "imediatos".

Opções de Relatórios Customizados Definidos pelo Usuário:

Esse tópico descreve as opções existentes para gerar relatórios customizados definidos pelo usuário do Protocolo de Alerta Comum.

É possível criar um relatório customizado para eventos usando o portlet Relatórios. Comece selecionando como deseja agrupar eventos. Por exemplo, para visualizar todos os eventos por uma categoria específica, selecione **Categoria** no campo **Agrupar por**. Em seguida, nos campos **Selecionar Dados**, escolha os dados específicos das informações que deseja visualizar. Também é possível indicar uma data ou intervalo de datas para os eventos no relatório. Clique em **Atualizar** e o gráfico muda para refletir as informações solicitadas.

Para recuperar a URL para o novo relatório, clique em **URL para Este Relatório**.

Para acessar os relatórios definidos pelo usuário customizados a partir da página IBM Cognos Connection, clique em **Pastas Públicas > ioc_cap_model > relatórios > Relatórios Definidos pelo Usuário > Relatório Definido pelo Usuário**.

Tabela 70. Opções customizadas definidas pelo usuário do Protocolo de Alerta Comum

Relatório	Descrição
Agrupar por	Selecione a opção pela qual deseja agrupar eventos.
Severidade	Exibe eventos com base na severidade. Por exemplo, os eventos podem ser extremos ou graves.
Certeza	Exibe eventos com base na probabilidade de eles ocorrerem. Por exemplo, se ocorreu um acidente de trânsito, a certeza pode ser "observada."
Urgência	Exibe eventos com base em sua urgência. Por exemplo, o evento pode estar ocorrendo e pode ser descrito como "imediato".
Categoria da Ocorrência	Exibe eventos com base na categoria de evento. Por exemplo, é possível visualizar todos os eventos ambientais, de incêndio ou de transporte.
Tipo de Ocorrência	Exibe eventos com base no tipo. Por exemplo, o evento pode ser um tornado se aproximando ou um acidente de trânsito.
Data Inicial	Insira a data para a qual você está visualizando eventos. Para um intervalo de datas, insira a data de início.
À data	Insira a data através da qual você está visualizando eventos.

Configurando Relatórios de Modelos de Dados de Esquema Comuns

Use esse tópico para configurar propriedades gerais e específicas para relatórios de modelos de dados de esquema comuns.

Antes de Iniciar

Você deve ter acesso de Administrador para executar esse procedimento.

Sobre Esta Tarefa

Use o console do IBM Intelligent Operations Center para configurar esses relatórios.

Procedimento

1. Na guia Administração do console do IBM Intelligent Operations Center, clique em **Intelligent Operations > Ferramentas de Administração > Consoles de Administração**. A página Consoles de Administração é exibida.
2. Em Servidor de Aplicativos, clique em **Administração de Relatório**. A página IBM Cognos Connection é exibida.
3. Selecione a caixa de seleção **modelo comum de ioc** e, em seguida, clique em **Mais**. A página Ações Disponíveis é exibida.
4. Clique em **Configurar Propriedades**. A página Propriedades Gerais é exibida.
5. Selecione os valores para as propriedades gerais do relatório.
6. Na guia Permissões, selecione as permissões para os relatórios de modelos de dados de esquema comuns.
7. Na guia Recursos, selecione os recursos para os relatórios.
8. Clique em **OK**.

Configurando Relatórios de Modelos de Dados de Esquema do Protocolo de Alerta Comum

Use esse tópico para configurar propriedades gerais, configurar permissões e designar recursos a tipos de usuários para relatórios de modelos de dados de esquema do Protocolo de Alerta Comum.

Antes de Iniciar

Você deve ter acesso de Administrador para executar esse procedimento.

Sobre Esta Tarefa

Use o console do IBM Intelligent Operations Center para configurar esses relatórios.

Procedimento

1. Na guia Administração do console do IBM Intelligent Operations Center, clique em **Intelligent Operations > Ferramentas de Administração > Consoles de Administração**. A página Consoles de Administração é exibida.
2. Em Servidor de Aplicativos, clique em **Administração de Relatório**. A página IBM Cognos Connection é exibida.
3. Selecione a caixa de seleção **modelo de ioc cap** e, em seguida, clique em **Mais**. A página Ações Disponíveis é exibida.
4. Clique em **Configurar Propriedades**. A página Propriedades Gerais é exibida.
5. Selecione os valores para as propriedades gerais do relatório.
6. Na guia Permissões, selecione as permissões para os relatórios de modelos de dados de esquema do Protocolo de Alerta Comum.
7. Na guia Recursos, selecione os recursos para os usuários dos relatórios.
8. Clique em **OK**.

Mais Opções de Relatórios

Esse tópico descreve opções de relatórios adicionais para relatórios comuns e Protocolo de Alerta Comum.

Para acessar essas opções, clique em **Mais**, à direita do link para um relatório específico.

Tabela 71. Opções adicionais disponíveis para cada relatório

Opção	Descrição
Configurar propriedades	Configure propriedades gerais para o relatório escolhido.
Visualizar versão de saída do relatório	Escolha a versão de saída para visualizar, clicando em um hiperlink de formato.
Visualizar minhas permissões	Visualize as permissões de acesso que você possui para esta entrada.
Executar com opções	Selecione como deseja executar e receber o relatório. Os exemplos incluem HTML e PDF.
Abrir com o Report Studio	Exibe o relatório em outro navegador usando o Report Studio.
Abrir com o Business Insight Advanced	Exibe o relatório em outro navegador usando o IBM Cognos Business Insight Advanced.
Novo planejamento	Planeja um relatório com base em vários critérios.
Mover	Move um relatório para um local diferente.
Copiar	Copia um relatório de um local para outro.
Criar um atalho para esta entrada	Cria um atalho em sua área de trabalho para acessar o relatório.
Criar uma visualização de relatório desse relatório	Cria uma visualização em sua área de trabalho para este relatório que é armazenada em um diretório local.
Excluir	Exclui um relatório que é exibido.

Capítulo 6. Gerenciando a Solução

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

Sobre

Use o portlet Sobre para visualizar detalhes da versão do IBM Intelligent Operations Center e IBM Smarter Cities Software Solutions integrado que você instalou. Também é possível visualizar detalhes de quaisquer atualizações aplicadas desde sua instalação.

Para ativar o portlet Sobre, na interface de administração do WebSphere Portal, clique em **Intelligent Operations > Sobre**.

O portlet Sobre fornece as informações a seguir:

- O local de todos os produtos de software e componentes instalados
- O nome e a versão dos produtos instalados
- O nome e a versão dos componentes instalados
- Os detalhes de quaisquer correções aplicadas

Os componentes que são identificados são componentes ou partes de um produto, por exemplo:

- Uma parte de um produto que tem um fluxo de manutenção ou serviço dedicado
- Uma parte opcionalmente instalável de um produto
- Partes de um produto que são compartilhadas por diversos produtos

Nota: As informações exibidas para cada correção dependem da conclusão da etapa apropriada nas instruções de instalação fornecidas com essa correção.

Customizando o Portlet Sobre

É possível customizar este portlet. Clique no botão no canto superior direito do portlet para ver as opções de customização do menu de portlet. As configurações compartilhadas afetam o conteúdo desse portlet para todos os usuários, mas apenas para esta ocorrência do portlet.

Tarefas relacionadas:

“Verificando a instalação” na página 50

Depois de instalar o IBM Intelligent Operations Center, verifique se o produto foi instalado corretamente.

Referências relacionadas:

“Configurações do Portlet do Sobre” na página 146

Customize o portlet do Sobre alterando as configurações nos campos da janela **Configurações Compartilhadas**.

Controlando os Serviços

Os serviços do IBM Intelligent Operations Center em execução nos serviços do IBM Intelligent Operations Center podem ser controlados e consultados.

Iniciando os Serviços

O Ferramenta de Controle de Plataforma está disponível para iniciar os serviços em execução nos servidores IBM Intelligent Operations Center.

Sobre Esta Tarefa

O comando **IOControl.sh** deve ser executado como o usuário `ibmadmin`. Se não efetuou login como `ibmadmin`, execute o comando **su - ibmadmin** para alternar para o usuário `ibmadmin`.

Atenção: O início dos serviços individuais somente deve ser feito por administradores experientes do IBM Intelligent Operations Center. Resultados imprevisíveis podem ocorrer se os serviços não forem iniciados na ordem requerida.

Procedimento

No Servidor de Gerenciamento execute o seguinte comando para iniciar todos os serviços do IBM Intelligent Operations Center.

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

em que *password* é a senha para o Ferramenta de Controle de Plataforma definido quando o Ferramenta de Controle de Plataforma foi instalado.

Os serviços são iniciados na ordem requerida. Serviços de pré-requisito são iniciados antes dos serviços dependentes. Por exemplo, os serviços de banco de dados e diretório são iniciados primeiro.

Para iniciar somente um serviço, execute o seguinte comando.

```
/opt/IBM/ISP/mgmt/scripts/IOControl.sh start service_ID password
```

em que *service_ID* é um ID listado sob **Opções de Destino** na ajuda de **IOControl** e *password* é a senha para o Ferramenta de Controle de Plataforma definida quando o Ferramenta de Controle de Plataforma foi instalado.

Resultados

Os serviços requeridos do IBM Intelligent Operations Center são iniciados.

O que Fazer Depois

Após executar o comando **IOControl.sh**, verifique os logs no diretório `/opt/IBM/ISP/mgmt/logs`. Os logs contêm os resultados do comando **IOControl.sh**.

Tarefas relacionadas:

“Parando os Serviços” na página 199

O Ferramenta de Controle de Plataforma está disponível para parar os serviços do IBM Intelligent Operations Center.

“Consultando o Status dos Serviços” na página 202

O Ferramenta de Controle de Plataforma está disponível para determinar o status dos serviços do IBM Intelligent Operations Center.

“Obtendo Ajuda para o Ferramenta de Controle de Plataforma” na página 203

As informações sobre as opções de ação e de destino para o Ferramenta de Controle de Plataforma estão disponíveis.

“Verificando a instalação” na página 50

Depois de instalar o IBM Intelligent Operations Center, verifique se o produto foi instalado corretamente.

“Instalando o Ferramenta de Controle de Plataforma” na página 47

O Ferramenta de Controle de Plataforma é usado para gerenciar o ambiente do servidor do IBM Intelligent Operations Center. A ferramenta é instalada separadamente do produto.

“Instalando a Ferramenta do Verificação do Sistema” na página 48

A ferramenta do Verificação do Sistema é usada para verificar o status operacional dos componentes no IBM Intelligent Operations Center. A ferramenta é instalada separadamente do produto.

Ordem de Início Requerida

Os serviços do IBM Intelligent Operations Center devem ser iniciados em uma ordem específica.

O Ferramenta de Controle de Plataforma é usado para iniciar os serviços do IBM Intelligent Operations Center. Enquanto é recomendado que a opção **iniciar tudo** do Ferramenta de Controle de Plataforma seja usada para iniciar todos os serviços, pode haver momentos em que os serviços precisem ser iniciados.

Alguns serviços dependem de outros serviços, assim os serviços devem ser iniciados em uma ordem específica.

Em geral, os serviços devem ser iniciados em três grupos:

Group 1

tds, db24po, db24sms, db24wbm, db24ana, db24tsrm, db24sol, db24mgmt

Grupo 2

ihs, appdmgr, st

Grupo 3

todos os serviços restantes

Inicie os serviços no grupo 1 primeiro, depois inicie o grupo 2 e, finalmente, o grupo 3. Os serviços dentro de cada grupo podem ser iniciados em qualquer ordem.

Tabela 72. Dependências da Ordem de Início do Serviço do IBM Intelligent Operations Center

Serviço	Descrição	Serviços que devem estar em execução antes que esse serviço seja iniciado
db24po	DB2 Enterprise Server Edition para WebSphere Portal Server	Nenhuma
db24wbm	DB2 Enterprise Server Edition para WebSphere Business Modeler	Nenhuma
db24sol	DB2 Enterprise Server Edition para IBM Intelligent Operations Center	Nenhuma
db24ana	DB2 Enterprise Server Edition para Cognos	Nenhuma

Tabela 72. Dependências da Ordem de Início do Serviço do IBM Intelligent Operations Center (continuação)

Serviço	Descrição	Serviços que devem estar em execução antes que esse serviço seja iniciado
db24mgmt	DB2 Enterprise Server Edition para serviços do Tivoli Enterprise Portal	Nenhuma
db24tsrm	DB2 Enterprise Server para Tivoli Service Request Manager	Nenhuma
db24sms	DB2 Enterprise Server para serviços de modelo semântico	Nenhuma
tds	Tivoli Directory Server	Nenhuma
tdspxyapp	Proxy do Tivoli Directory Server (servidor de aplicativos)	tds
tdspxyevt	Proxy do Tivoli Directory Server ()	tds
tdspxymgt	Proxy do Tivoli Directory Server (Servidor de Gerenciamento)	tds
tdsappsrv	Servidor de Aplicativos do Tivoli Directory Server	Nenhuma
tamps	Policy Server do Tivoli Access Manager	tamas
tamas	Servidor de Autorização do Tivoli Access Manager	tds
tamwpm	Gerenciador de Portal da Web do Tivoli Access Manager	Nenhuma
tamweb	Tivoli Access Manager WebSEAL	tamas
tems	Tivoli Monitoring Enterprise Monitoring Server	Nenhuma
teps	Servidor do Enterprise Portal do Tivoli Monitoring	tems, db24mgmt
tim	Tivoli Identity Manager	tds
appdmgr	WebSphere Application Server Network Deployment	Nenhuma
cplex	WebSphere Application Server para CPLEX	db24sms
ihs	Servidor de HTTP para Tempo de Execução do (servidor de aplicativos)	Nenhuma
ihsevt	Servidor de HTTP para Tempo de Execução do ()	ihs
ihsmt	Servidor de HTTP para Tempo de Execução do (Servidor de Gerenciamento)	ihs
ncob	Tivoli Netcool/OMNIBus	Nenhuma
nci	Tivoli Netcool/Impact	ncob
wbm	IBM WebSphere Business Monitor	db24wbm
st	Lotus Sametime	Nenhuma
stpxy	Servidor de Aplicativos Proxy do Lotus Sametime	st
wpe	WebSphere Portal Extend	tdspxyapp, db24po, appdmgr
wmb	WebSphere Message Broker	Nenhuma
cognos	IBM Cognos Business Intelligence	db24ana, appdmgr
tsrm	Tivoli Service Request Manager	appdmgr, db24tsrm
wodm	WebSphere Operations Decision Manager	appdmgr
wodmdc	WebSphere Operations Decision Manager (Decision Center)	Nenhuma
smsclt	Serviços de modelo semântico (Serviços do Cliente)	appdmgr
smsdaaq	Serviços de modelo semântico (Serviços de Dados)	appdmgr
smsmdl	Serviços de modelo semântico (Serviços de Modelos)	appdmgr
smsgmt	Serviços de modelo semântico (Gerenciamento de Serviços)	appdmgr
smsrtc	Serviços de modelo semântico (RTC Services)	appdmgr

Tabela 72. Dependências da Ordem de Início do Serviço do IBM Intelligent Operations Center (continuação)

Serviço	Descrição	Serviços que devem estar em execução antes que esse serviço seja iniciado
iocxml	Análise de XML do IBM Intelligent Operations Center	db24so1

Iniciando e Parando 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

A análise faz parte do script do IOCControl. A análise é iniciada e parada quando você inicia e para o Tivoli Netcool/OMNIBus. A análise do Tivoli Netcool/OMNIBus é vinculado com o Tivoli Netcool/OMNIBus no script. Use o seguinte procedimento para parar, iniciar e verificar o status da análise.

Procedimento

1. Para parar a análise, no Servidor de Gerenciamento, execute:
`/opt/IBM/ISP/mgmt/scripts/IOCControl.sh stop ncob password`
2. Para parar a análise, no Servidor de Gerenciamento, execute:
`/opt/IBM/ISP/mgmt/scripts/IOCControl.sh start ncob password`
3. Para verificar o status da análise:
 - No Servidor de Gerenciamento, execute o comando:
`/opt/IBM/ISP/mgmt/scripts/IOCControl.sh start iocxml password`
 - No , execute o comando:
`tail -f /opt/IBM/netcool/omnibus/log/ioc_xml.log`

Parando os Serviços

O Ferramenta de Controle de Plataforma está disponível para parar os serviços do IBM Intelligent Operations Center.

Sobre Esta Tarefa

O comando **IOCControl.sh** deve ser executado como o usuário `ibmadmin`. Se não efetuou login como `ibmadmin`, execute o comando `su - ibmadmin` para alternar para o usuário `ibmadmin`.

Atenção: A interrupção dos serviços individuais somente deve ser feito por administradores experientes do IBM Intelligent Operations Center. Resultados imprevisíveis podem ocorrer se os serviços não forem interrompidos na ordem requerida.

Procedimento

No Servidor de Gerenciamento execute o seguinte comando para parar todos os serviços do IBM Intelligent Operations Center.

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

em que *password* é a senha para o Ferramenta de Controle de Plataforma definido quando o Ferramenta de Controle de Plataforma foi instalado.

Para parar somente um serviço, execute o seguinte comando.

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

em que *service_ID* é um ID listado sob **Opções de Destino** na ajuda de **IOControl** e *password* é a senha para o Ferramenta de Controle de Plataforma definida quando o Ferramenta de Controle de Plataforma foi instalado.

Resultados

Os serviços requeridos do IBM Intelligent Operations Center são interrompidos.

O que Fazer Depois

Após executar o comando **IOControl.sh**, verifique os logs no diretório/opt/IBM/ISP/mgmt/logs. Os logs contêm os resultados do comando **IOControl.sh**.

Tarefas relacionadas:

“Iniciando os Serviços” na página 195

O Ferramenta de Controle de Plataforma está disponível para iniciar os serviços em execução nos servidores IBM Intelligent Operations Center.

“Consultando o Status dos Serviços” na página 202

O Ferramenta de Controle de Plataforma está disponível para determinar o status dos serviços do IBM Intelligent Operations Center.

“Obtendo Ajuda para o Ferramenta de Controle de Plataforma” na página 203

As informações sobre as opções de ação e de destino para o Ferramenta de Controle de Plataforma estão disponíveis.

“Verificando a instalação” na página 50

Depois de instalar o IBM Intelligent Operations Center, verifique se o produto foi instalado corretamente.

“Instalando o Ferramenta de Controle de Plataforma” na página 47

O Ferramenta de Controle de Plataforma é usado para gerenciar o ambiente do servidor do IBM Intelligent Operations Center. A ferramenta é instalada separadamente do produto.

“Instalando a Ferramenta do Verificação do Sistema” na página 48

A ferramenta do Verificação do Sistema é usada para verificar o status operacional dos componentes no IBM Intelligent Operations Center. A ferramenta é instalada separadamente do produto.

Ordem de Interrupção Necessária

Os serviços do IBM Intelligent Operations Center devem ser interrompidos em uma ordem específica.

O Ferramenta de Controle de Plataforma é usado para parar os serviços do IBM Intelligent Operations Center. Enquanto é recomendado que a opção **interromper tudo** do Ferramenta de Controle de Plataforma seja usada para interromper todos os serviços, pode haver momentos em que os serviços precisem ser interrompidos.

Alguns serviços dependem de outros serviços, assim os serviços devem ser interrompidos em uma ordem específica.

Em geral, os serviços devem ser parados em três grupos:

Group 1

tds, db24po, db24sms, db24wbm, db24ana, db24tsrm, db24sol, db24mgmt

Grupo 2

ihs, appdmgr, st

Grupo 3

todos os serviços restantes

Pare os serviços no grupo 3 primeiro, depois pare o grupo 2 e, finalmente, o grupo 1. Os serviços dentro de cada grupo podem ser parados em qualquer ordem.

Tabela 73. Dependências da Ordem de Parada de Serviço do IBM Intelligent Operations Center

Serviço	Descrição	Serviços que devem estar parados antes que esse serviço seja interrompido
db24po	DB2 Enterprise Server Edition para WebSphere Portal Server	wpe
db24wbm	DB2 Enterprise Server Edition para WebSphere Business Modeler	wbm
db24sol	DB2 Enterprise Server Edition para IBM Intelligent Operations Center	iocxml
db24ana	DB2 Enterprise Server Edition para Cognos	cognos
db24mgmt	DB2 Enterprise Server Edition para serviços do Tivoli Enterprise Portal	teps
db24tsrm	DB2 Enterprise Server para Tivoli Service Request Manager	tsrm
db24sms	DB2 Enterprise Server para serviços de modelo semântico	cplex
tds	Tivoli Directory Server	tdsprxyapp, tdspxyevt, tdspxymgt, tamas, tim
tdsprxyapp	Proxy do Tivoli Directory Server (servidor de aplicativos)	wpe
tdspxyevt	Proxy do Tivoli Directory Server ()	Nenhuma
tdspxymgt	Proxy do Tivoli Directory Server (Servidor de Gerenciamento)	Nenhuma
tdsappsrv	Servidor de Aplicativos do Tivoli Directory Server	Nenhuma
tamps	Policy Server do Tivoli Access Manager	Nenhuma
tamas	Servidor de Autorização do Tivoli Access Manager	tamps
tamwpm	Gerenciador de Portal da Web do Tivoli Access Manager	Nenhuma
tamweb	Tivoli Access Manager WebSEAL	Nenhuma
tems	Tivoli Monitoring Enterprise Monitoring Server	teps
teps	Servidor do Enterprise Portal do Tivoli Monitoring	Nenhuma
tim	Tivoli Identity Manager	Nenhuma
appdmgr	WebSphere Application Server Network Deployment	wpe, cognos, tsrm, wodm, smsclt, smsdaaq, smsmdl, smsrtc, smsgmt
cplex	WebSphere Application Server para CPLEX	Nenhuma
ihs	Servidor de HTTP para Tempo de Execução do (servidor de aplicativos)	ihsevt, ihsmgt
ihsevt	Servidor de HTTP para Tempo de Execução do ()	Nenhuma
ihsmgt	Servidor de HTTP para Tempo de Execução do (Servidor de Gerenciamento)	Nenhuma
ncob	Tivoli Netcool/OMNIBus	nci
nci	Tivoli Netcool/Impact	Nenhuma
wbm	IBM WebSphere Business Monitor	Nenhuma
st	Lotus Sametime	stpxy
stpxy	Servidor de Aplicativos Proxy do Lotus Sametime	Nenhuma
wpe	WebSphere Portal Extend	Nenhuma
wmb	WebSphere Message Broker	Nenhuma

Tabela 73. Dependências da Ordem de Parada de Serviço do IBM Intelligent Operations Center (continuação)

Serviço	Descrição	Serviços que devem estar parados antes que esse serviço seja interrompido
cognos	IBM Cognos Business Intelligence	Nenhuma
tsrm	Tivoli Service Request Manager	Nenhuma
wodm	WebSphere Operations Decision Manager	Nenhuma
wodmdc	WebSphere Operations Decision Manager (Decision Center)	Nenhuma
smsclt	Serviços de modelo semântico (Serviços do Cliente)	Nenhuma
smsdaaq	Serviços de modelo semântico (Serviços de Dados)	Nenhuma
smsmdl	Serviços de modelo semântico (Serviços de Modelos)	Nenhuma
smsgmt	Serviços de modelo semântico (Gerenciamento de Serviços)	Nenhuma
smsrtc	Serviços de modelo semântico (RTC Services)	Nenhuma
iocxml	Análise de XML do IBM Intelligent Operations Center	Nenhuma

Consultando o Status dos Serviços

O Ferramenta de Controle de Plataforma está disponível para determinar o status dos serviços do IBM Intelligent Operations Center.

Sobre Esta Tarefa

O comando **IOControl.sh** deve ser executado como o usuário `ibmadmin`. Se não efetuou login como `ibmadmin`, execute o comando `su - ibmadmin` para alternar para o usuário `ibmadmin`.

Procedimento

No Servidor de Gerenciamento execute o seguinte comando para consultar o status de todos os serviços do IBM Intelligent Operations Center.

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

em que *password* é a senha para o Ferramenta de Controle de Plataforma definido quando o Ferramenta de Controle de Plataforma foi instalado.

Para verificar somente um serviço, execute o seguinte comando.

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

em que *service_ID* é um ID listado sob **Opções de Destino** na ajuda de **IOControl** e *password* é a senha para o Ferramenta de Controle de Plataforma definida quando o Ferramenta de Controle de Plataforma foi instalado.

Resultados

Serviços que são iniciados exibirão **[on]**. Serviços que não são iniciados exibirão **[off]**.

O que Fazer Depois

Após executar o comando **IOControl.sh**, verifique os logs no diretório `/opt/IBM/ISP/mgmt/logs`. Os logs contêm os resultados do comando **IOControl.sh**.

Tarefas relacionadas:

“Iniciando os Serviços” na página 195

O Ferramenta de Controle de Plataforma está disponível para iniciar os serviços em execução nos servidores IBM Intelligent Operations Center.

“Parando os Serviços” na página 199

O Ferramenta de Controle de Plataforma está disponível para parar os serviços do IBM Intelligent Operations Center.

“Obtendo Ajuda para o Ferramenta de Controle de Plataforma”

As informações sobre as opções de ação e de destino para o Ferramenta de Controle de Plataforma estão disponíveis.

“Instalando o Ferramenta de Controle de Plataforma” na página 47

O Ferramenta de Controle de Plataforma é usado para gerenciar o ambiente do servidor do IBM Intelligent Operations Center. A ferramenta é instalada separadamente do produto.

Obtendo Ajuda para o Ferramenta de Controle de Plataforma

As informações sobre as opções de ação e de destino para o Ferramenta de Controle de Plataforma estão disponíveis.

Sobre Esta Tarefa

O comando **IOControl.sh** deve ser executado como o usuário `ibmadmin`. Se não efetuou login como `ibmadmin`, execute o comando `su - ibmadmin` para alternar para o usuário `ibmadmin`.

Procedimento

No Servidor de Gerenciamento 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 Serviços” na página 195

O Ferramenta de Controle de Plataforma está disponível para iniciar os serviços em execução nos servidores IBM Intelligent Operations Center.

“Parando os Serviços” na página 199

O Ferramenta de Controle de Plataforma está disponível para parar os serviços do IBM Intelligent Operations Center.

“Consultando o Status dos Serviços” na página 202

O Ferramenta de Controle de Plataforma está disponível para determinar o status dos serviços do IBM Intelligent Operations Center.

Consoles de Administração

Utilize o portlet do Consoles de Administração para administrar os serviços fornecidos pela solução.

Para acessar o portlet do Consoles de Administração, na interface de Administração do WebSphere Portal, clique em **Intelligent Operations > Ferramentas de Administração > Consoles de Administração**.

Para cada serviço, os links no portlet do Consoles de Administração o direcionam tanto para o console de administração quanto para as informações sobre como acessar a administração.

Nota: Se estiver usando o Microsoft Internet Explorer versão 8.0, você pode encontrar um problema com o link de administração de relatório. A mensagem é: Não é possível localizar o recurso que foi solicitado. A solução é editar a URL no campo do endereço do navegador incluindo /cognos, entre o nome do host e o / ServletGateway.

Servidor de Aplicativos

Tabela 74. Administração no Servidor de Aplicativos

Console	Administração
Servidor de Aplicativos	Para administrar vários serviços fornecidos pelo IBM Intelligent Operations Center, utilize o link para o console baseado na web para WebSphere Application Server. É possível controlar os servidores, gerenciar recursos e fornecedores de serviços, alterar o host e outra configurações do ambiente.
Administração de relatórios	Para configurar relatórios, utilize o link para o console baseado na web para o IBM Cognos Connection . É possível criar novos relatórios ou modificar os já existentes. É possível também configurar origens de dados, configurar pastas públicas e privadas, definir permissões e distribuições, e planejar relatórios para serem executados automaticamente.

Servidor de dados

Tabela 75. Administração no Servidor de Dados

Console	Administração
Banco de Dados	Para obter detalhes sobre como administrar o banco de dados com o DB2 Enterprise Server Edition, utilize o link para o centro de informações. É possível executar tarefas com a GUI do centro de controle do banco de dados ou com a linha de comandos.

Servidor de eventos

Tabela 76. Administração no Servidor de Eventos

Console	Administração
Contatos	Para visualizar as configurações atuais no banco de dados names.nsf, utilize o link para o console baseado na web para o Servidor do Lotus Domino. O names.nsf é usado para configurar o Servidor do Lotus Domino. As mudanças na configuração podem ser realizadas com o Domino Administration Client.
Administração de contatos	Para obter detalhes sobre como fazer o download e configurar o Domino Administration Client para administração de contatos do Lotus Domino, utilize o link para o centro de informações.
Tratamento de Eventos	Para administrar a manipulação de eventos com a GUI do servidor de objeto, utilize o link para o console baseado na web para Tivoli Netcool/OMNIBus.

Tabela 76. Administração no Servidor de Eventos (continuação)

Console	Administração
Processamento e Aprimoramento de Eventos	Para administrar o processamento de eventos, utilize o link para o console baseado na web para o Tivoli Netcool/Impact. Por exemplo, é possível verificar as conexões com o banco de dados, conexões de origem de dados, inicialização do processamento de eventos, status da política e logs.
Servidor de Mensagens Instantâneas	Para administrar mensagens instantâneas, utilize o link para o console baseado na web para o Lotus Sametime Community Server.
Barramento de mensagem	Para obter detalhes sobre como verificar o status da mensagem com o WebSphere Message Broker, utilize o link para o centro de informações.
Administração do Procedimento Padrão de Operação	Para definir os recursos e o procedimentos padrão de operação, utilize o link para o console baseado na web para o Tivoli Service Request Manager Start Center. É possível definir recursos e atividades disponíveis para o gerenciamento de eventos no IBM Intelligent Operations Center.
Servidor de aplicativos do Procedimento Padrão de Operação	Para administrar, utilize o link para o console baseado na web para o WebSphere Application Server, que serve o Tivoli Service Request Manager.

Servidor de Gerenciamento

Tabela 77. Administração no Servidor de Gerenciamento

Console	Administração
Monitoramento de Aplicativo	Para administrar o monitoramento de aplicativos, utilize o link para o console baseado na web para o Tivoli Monitoring. É possível trabalhar com este console para verificações de funcionamento do sistema.
Servidor de aplicativos para gerenciamento	Para administrar os aplicativos integrados, utilize o link para o console baseado na web para o WebSphere Application Server. Esta administração inclui a administração de segurança com o Tivoli Access Manager e WebSEAL.
Banco de Dados	Para obter detalhes sobre como administrar o banco de dados com o DB2 Enterprise Server Edition, utilize o link para o centro de informações. É possível executar tarefas com a GUI do centro de controle do banco de dados ou com a linha de comandos.
Diretório	Para administrar o diretório do usuário, use o link para o console baseado na web para Tivoli Directory Server. Para obter detalhes sobre como usar o console baseado na web do Tivoli Directory Server, use o link para o centro de informações.




Customizando o portlet do Consoles de Administração

É possível customizar este portlet. Clique no botão no canto superior direito do portlet para ver as opções de customização do menu de portlet. As configurações compartilhadas afetam o conteúdo desse portlet para todos os usuários, mas apenas para esta ocorrência do portlet.

Referências relacionadas:

“Configurações do Portlet do Consoles de Administração” na página 146
Customize o portlet do Consoles de Administração alterando as configurações nos campos da janela **Configurações Compartilhadas**.

Informações relacionadas:

-  Centro de Informações do Lotus Domino e Lotus Notes
-  Centro de Informações do IBM DB2 Database
-  Centro de Informações do IBM Tivoli Directory Server

Gerenciando os Serviços

O portlet do Consoles de Administração fornece links para locais nos quais é possível gerenciar os serviços fornecidos pela solução, ou localizar mais informações detalhadas sobre o gerenciamento de serviços.

Servidor de aplicativos

Serviço de Servidor de Aplicativos

É possível executar uma ampla variedade de tarefas de gerenciamento de aplicativo em um console baseado na web comum, o Integrated Solutions Console:

- Verifique o status dos servidores.
- Inicie e pare servidores e clusters.
- Implemente aplicativos ou correções.
- Gerencie a lista de portlets disponíveis.
- Monitore os serviços.
- Trabalhe com políticas de serviço de aplicativo.
- Gerencie provedores de serviço, incluindo provedores de serviço REST.
- Gerencie recursos.
- Gerencie a segurança de seus aplicativos.
- Trabalhe com hosts virtuais e outras configurações de ambiente.
- Execute administração do sistema.
- Gerencie a integração de serviço.
- Administre o Servidor HTTP.
- Gerencie a criação de log e o rastreamento.

Para obter informações adicionais sobre o serviço do aplicativo, consulte a ajuda online para o Integrated Solutions Console, ou veja o link para o centro de informações do WebSphere Application Server no final da seção servidor de aplicativos.

Serviço de Administração de Relatório

Para todas as tarefas associadas com o fornecimento de relatório dentro do IBM Intelligent Operations Center, é possível usar o console de administração de relatório baseado na web:

- Configure a origem de dados.
- Crie, edite e exclua relatórios.
- Gerencie o acesso aos relatórios.
- Planeje relatórios.
- Configure a distribuição de relatórios.

Para obter informações adicionais sobre o serviço de administração de relatórios, consulte o link para o centro de informações do IBM Cognos Business Intelligence na final da seção servidor de aplicativos.

Informações relacionadas:

 [Centro de Informações do WebSphere Application Server Versão 7.0](#)

 [Centro de Informações do IBM Cognos Business Intelligence](#)

servidor de dados

Serviço de bancos de dados

É possível gerenciar os bancos de dados IBM Intelligent Operations Center por meio de instâncias de serviço de banco de dados hospedadas no servidor de dados. Uma instância de serviço de banco de dados é um processo independente separado que executa em um servidor. Uma instância pode hospedar diversos bancos de dados. Cada instância tem um nome *instance-name*. As seguintes instâncias são hospedadas no servidor de dados:

Tabela 78. Instâncias de Banco de Dados Hospedadas no servidor de dados

Ocorrência	Usado por
dsrdbm01	serviço do diretório
db2inst1	reservado para soluções
db2inst2	servidor de portal
db2inst3	administração de relatórios
db2inst4	regras de negócios e serviço do monitoramento de negócios
db2inst5	serviços do modelo semântico
db2inst6	serviço do administração de procedimento operacional padrão
db2inst7	serviço de gerenciamento de identidade
db2inst8	reservado para aplicativos

Para administrar uma instância de uma janela do terminal:

1. Efetue login como o usuário *instance-name* .
2. Execute o comando **db2** para inserir o modo de comando.
3. Digite **?** para ver uma lista de comandos disponíveis. Muitos comandos requerem uma conexão ativa com um banco de dados.
 - Para ver os bancos de dados disponíveis para uma instância, execute o comando **list database directory**.
 - Para se conectar a um banco de dados, execute o comando **connect to database_name**.
4. Para desconectar de um banco de dados e encerrar o modo de comando solicitado, execute o comando **terminate**.

Para obter informações adicionais sobre o serviço do banco de dados, consulte o link para o centro de informações do Banco de Dados DB2 no final da seção servidor de dados.

Informações relacionadas:

 Centro de Informações do IBM DB2 Database

Servidor de eventos

Contatos, administração de contatos, e Serviços do sistema de mensagens instantâneas

É possível gerenciar os serviços do contatos, administração de contatos e do sistema de mensagens instantâneas por meio de:

- Lotus Domino Console do servidor para visualizar seus contatos atuais.
- Lotus Domino Cliente de Administração para configurar conexão única, administrar o servidor de mensagem instantânea e o Lotus Sametime Client.
- Lotus Sametime Community Server para registrar e verificar a disponibilidade do servido de mensagem instantânea.

Nota: Contatos visualizados no console do servidor do Lotus Domino se aplicam somente ao portlet do Contatos e não são os mesmos dos usuários do IBM Intelligent Operations Center.

Para obter informações adicionais sobre os serviços do contatos, administração de contatos e sistema de mensagens instantâneas, consulte o link para o centro de informações do Lotus Domino e Notes no final da seção .

Serviço de Manipulação de Eventos

É possível gerenciar a captura e armazenamento de eventos no IBM Intelligent Operations Center por meio da GUI do servidor de objeto do Tivoli Netcool/OMNIBus.

1. Abra uma sessão de terminal ativada pata X Window System
2. Efetue logon como raiz no servidor.
3. Acesse o diretório /opt/IBM/netcool/omnibus.
4. Para abrir o aplicativo GUI, execute o comando: bin/nco_config

Para obter informações adicionais sobre o serviço do manipulação de eventos, consulte o link para o centro de informações do Tivoli Netcool/Impact no final da seção .

Serviço de Processamento e Aprimoramento de Eventos

É possível gerenciar o processamento de eventos por meio do console baseado na web para o Tivoli Netcool/Impact:

- Verifique as conexões com o banco de dados e a origem de dados.
- Verifique se o EventProcessor está executando.
- Verifique a criação de log para políticas existentes e atualize o nível de log.
- Atualize políticas existentes ou crie novas políticas.

Para obter informações adicionais sobre o serviço do processamento e aprimoramento de eventos, consulte o link para o centro de informações doTivoli Netcool/Impact no final da seção .

Barramento de Mensagem

Os três principais métodos para gerenciar o serviço de barramento de mensagens são:

- Linha de comandos
- Explorer: um aplicativo administrativo baseado no Eclipse
- Kit de Ferramentas: um aplicativo baseado em Eclipse que permite ambos, administração e desenvolvimento de aplicativos

É possível gerenciar fluxos de comunicação, definir testes, transformações, integrações e criação de log com a ferramenta de desenvolvimento de GUI.

O Kit de Ferramentas do WebSphere Message Broker é fornecido com o IBM Intelligent Operations Center. Para obter informações sobre a instalação e utilização do kit de ferramentas, consulte o link para o Centro de Informações do WebSphere Message Broker no final da seção

Para configurar o ambiente da linha de comandos e consultar instâncias do WebSphere Message Broker:

- Efetue logon no servidor como usuário mqm.
- Acesse o diretório /opt/IBM/mqsi/8.0.0.0.
- Para configurar o ambiente, execute o comando `source bin/mqsiprofile`.
- Para consultar instâncias do WebSphere Message Broker, execute o comando: `bin/mqsilist`.

Para obter informações adicionais sobre o serviço do barramento de mensagem, consulte o link para o centro de informações do WebSphere Message Broker no final da seção .

Serviço de Administração do procedimento padrão de operação

É possível definir recursos e atividades para gerenciar eventos por meio do console do administração de procedimento operacional padrão baseado na web e centro de início do Tivoli Service Request Manager.

Para obter informações adicionais sobre o serviço do administração de procedimento operacional padrão, consulte o link para o centro de informações do Tivoli Service Request Manager no final da seção .

Serviço de Aplicativo do procedimento padrão de operação

É possível gerenciar aplicativos associados com recursos e atividades por meio do console baseado na web para o WebSphere Application Server, que entrega para o Tivoli Service Request Manager.





Para obter informações adicionais sobre o serviço de aplicativo do procedimento padrão de operação, consulte a ajuda online ou consulte o link para o centro de informações do WebSphere Application Server Versão 7.0 no final da seção servidor de aplicativos.

Conceitos relacionados:

“Configurando o Tivoli Service Request Manager” na página 123

Na interface com o usuário do Tivoli Service Request Manager, é possível gerenciar o procedimentos padrão de operação, fluxos de trabalho e os recursos.

Informações relacionadas:

-  Centro de Informações do Lotus Domino e Lotus Notes
-  Centro de Informações do IBM Tivoli Netcool/Impact
-  Centro de Informações do IBM WebSphere Message Broker
-  Centro de Informações do IBM Tivoli Service Request Manager

Servidor de Gerenciamento

Serviço de Monitoramento de Aplicativo

É possível gerenciar o monitoramento de aplicativo por meio do console baseado na web para o Tivoli Monitoring. Faça o download do aplicativo e execute-o para verificar o status dos servidores e ver todos os agentes de monitoramento que estão em execução. Para efetuar logon, insira o seu ID e senha do usuário. O ID de usuário padrão é sysadmin e a senha de topologia inserida durante a instalação.

Para obter informações adicionais sobre o serviço de monitoramento de aplicativo, consulte o link para o Guia do Usuário do Tivoli Enterprise Portal no final do tópico.

Servidor de Aplicativos para Serviço de Gerenciamento

É possível gerenciar junções para o Tivoli Access Manager WebSEAL no console baseado na web comum, o Integrated Solutions Console.

Para obter informações detalhadas sobre esse serviço, consulte a ajuda online ou consulte o link para o centro de informações do WebSphere Application Server Versão 7.0 no final da seção servidor de aplicativos.

Serviço de bancos de dados

Existe uma instância de serviço do banco de dados, db2inst2, hospedada no servidor de gerenciamento. É possível usar essa instância para gerenciamento de sistema e armazenamento de dados específico para o Tivoli Access Manager.

Para obter informações detalhadas sobre o serviço do banco de dados, consulte o link para o centro de informações do IBM DB2 Database no final da seção servidor de dados.

Serviço de Diretório

Ao gerenciar o diretório de usuários por meio do console baseado na web para o Tivoli Directory Server, é possível visualizar, incluir ou mudar usuários no LDAP.

Para obter informações mais detalhadas sobre o serviço do diretório, consulte o link para o centro de informações do Tivoli Directory Server, no final desse tópico.

Informações relacionadas:



Guia do Usuário do IBM Tivoli Monitoring, Tivoli Enterprise Portal



Centro de Informações do IBM Tivoli Directory Server

Verificando os Componentes

A ferramenta Verificação do Sistema testa componentes dentro do IBM Intelligent Operations Center para determinar se eles estão acessíveis e operacionais.

Como Usar a Ferramenta Verificação do Sistema

A ferramenta do Verificação do Sistema é usada para determinar o status operacional dos serviços que abrangem o sistema IBM Intelligent Operations Center.

Sobre Esta Tarefa

A ferramenta Verificação do Sistema verifica os recursos do sistema.

Para obter detalhes sobre testes individuais e resolução de problemas se os testes falharem, clique em **Ajuda** para o teste.




Propriedades fornece informações adicionais sobre o teste para usar ao ligar para o Suporte de Software IBM.

Procedimento

1. Efetue logon no IBM Intelligent Operations Center como usuário com autoridade do administrador.

2. Clique em **Intelligent Operations > Ferramentas de Administração > Checagem de Verificação do Sistema**.
3. Selecione o teste ou testes a serem executados, executando um dos seguintes procedimentos:
 - Clique em um teste específico a ser executado.
 - Clique em **Executar Todos os Testes** para testar os recursos de todas as seleções.

Resultados

O ícone  será exibido quando um teste for concluído com êxito. O ícone  será exibido quando um teste falhar. Se um teste falhar, siga as instruções de determinação de problema para o teste para resolver os erros. Essas instruções também podem ser acessadas clicando no ícone  ou **Ajuda**.

Se um teste específico foi executado, os resultados da execução do teste serão exibidos na parte inferior do portlet juntamente com o tempo de execução de teste. Se **Executar Todos os Testes** foi selecionado, estas informações não serão exibidas.

O que Fazer Depois

A ferramenta pode ser reconfigurada e todos os resultados limpos clicando em **Reconfigurar**.

Tarefas relacionadas:

“Verificando a instalação” na página 50

Depois de instalar o IBM Intelligent Operations Center, verifique se o produto foi instalado corretamente.

“Instalando a Ferramenta do Verificação do Sistema” na página 48

A ferramenta do Verificação do Sistema é usada para verificar o status operacional dos componentes no IBM Intelligent Operations Center. A ferramenta é instalada separadamente do produto.

Testes do Verificação do Sistema

O IBM Intelligent Operations Center fornece vários testes do Verificação do Sistema que podem ser usados para determinar o status operacional de diversos serviços e componentes do IBM Intelligent Operations Center.

Os testes são agrupados logicamente por função. Por exemplo, colaboração e monitoramento.

Account Management (API do Tivoli Identity Manager) Teste

O teste do Account Management (API do Tivoli Identity Manager) testa o acesso à API do Tivoli Identity Manager acessando a porta IIOP.

Recursos

O teste do Account Management (API do Tivoli Identity Manager) usa o seguinte recurso:

- Tivoli Identity Manager Server (no Servidor de Gerenciamento).

Determinação de problemas

Se o teste do Account Management (API do Tivoli Identity Manager) falhar, faça o seguinte para localizar e resolver o problema.

Procedimento

1. Verifique se existe conectividade de rede entre o servidor de aplicativos e o Servidor de Gerenciamento. Isto pode ser feito enviando comandos **ping** com o nome do host abreviado e completo do Servidor de Gerenciamento a partir do servidor de aplicativos. Os resultados dos comandos **ping** serão mostrados se o nome do host estiver sendo resolvido corretamente pelo DNS ou pelo arquivo `/etc/hosts`.

2. Revise os arquivos de log para as exceções de tempo de execução.
 - a. No servidor de aplicativos revise os seguintes logs do WebSphere Portal:
 - /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log
 - /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log
 - b. No Servidor de Gerenciamento revise os seguintes logs do Tivoli Identity Manager:
 - /opt/IBM/WebSphere/AppServer/profiles/timProfile/logs/timServer1/SystemOut.log
 - /opt/IBM/WebSphere/AppServer/profiles/timProfile/logs/timServer1/SystemErr.log
 - Todos os logs em subdiretórios V6 do diretório /var/idsldap/.
3. Verifique se os sistemas de arquivos no servidor de aplicativos e Servidor de Gerenciamento não atingiram a capacidade. Isto pode ser determinado usando o comando **df -h**.
4. Verifique se o servidor Tivoli Identity Manager foi iniciado. A verificação pode ser feita usando o WebSphere Application Server Administrative Console ou por etapas manuais. A seguir estão as etapas manuais:
 - a. No sistema Servidor de Gerenciamento, efetue logon como **ibmadmin**.
 - b. Em uma janela de comando, execute: `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/serverStatus.sh -all -username waswebadmin -password WAS_ADMIN_PWD` em que **WAS_ADMIN_PWD** é a senha do administrador do WebSphere Application Server.
 - c. Se a mensagem **ADMU0509I: O Servidor de Aplicativos "nodeagent" não pode ser acessado. Ele parece estar interrompido.** for exibida, inicie o **nodeagent** usando o seguinte comando: `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/startNode.sh`. Ignore esta etapa se a mensagem **ADMU0508I: O Servidor de Aplicativos "nodeagent" está INICIADO.** for exibida. Se foi necessário iniciar o **nodeagent**, uma mensagem semelhante à seguinte será exibida: **ADMU3000I: Servidor nodeagent aberto para e-business; o ID do processo é 26654.**
 - a. Se a mensagem **ADMU0509I: O Servidor de Aplicativos "timServer1" não pode ser acessado. Ele parece estar interrompido.** for exibida, inicie o **timServer1** usando o seguinte comando: `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/startServer.sh timServer1`. Ignore esta etapa se a mensagem **ADMU0508I: O Servidor de Aplicativos "timServer1" está INICIADO.** for exibida. Se você teve que iniciar o **timServer1**, uma mensagem semelhante à seguinte será exibida: **ADMU3000I: Servidor timserver aberto para e-business; o ID do processo é 26654.**

Importante: Os servidores devem ser iniciados e parados em uma ordem específica.

Inicie os servidores nesta ordem:

- a. **nodeagent**
- b. **timServer1**




Pare os servidores nesta ordem:

- a. **timServer1**
- b. **nodeagent**

O servidor **timServer1** é interrompido executando o seguinte comando em uma janela de comando no servidor de aplicativos: `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/stopServer.sh timServer1 -username waswebadmin -password WAS_ADMIN_PWD` em que **WAS_ADMIN_PWD** é a senha do administrador do WebSphere.

O **nodeagent** é interrompido executando o seguinte comando em uma janela de comando no Servidor de Gerenciamento: `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` em que **WAS_ADMIN_PWD** é a senha do administrador do WebSphere.

5. Verifique se o servidor Tivoli Identity Manager foi iniciado. A verificação pode ser feita usando o WebSphere Application Server Administrative Console ou por etapas manuais. A seguir estão as etapas que usam o WebSphere Application Server Administrative Console:

- a. Efetue login no WebSphere Application Server Administrative Console em `http://MANAGEMENT_SERVER_HOST:9060/admin` usando o ID admin e a senha do WebSphere Application Server Administrative. *MANAGEMENT_SERVER_HOST* é o nome do host para o Servidor de Gerenciamento.
- b. Visualize o status do servidor timServer1 clicando em **Servidores > Tipos de Servidores > Servidores de Aplicativos WebSphere**.
 - O ícone  significa que o servidor está iniciado. Se necessário, selecione o servidor e clique em **Reiniciar** para reiniciar o servidor.
 - O ícone  significa que o servidor está interrompido. Selecione o servidor e clique em **Iniciar** para iniciar o servidor.
 - O ícone  significa que o status de servidor é indisponível. O Agente do Nó pode não estar em execução. Para iniciar o Agente do Nó, execute o comando `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/startNode.sh` em uma janela de comando.

Importante: Os servidores devem ser iniciados e parados em uma ordem específica.

Inicie os servidores nesta ordem:

- a. nodeagent
- b. timServer1

Pare os servidores nesta ordem:

- a. timServer1
- b. nodeagent

Para parar o servidor timServer1, selecione o servidor e clique em **Parar**.

O nodeagent é interrompido executando o seguinte comando em uma janela de comando no Servidor de Gerenciamento: `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` em que *WAS_ADMIN_PWD* é a senha d administrador do WebSphere.

6. Verifique se o console do Tivoli Identity Manager pode ser acessado a partir do sistema WebSphere Portal, no servidor de aplicativos, usando a seguinte URL: `http://MANAGEMENT_SERVER_HOST:9080/itim/console/main`. Em que *MANAGEMENT_SERVER_HOST* é o nome do host para o Servidor de Gerenciamento. Efetue login com o ID do usuário itim manager.

O que Fazer Depois

Resolva quaisquer problemas ou erros localizados e tente novamente o teste.

Account Management (Console do Tivoli Identity Manager)Teste

O teste do Account Management (Console do Tivoli Identity Manager) determina se o Tivoli Identity Manager está acessível acessando a URL do Tivoli Identity Manager Administration.

Recursos

O teste do Account Management (Console do Tivoli Identity Manager) usa o seguinte recurso:

- Tivoli Identity Manager Server (no Servidor de Gerenciamento)

Determinação de problemas

Se o teste do Account Management (Console do Tivoli Identity Manager) falhar, faça o seguinte para localizar e resolver o problema.

Procedimento

1. Verifique se existe conectividade de rede entre o servidor de aplicativos e o Servidor de Gerenciamento. Isto pode ser feito enviando comandos **ping** com o nome do host abreviado e

completo do Servidor de Gerenciamento a partir do servidor de aplicativos. Os resultados dos comandos **ping** serão mostrados se o nome do host estiver sendo resolvido corretamente pelo DNS ou pelo arquivo `/etc/hosts`.

2. Revise os arquivos de log para as exceções de tempo de execução.
 - a. No servidor de aplicativos revise os seguintes logs do WebSphere Portal:
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
 - b. No Servidor de Gerenciamento revise os seguintes logs do Tivoli Identity Manager:
 - `/opt/IBM/WebSphere/AppServer/profiles/timProfile/logs/timServer1/SystemOut.log`
 - `/opt/IBM/WebSphere/AppServer/profiles/timProfile/logs/timServer1/SystemErr.log`
 - Todos os logs em subdiretórios V6 do diretório `/var/idsldap/`.
3. Verifique se os sistemas de arquivos no servidor de aplicativos e Servidor de Gerenciamento não atingiram a capacidade. Isto pode ser determinado usando o comando **df -h**.
4. Verifique se o servidor Tivoli Identity Manager foi iniciado. A verificação pode ser feita usando o WebSphere Application Server Administrative Console ou por etapas manuais. A seguir estão as etapas manuais:
 - a. No sistema Servidor de Gerenciamento, efetue logon como `ibmadmin`.
 - b. Em uma janela de comando, execute: `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/serverStatus.sh -all -username waswebadmin -password WAS_ADMIN_PWD` em que `WAS_ADMIN_PWD` é a senha do administrador do WebSphere Application Server.
 - c. Se a mensagem `ADMU0509I: O Servidor de Aplicativos "nodeagent" não pode ser acessado. Ele parece estar interrompido.` for exibida, inicie o `nodeagent` usando o seguinte comando: `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/startNode.sh`. Ignore esta etapa se a mensagem `ADMU0508I: O Servidor de Aplicativos "nodeagent" está INICIADO.` for exibida. Se foi necessário iniciar o `nodeagent`, uma mensagem semelhante à seguinte será exibida: `ADMU3000I: Servidor nodeagent aberto para e-business; o ID do processo é 26654.`
 - a. Se a mensagem `ADMU0509I: O Servidor de Aplicativos "timServer1" não pode ser acessado. Ele parece estar interrompido.` for exibida, inicie o `timServer1` usando o seguinte comando: `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/startServer.sh timServer1`. Ignore esta etapa se a mensagem `ADMU0508I: O Servidor de Aplicativos "timServer1" está INICIADO.` for exibida. Se você teve que iniciar o `timServer1`, uma mensagem semelhante à seguinte será exibida: `ADMU3000I: Servidor timserv aberto para e-business; o ID do processo é 26654.`

Importante: Os servidores devem ser iniciados e parados em uma ordem específica.

Inicie os servidores nesta ordem:




- a. `nodeagent`
- b. `timServer1`

Pare os servidores nesta ordem:

- a. `timServer1`
- b. `nodeagent`

O servidor `timServer1` é interrompido executando o seguinte comando em uma janela de comando no servidor de aplicativos: `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/stopServer.sh timServer1 -username waswebadmin -password WAS_ADMIN_PWD` em que `WAS_ADMIN_PWD` é a senha do administrador do WebSphere.

O `nodeagent` é interrompido executando o seguinte comando em uma janela de comando no Servidor de Gerenciamento: `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` em que `WAS_ADMIN_PWD` é a senha do administrador do WebSphere.

5. Verifique se o servidor Tivoli Identity Manager foi iniciado. A verificação pode ser feita usando o WebSphere Application Server Administrative Console ou por etapas manuais. A seguir estão as etapas que usam o WebSphere Application Server Administrative Console:
 - a. Efetue logon no WebSphere Application Server Administrative Console em `http://MANAGEMENT_SERVER_HOST:9060/admin` usando o ID `admin` e a senha do WebSphere Application Server Administrative. `MANAGEMENT_SERVER_HOST` é o nome do host para o Servidor de Gerenciamento.
 - b. Visualize o status do servidor `timServer1` clicando em **Servidores > Tipos de Servidores > Servidores de Aplicativos WebSphere**.
 - O ícone  significa que o servidor está iniciado. Se necessário, selecione o servidor e clique em **Reiniciar** para reiniciar o servidor.
 - O ícone  significa que o servidor está interrompido. Selecione o servidor e clique em **Iniciar** para iniciar o servidor.
 - O ícone  significa que o status de servidor é indisponível. O Agente do Nó pode não estar em execução. Para iniciar o Agente do Nó, execute o comando `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/startNode.sh` em uma janela de comando.

Importante: Os servidores devem ser iniciados e parados em uma ordem específica.

Inicie os servidores nesta ordem:

- a. `nodeagent`
- b. `timServer1`

Pare os servidores nesta ordem:

- a. `timServer1`
- b. `nodeagent`

Para parar o servidor `timServer1`, selecione o servidor e clique em **Parar**.

O `nodeagent` é interrompido executando o seguinte comando em uma janela de comando no Servidor de Gerenciamento: `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` em que `WAS_ADMIN_PWD` é a senha d administrador do WebSphere.

6. Verifique se o console do Tivoli Identity Manager pode ser acessado a partir do sistema WebSphere Portal, no servidor de aplicativos, usando a seguinte URL: `http://MANAGEMENT_SERVER_HOST:9080/itim/console/main`. Em que `MANAGEMENT_SERVER_HOST` é o nome do host para o Servidor de Gerenciamento. Efetue logon com o ID do usuário `itim manager`.

O que Fazer Depois

Resolva quaisquer problemas ou erros localizados e tente novamente o teste.

Account Management (Tivoli Directory Integrator list assembly)Teste

O teste do Account Management (Tivoli Directory Integrator list assembly) determina se os recursos do Tivoli Directory Integrator List Assembly estão disponíveis. Para isso, o comando `tdisrvct1`, que gerencia remotamente configurações, linhas de montagem e outras funções, é executado no Servidor de Gerenciamento e o teste procura as `"--- AssemblyLines ---"` a serem retornadas.

Recursos

O teste do Account Management (Tivoli Directory Integrator list assembly) usa os seguintes recursos:

- Tivoli Directory Server (no servidor de dados)
- Tivoli Directory Integrator (no Servidor de Gerenciamento)

Determinação de problemas

Se o teste do Account Management (Tivoli Directory Integrator list assembly) falhar, faça o seguinte para localizar e resolver o problema.

Procedimento

1. Verifique se existe conectividade de rede entre o servidor de aplicativos e o servidor de dados. Isto pode ser feito enviando comandos **ping** com o nome do host abreviado e completo do servidor de dados a partir do servidor de aplicativos. Os resultados dos comandos **ping** serão mostrados se o nome do host estiver sendo resolvido corretamente pelo DNS ou pelo arquivo `/etc/hosts`.
2. Revise os arquivos de log para as exceções de tempo de execução.
 - a. No servidor de aplicativos revise os seguintes logs do WebSphere Portal:
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
3. Verifique se os sistemas de arquivos nos sistemas servidor de dados e servidor de aplicativos não atingiram a capacidade. Isto pode ser determinado usando o comando **df -h**.
4. Verifique se o Tivoli Directory Integrator Server está em execução.

- a. Efetue logon em uma sessão do terminal Servidor de Gerenciamento como `ibmadmin`.
- b. Execute o comando **ps -ef | grep ibmdisrv**. Os resultados serão semelhantes ao seguinte:

```
ibmadmin 11411 1 0 Sep06 pts/1 00:00:00 /bin/sh /opt/IBM/TDI/V7.1/ibmdisrv -s /opt/IBM/TDI/V7.1/timsol -c ITIM_RMI.xml -d
ibmadmin 32080 19149 0 23:17 pts/1 00:00:00 grep ibmdisrv
```

Este exemplo mostra que o daemon do Tivoli Directory Integrator Server, `ibmdisrv`, está em execução.

5. Inicie o Tivoli Directory Integrator Server, `ibmdisrv`, se ele não estiver em execução.
 - a. Efetue logon em uma sessão do terminal no Servidor de Gerenciamento como `raiz`.
 - b. Execute `/etc/init.d/ITIMAd start`.
6. Verifique se o servidor LDAP do Tivoli Directory Server está em execução.
 - a. Efetue logon em uma sessão do terminal no servidor de dados como `raiz`.
 - b. Execute o comando **ps -ef | grep ibmslapd**. Os resultados serão semelhantes ao seguinte:

```
dsrdbm01 13797 1 0 Apr26 pts/1 00:00:09 /opt/ibm/ldap/V6.3/sbin/64/ibmslapd -I dsrdbm01 -t -n
root 32080 19149 0 23:17 pts/1 00:00:00 grep ibmslapd
```

Este exemplo mostra que o daemon do Tivoli Directory Server, `ibmslapd`, está em execução.
 - c. Execute o comando **ps -ef | grep ibmdiradm**. Os resultados serão semelhantes ao seguinte:

```
root 4394 14038 0 14:17 pts/2 00:00:00 grep ibmdiradm
dsrdbm01 11055 1 0 Apr26 pts/1 00:00:00 /opt/ibm/ldap/V6.3/sbin/64/ibmdiradm -I dsrdbm01 -t
```

Este exemplo mostra que o daemon do Tivoli Directory Server, `ibmdiradm`, está em execução.

7. Se o Tivoli Directory Server, `ibmslapd`, não estiver em execução, faça o seguinte.
 - a. Como um usuário `raiz` Linux, execute `/opt/ibm/ldap/V6.3/sbin/ibmslapd -I dsrdbm01` para iniciar o Directory Server
8. Se o Tivoli Directory Administration Server, `ibmdiradm`, não estiver em execução, faça o seguinte.
 - a. Em uma sessão de terminal no servidor de dados, execute **su - dsrdbm01**.
 - b. Execute `/opt/ibm/ldap/V6.3/sbin/64/ibmdiradm -I dsrdbm01 -t` para iniciar o servidor de aplicativos.
9. Se o Tivoli Directory Server, `ibmslapd`, estiver em execução, faça o seguinte.

Nota: Execute essa etapa mesmo se o Tivoli Directory Server tiver sido iniciado na etapa anterior.

- a. Efetue logon em uma sessão do terminal no servidor de dados como `dsrdbm01`.
- b. Execute **idsldapsearch -h localhost -D "cn=root" -w "ADMIN_PASSWORD" -s sub uid=***, em que `ADMIN_PASSWORD` é a senha de conta do Administrador Raiz de LDAP. Os objetos de usuário de LDAP existentes serão exibidos.

10. Verifique se o Tivoli Directory Server Web Administration Tool está executando. O Tivoli Directory Server Web Administration Tool é usado para parar e iniciar a instância do LDAP, incluir usuários ou contas e visualizar arquivos de log.
 - a. Efetue logon em uma sessão do terminal no Servidor de Gerenciamento como `ibmadmin`.
 - b. Execute o comando `/opt/IBM/WebSphere/AppServer/profiles/tdsProfile/bin/serverStatus.sh -all -username waswebadmin -password WAS_ADMIN_PASSWORD` no Servidor de Gerenciamento em que `WAS_ADMIN_PASSWORD` é a senha do administrador do WebSphere Application Server. Se a ferramenta estiver em execução, uma mensagem semelhante à seguinte será retornada.


```
ADMU0508I: O Servidor de Aplicativos "tdsServer" está INICIADO
```

 Se a seguinte mensagem for retornada, o `tdsServer` precisa ser iniciado.


```
ADMU0509I: O Servidor de Aplicativos "tdsServer" não pode ser acessado. Ele parece estar interrompido.
```
 - c. Inicie o `tdsServer` executando o comando `/opt/IBM/WebSphere/AppServer/profiles/tdsProfile/bin/startServer.sh tdsServer`. O servidor, `tdsServer`, iniciará e uma mensagem semelhante à seguinte será exibida.


```
ADMU3000I: Servidor tdsServer aberto para e-business; o ID do processo é 26654
```
11. Acesse o Tivoli Directory Server Web Administration Tool em: `http://MANAGEMENT_SERVER_HOST:9062/IDSWebApp/IDSjsp/Login.jsp` em que `MANAGEMENT_SERVER_HOST` é o nome do host do Servidor de Gerenciamento.
12. Efetue logon com a Conta do Administrador Raiz de LDAP, `cn=root`, e a senha apropriada. O nome do Servidor LDAP deve ser `DATABASE_DIRECTORY_SERVER_HOST:389`, em que `DATABASE_DIRECTORY_SERVER_HOST` é o nome do host do servidor de dados.
13. Clique em **Administração do Servidor > Iniciar/Parar/Reconfigurar Servidor**. O status do servidor LDAP será exibido. Esta página também pode ser usada para iniciar, parar ou reconfigurar o servidor LDAP.

O que Fazer Depois

Resolva quaisquer problemas ou erros localizados e tente novamente o teste.

Account Management (Tivoli Directory Server) Teste

O teste do Account Management (Tivoli Directory Server) determina se o Tivoli Directory Server está disponível enviando uma solicitação de HTTP para o servidor.

Recursos

O teste do Account Management (Tivoli Directory Server) usa o seguinte recurso:

- Tivoli Directory Server (no servidor de dados)

Determinação de problemas

Se o **Teste de HTTP do Tivoli Directory Server** falhar, faça o seguinte para localizar e resolver o problema.

Procedimento

1. Revise os arquivos de log para as exceções de tempo de execução.
 - a. No servidor de aplicativos revise os seguintes logs do WebSphere Portal:
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
2. Verifique se os sistemas de arquivos no servidor de dados não atingiram a capacidade. Isto pode ser determinado usando o comando `df -h`.
3. Verifique se o servidor LDAP do Tivoli Directory Server está em execução.
 - a. Efetue logon em uma sessão do terminal no servidor de dados como `raiz`.

- b. Execute o comando **ps -ef | grep ibmslapd**. Os resultados serão semelhantes ao seguinte:

```
dsrdbm01 13797      1  0 Apr26 pts/1    00:00:09 /opt/ibm/ldap/V6.3/sbin/64/ibmslapd -I dsrdbm01 -t -n
root     32080 19149  0 23:17 pts/1    00:00:00 grep ibmslapd
```

Este exemplo mostra que o daemon do Tivoli Directory Server, `ibmslapd`, está em execução.

- c. Execute o comando **ps -ef | grep ibmdiradm**. Os resultados serão semelhantes ao seguinte:

```
root     4394 14038  0 14:17 pts/2    00:00:00 grep ibmdiradm
dsrdbm01 11055      1  0 Apr26 pts/1    00:00:00 /opt/ibm/ldap/V6.3/sbin/64/ibmdiradm -I dsrdbm01 -t
```

Este exemplo mostra que o daemon do Tivoli Directory Server, `ibmdiradm`, está em execução.

- Se o Tivoli Directory Server, `ibmslapd`, não estiver em execução, faça o seguinte.
 - Como um usuário *raiz* Linux, execute `/opt/ibm/ldap/V6.3/sbin/ibmslapd -I dsrdbm01` para iniciar o Directory Server
- Se o Tivoli Directory Administration Server, `ibmdiradm`, não estiver em execução, faça o seguinte.
 - Em uma sessão de terminal no servidor de dados, execute `su - dsrdbm01`.
 - Execute `/opt/ibm/ldap/V6.3/sbin/64/ibmdiradm -I dsrdbm01 -t` para iniciar o servidor de aplicativos.
- Se o Tivoli Directory Server, `ibmslapd`, estiver em execução, faça o seguinte.

Nota: Execute essa etapa mesmo se o Tivoli Directory Server tiver sido iniciado na etapa anterior.

- Efetue logon em uma sessão do terminal no servidor de dados como `dsrdbm01`.
 - Execute `idsldapsearch -h localhost -D "cn=root" -w "ADMIN_PASSWORD" -s sub uid=*`, em que `ADMIN_PASSWORD` é a senha de conta do Administrador Raiz de LDAP. Os objetos de usuário de LDAP existentes serão exibidos.
- Verifique se o Tivoli Directory Server Web Administration Tool está executando. O Tivoli Directory Server Web Administration Tool é usado para parar e iniciar a instância do LDAP, incluir usuários ou contas e visualizar arquivos de log.
 - Efetue logon em uma sessão do terminal no Servidor de Gerenciamento como `ibmadmin`.
 - Excute o comando `/opt/IBM/WebSphere/AppServer/profiles/tdsProfile/bin/serverStatus.sh -all -username waswebadmin -password WAS_ADMIN_PASSWORD` no Servidor de Gerenciamento em que `WAS_ADMIN_PASSWORD` é a senha do administrador do WebSphere Application Server. Se a ferramenta estiver em execução, uma mensagem semelhante à seguinte será retornada.
ADMU0508I: 0 Servidor de Aplicativos "tdsServer" está INICIADO
Se a seguinte mensagem for retornada, o `tdsServer` precisa ser iniciado.
ADMU0509I: 0 Servidor de Aplicativos "tdsServer" não pode ser acessado. Ele parece estar interrompido.
 - Inicie o `tdsServer` executando o comando `/opt/IBM/WebSphere/AppServer/profiles/tdsProfile/bin/startServer.sh tdsServer`. O servidor, `tdsServer`, iniciará e uma mensagem semelhante à seguinte será exibida.
ADMU3000I: Servidor `tdsServer` aberto para e-business; o ID do processo é 26654
 - Acesse o Tivoli Directory Server Web Administration Tool em: `http://MANAGEMENT_SERVER_HOST:9062/IDSWebApp/IDSjsp/Login.jsp` em que `MANAGEMENT_SERVER_HOST` é o nome do host do Servidor de Gerenciamento.
 - Efetue logon com a Conta do Administrador Raiz de LDAP, `cn=root`, e a senha apropriada. O nome do Servidor LDAP deve ser `DATABASE_DIRECTORY_SERVER_HOST:389`, em que `DATABASE_DIRECTORY_SERVER_HOST` é o nome do host do servidor de dados.
 - Clique em **Administração do Servidor > Iniciar/Parar/Reconfigurar Servidor**. O status do servidor LDAP será exibido. Esta página também pode ser usada para iniciar, parar ou reconfigurar o servidor LDAP.

O que Fazer Depois

Resolva quaisquer problemas ou erros localizados e tente novamente o teste.

Analytics (Console do Cognos Gateway) Teste

O teste do Analytics (Console do Cognos Gateway) determina se o Cognos, no servidor de aplicativos, pode ser acessado pelo Cognos Servlet Gateway e pela URL do Cognos Administration Portal.

Recursos

O teste do Analytics (Console do Cognos Gateway) usa o seguinte recurso:

- Cognos (no sistema servidor de aplicativos).

Determinação de problemas

Se o teste do Analytics (Console do Cognos Gateway) falhar, faça o seguinte para localizar e resolver o problema de acesso.

Procedimento

1. Revise os arquivos de log para as exceções de tempo de execução.
 - a. No servidor de aplicativos revise os seguintes logs do WebSphere Portal:
 - /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log
 - /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log
 - b. No servidor de aplicativos revise os seguintes logs do Cognos:
 - /opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/logs/CognosX_Displ/SystemOut.log
 - /opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/logs/CognosX_Displ/SystemErr.log
 - /opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/logs/CognosX_GW1/SystemOut.log
 - /opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/logs/CognosX_GW1/SystemErr.log
 - Todos os logs no diretório /opt/IBM/cognos/c10_64/logs/.
2. Verifique se os sistemas de arquivos no sistema servidor de aplicativos não atingiram a capacidade. Isto pode ser determinado usando o comando **df -h**.
3. Verifique se os servidores Cognos Dispatcher e Cognos Gateway estão iniciados. A verificação pode ser feita usando o WebSphere Application Server Administrative Console ou por etapas manuais. A seguir estão as etapas manuais:
 - a. No sistema servidor de aplicativos, efetue logon como **cgnsadm** (usuário do Cognos).
 - b. Em uma janela de comando, execute: `/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/bin/serverStatus.sh -all -username waswebadmin -password WAS_ADMIN_PWD`, em que **WAS_ADMIN_PWD** é a senha do administrador do WebSphere Application Server.
 - c. Se a mensagem **ADMU0509I: O Servidor de Aplicativos "nodeagent" não pode ser atingido. Ele parece estar interrompido.** for exibida, inicie o **nodeagent** usando o seguinte comando: `/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/bin/startNode.sh`. Ignore esta etapa se a mensagem **ADMU0508I: O Servidor de Aplicativos "nodeagent" está INICIADO.** for exibida. Se você precisava iniciar o agente do nó, uma mensagem semelhante à seguinte será exibida: **ADMU3000I: Agente do nó do servidor aberto para e-business; o ID do processo é 26654.**
 - d. Se a mensagem **ADMU0509I: O Servidor de Aplicativos "CognosX_Displ" não pode ser acessado. Ele parece estar parado.** for exibida, inicie o **CognosX_Displ** usando o seguinte comando: `/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/bin/startServer.sh CognosX_Displ`. Ignore esta etapa se a mensagem **ADMU0508I: O Servidor de Aplicativos "CognosX_Displ" está INICIADO.** for exibida. Se você teve que iniciar o **CognosX_Displ**, uma mensagem semelhante à seguinte será exibida: **ADMU3000I: Servidor CognosX_Displ aberto para e-business; o ID do processo é 26654.**
 - e. Se a mensagem **ADMU0509I: O Servidor de Aplicativos "CognosX_GW1" não pode ser acessado. Ele parece estar parado.** for exibida, inicie o **CognosX_GW1** usando o seguinte comando: `/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/bin/startServer.sh CognosX_GW1`. Ignore esta etapa se a mensagem **ADMU0508I: O Servidor de Aplicativos "CognosX_GW1" está**

INICIADO. for exibida. Se você teve que iniciar o CognosX_GW1, uma mensagem semelhante à seguinte será exibida: ADMU3000I: Servidor CognosX_GW1 aberto para e-business; o ID do processo é 26676.

Importante: Os servidores devem ser iniciados e interrompidos em uma ordem específica.

Inicie os servidores nesta ordem:

- a. nodeagent
- b. CognosX_Displ
- c. CognosX_GW1




Pare os servidores nesta ordem:

- a. CognosX_GW1
- b. CognosX_Displ
- c. nodeagent

O servidor CognosX_GW1 é interrompido executando o seguinte comando em uma janela de comando no servidor de aplicativos: `/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/bin/stopServer.sh CognosX_GW1 -username waswebadmin -password WAS_ADMIN_PWD`, em que `WAS_ADMIN_PWD` é a senha do administrador do WebSphere.

O servidor CognosX_Displ é interrompido executando o seguinte comando em uma janela de comando no servidor de aplicativos: `/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/bin/stopServer.sh CognosX_Displ -wasadmin admin -password WAS_ADMIN_PWD`, em que `WAS_ADMIN_PWD` é a senha do administrador do WebSphere.

O nodeagent é interrompido executando o seguinte comando em uma janela de comando no servidor de aplicativos: `/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD`, em que `WAS_ADMIN_PWD` é a senha do administrador do WebSphere.

4. Verifique se os servidores Cognos Dispatcher e Cognos Gateway estão iniciados. A verificação pode ser feita usando o WebSphere Application Server Administrative Console ou por etapas manuais. A seguir estão as etapas que usam o WebSphere Application Server Administrative Console:
 - a. Efetue login no WebSphere Application Server Administrative Console em `http://APPLICATION_SERVER_HOST:9060/admin` usando o ID `admin` e a senha do WebSphere Application Server Administrative. `APPLICATION_SERVER_HOST` é o nome do host para o servidor de aplicativos.
 - b. Visualize o status dos servidores CognosX-Disp1 e CognosX_GW1, clicando em **Servidores > Tipos de Servidores > Servidores de Aplicativos WebSphere**.
 - O ícone  significa que o servidor está iniciado. Se necessário, selecione o servidor e clique em **Reiniciar** para reiniciá-lo.
 - O ícone  significa que o servidor está interrompido. Selecione o servidor e clique em **Iniciar** para iniciá-lo.
 - O ícone  significa que o status de servidor é indisponível. O Agente do Nó pode não estar em execução. Para iniciar o Agente do Nó, execute o comando `/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/bin/startNode.sh` em uma janela de comando.

Importante: Os servidores devem ser iniciados e interrompidos em uma ordem específica.

Inicie os servidores nesta ordem:

- a. nodeagent
- b. CognosX_Displ
- c. CognosX_GW1

Pare os servidores nesta ordem:

- a. CognosX_GW1
- b. CognosX_Displ
- c. nodeagent

Para parar os servidores CognosX_GW1 e CognosX_Displ, selecione o servidor e clique em **Parar**.

O nodeagent é interrompido executando o seguinte comando em uma janela de comando no servidor de aplicativos: `/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD`, em que `WAS_ADMIN_PWD` é a senha do administrador do WebSphere.

5. Verifique se o Cognos Administration Portal pode ser acessado a partir do sistema WebSphere Portal, no servidor de aplicativos, usando a seguinte URL: `http://APPLICATION_SERVER_HOST:9081/ServletGateway/servlet/Gateway`. Em que `APPLICATION_SERVER_HOST` é o nome do host para o servidor de aplicativos.

O que Fazer Depois

Resolva quaisquer problemas ou erros localizados e tente novamente o teste.

Application Server (WebSphere Application Server Web Service) Teste

O teste do Application Server (WebSphere Application Server Web Service) testa o acesso ao WebSphere Application Server Web Service acessando o serviço da web DrpGeoSvc.

Recursos

O teste do Application Server (WebSphere Application Server Web Service) usa o seguinte recurso:

- WebSphere Application Server (no servidor de aplicativos).

Determinação de problemas

Se o teste do Application Server (WebSphere Application Server Web Service) falhar, faça o seguinte para localizar e resolver o problema.

Procedimento

1. Revise os arquivos de log para as exceções de tempo de execução.
 - a. No servidor de aplicativos revise os seguintes logs do WebSphere Portal:
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
 - b. No servidor de aplicativos revise os seguintes logs de configuração do WebSphere UDDI Registry:
 - `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/logs/cpudServer1/SystemOut.log`
 - `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/logs/cpudServer1/SystemErr.log`
2. Verifique se o sistema de arquivo no servidor de aplicativos não atingiu a capacidade. Isto pode ser determinado usando o comando `df -h`.
3. Verifique se o servidor `cpudServer1` está iniciado. A verificação pode ser feita usando o WebSphere Application Server Administrative Console ou por etapas manuais. A seguir estão as etapas manuais:
 - a. No sistema servidor de aplicativos, efetue logon como `ibmadmin`.
 - b. Em uma janela de comando, execute: `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/serverStatus.sh -all -username waswebadmin -password WAS_ADMIN_PWD`, em que `WAS_ADMIN_PWD` é a senha do administrador do WebSphere Application Server.
 - c. Se a mensagem `ADMU0509I: O Servidor de Aplicativos "nodeagent" não pode ser acessado. Ele parece estar interrompido.` for exibida, inicie o nodeagent usando o seguinte comando: `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/startNode.sh`. Ignore esta etapa se a mensagem `ADMU0508I: O Servidor de Aplicativos "nodeagent" está INICIADO.` for exibida. Se for

necessário iniciar o nodeagent, uma mensagem semelhante à seguinte será exibida: ADMU3000I: Servidor nodeagent aberto para e-business; o ID do processo é 26654.

- a. Se a mensagem ADMU0509I: O Servidor de Aplicativos "cpudServer1" não pode ser acessado. Ele parece estar interrompido. for exibida, inicie o cpudServer1 usando o seguinte comando: /opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/startServer.sh cpudServer1. Ignore esta etapa se a mensagem ADMU0508I: O Servidor de Aplicativos "cpudServer1" está INICIADO. for exibida. Se você teve que iniciar o cpudServer1, uma mensagem semelhante à seguinte será exibida: ADMU3000I: Servidor cpudServer1 aberto para e-business; o ID do processo é 26654.

Importante: Os servidores devem ser iniciados e parados em uma ordem específica.

Inicie os servidores nesta ordem:

- a. nodeagent
- b. cpudServer1


Pare os servidores nesta ordem:

- a. cpudServer1
- b. nodeagent


O servidor cpudServer1 é interrompido executando o seguinte comando em uma janela de comando no servidor de aplicativos: /opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/stopServer.sh cpudServer1 -username waswebadmin -password WAS_ADMIN_PWD, em que WAS_ADMIN_PWD é a senha do administrador do WebSphere.

O nodeagent é interrompido executando o seguinte comando em uma janela de comando no servidor de aplicativos: /opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD, em que WAS_ADMIN_PWD é a senha do administrador do WebSphere.

4. Verifique se o servidor cpudServer1 está iniciado. A verificação pode ser feita usando o WebSphere Application Server Administrative Console ou por etapas manuais. A seguir estão as etapas que usam o WebSphere Application Server Administrative Console:
 - a. Efetue logon no WebSphere Application Server Administrative Console em `http://APPLICATION_SERVER_HOST:9060/admin` usando o ID admin e a senha do WebSphere Application Server Administrative. `APPLICATION_SERVER_HOST` é o nome do host para o Servidor de Aplicativos.
 - b. Visualize o status do servidor cpudServer1 clicando em **Servidores > Tipos de Servidores > Servidores de Aplicativos WebSphere**.

O ícone  significa que o servidor está iniciado. Se necessário, selecione o servidor e clique em **Reiniciar** para reiniciar o servidor.

O ícone  significa que o servidor está interrompido. Selecione o servidor e clique em **Iniciar** para iniciar o servidor.

O ícone  significa que o status de servidor é indisponível. O Agente do Nó pode não estar em execução. Para iniciar o Agente do Nó, execute o comando /opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/startNode.sh em uma janela de comando.

Importante: Os servidores devem ser iniciados e parados em uma ordem específica.

Inicie os servidores nesta ordem:

- a. nodeagent
- b. cpudServer1

Pare os servidores nesta ordem:

- a. cpudServer1

b. nodeagent

Para parar o servidor cpudServer, selecione o servidor e clique em **Parar**.

O nodeagent é interrompido executando o seguinte comando em uma janela de comando no servidor de aplicativos: `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD`, em que `WAS_ADMIN_PWD` é a senha do administrador do WebSphere.

5. Verifique se WebSphere UDDI User Console pode ser acessado.

a. No servidor de aplicativos, acesse: `https://APPLICATION_SERVER_HOST:9080/uddigui/`, em que `APPLICATION_SERVER_HOST` é o nome do host do servidor de aplicativos.

O que Fazer Depois

Resolva quaisquer problemas ou erros localizados e tente novamente o teste.

Business Rules (Console do WebSphere Operational Decision Manager JRules) Teste

O teste do Business Rules (Console do WebSphere Operational Decision Manager JRules) testa o acesso ao WebSphere Operational Decision Management JRules acessando o Rule Execution Server Console.

Recursos

O teste do Business Rules (Console do WebSphere Operational Decision Manager JRules) usa o seguinte recurso:

- WebSphere Operational Decision Management JRules (no servidor de aplicativos).

Determinação de problemas

Se o teste do Business Rules (Console do WebSphere Operational Decision Manager JRules) falhar, faça o seguinte para localizar e resolver o problema.

Procedimento

1. Revise os arquivos de log para as exceções de tempo de execução.

a. No servidor de aplicativos revise os seguintes logs do WebSphere Portal:

- `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
- `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`

b. No servidor de aplicativos revise os seguintes logs de configuração do WebSphere Operational Decision Management:

- `/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/logs/wodmServer1/SystemOut.log`
- `/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/logs/wodmServer1/SystemErr.log`

2. Verifique se o sistema de arquivo no servidor de aplicativos não atingiu a capacidade. Isto pode ser determinado usando o comando `df -h`.

3. Verifique se o Rule Execution Server está iniciado. A verificação pode ser feita usando o WebSphere Application Server Administrative Console ou por etapas manuais. A seguir estão as etapas manuais:

a. No sistema servidor de aplicativos, efetue logon como `ibmadmin`.

b. Em uma janela de comando, execute: `/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/serverStatus.sh -all -username waswebadmin -password WAS_ADMIN_PWD` em que `WAS_ADMIN_PWD` é a senha do administrador do WebSphere Application Server.

c. Se a mensagem `ADMU0509I: O Servidor de Aplicativos "nodeagent" não pode ser acessado. Ele parece estar interrompido.` for exibida, inicie o nodeagent usando o seguinte comando: `/opt/IBM/WebSphere/AppServer/profiles/wodmServer1/bin/startNode.sh`. Ignore esta etapa se a mensagem `ADMU0508I: O Servidor de Aplicativos "nodeagent" está INICIADO.` for exibida. Se foi necessário iniciar o nodeagent, uma mensagem semelhante à seguinte será exibida: `ADMU3000I: Servidor nodeagent aberto para e-business; o ID do processo é 26654.`

- a. Se a mensagem ADMU0509I: O Servidor de Aplicativos "wodmServer1" não pode ser acessado. Ele parece estar interrompido. For exibida, inicie o wodmServer1 usando o seguinte comando: `/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/startServer.sh wodmServer1`. Ignore esta etapa se a mensagem ADMU0508I: O Servidor de Aplicativos "wodmServer1" está INICIADO. For exibida. Se você teve que iniciar o wodmServer1, uma mensagem semelhante à seguinte será exibida: ADMU3000I: Servidor wodmServer1 aberto para e-business; o ID do processo é 26654.

Importante: Os servidores devem ser iniciados e parados em uma ordem específica.

Inicie os servidores nesta ordem:

- a. nodeagent
- b. wodmServer1

Pare os servidores nesta ordem:

- a. wodmServer1
- b. nodeagent


O servidor wodmServer1 é interrompido executando o seguinte comando em uma janela de comando no servidor de aplicativos: `/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/stopServer.sh wodmServer1 -username waswebadmin -password WAS_ADMIN_PWD`, em que `WAS_ADMIN_PWD` é a senha do administrador do WebSphere.

O nodeagent é interrompido executando o seguinte comando em uma janela de comando no servidor de aplicativos: `/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD`, em que `WAS_ADMIN_PWD` é a senha do administrador do WebSphere.


4. Verifique se o Rule Execution Server está iniciado. A verificação pode ser feita usando o WebSphere Application Server Administrative Console ou por etapas manuais. A seguir estão as etapas que usam o WebSphere Application Server Administrative Console:

- a. Efetue logon no WebSphere Application Server Administrative Console em `http://APPLICATION_SERVER_HOST:9060/admin` usando o ID `admin` e a senha do WebSphere Application Server Administrative. `APPLICATION_SERVER_HOST` é o nome do host para o servidor de aplicativos.

- b. Visualize o status do servidor wodmProfile clicando em **Servidores > Tipos de Servidores > Servidores de Aplicativos WebSphere**.

O ícone  significa que o servidor está iniciado. Se necessário, selecione o servidor e clique em **Reiniciar** para reiniciar o servidor.

O ícone  significa que o servidor está interrompido. Selecione o servidor e clique em **Iniciar** para iniciar o servidor.

O ícone  significa que o status de servidor é indisponível. O Agente do Nó pode não estar em execução. Para iniciar o Agente do Nó, execute o comando `/opt/IBM/WebSphere/AppServer/profiles/wodmServer1/bin/startNode.sh` em uma janela de comando.

Importante: Os servidores devem ser iniciados e parados em uma ordem específica.

Inicie os servidores nesta ordem:

- a. nodeagent
- b. wodmServer1

Pare os servidores nesta ordem:

- a. wodmServer1
- b. nodeagent

Para parar o servidor wodmProfile, selecione o servidor e clique em **Parar**.

O nodeagent é interrompido executando o seguinte comando em uma janela de comando no servidor de aplicativos: `/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD`, em que `WAS_ADMIN_PWD` é a senha do administrador do WebSphere.

5. Verifique se o Console do Rule Execution Server pode ser acessado a partir do servidor de aplicativos em `http://APPLICATION_SERVER_HOST:9083/res`, em que `APPLICATION_SERVER_HOST` é o nome do host do servidor de aplicativos. Efetue logon usando o ID do usuário `resAdmin1`.
6. No Console do Rule Execution Server, abra a guia Diagnósticos. Clique em **Executar Diagnósticos**. Um relatório será exibido com os testes executados. Clique em **Expandir Todos** para ver os detalhes sobre cada teste.

O que Fazer Depois

Resolva quaisquer problemas ou erros localizados e tente novamente o teste.

Business Rules (WebSphere Operational Decision Manager JRules Rule)Teste

O teste do Business Rules (WebSphere Operational Decision Manager JRules Rule) testa o acesso ao WebSphere Operational Decision Management JRules Rule Engine chamando a regra de negócios `cardTransactionRuleApp` instalada no Rules Execution Server e verificando a saída.

Recursos

O teste do Business Rules (WebSphere Operational Decision Manager JRules Rule) usa o seguinte recurso:

- WebSphere Operational Decision Management JRules (no servidor de aplicativos).

Determinação de problemas

Se o teste do Business Rules (WebSphere Operational Decision Manager JRules Rule) falhar, faça o seguinte para localizar e resolver o problema.

Procedimento

1. Revise os arquivos de log para as exceções de tempo de execução.
 - a. No servidor de aplicativos revise os seguintes logs do WebSphere Portal:
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
 - b. No servidor de aplicativos revise os seguintes logs de configuração do WebSphere Operational Decision Management:
 - `/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/logs/wodmServer1/SystemOut.log`
 - `/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/logs/wodmServer1/SystemErr.log`
2. Verifique se o sistema de arquivo no servidor de aplicativos não atingiu a capacidade. Isto pode ser determinado usando o comando **df -h**.
3. Verifique se o Rule Execution Server está iniciado. A verificação pode ser feita usando o WebSphere Application Server Administrative Console ou por etapas manuais. A seguir estão as etapas manuais:
 - a. No sistema servidor de aplicativos, efetue logon como `ibmadmin`.
 - b. Em uma janela de comando, execute: `/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/serverStatus.sh -all -username waswebadmin -password WAS_ADMIN_PWD` em que `WAS_ADMIN_PWD` é a senha do administrador do WebSphere Application Server.
 - c. Se a mensagem `ADMU0509I: O Servidor de Aplicativos "nodeagent" não pode ser acessado. Ele parece estar interrompido.` for exibida, inicie o nodeagent usando o seguinte comando: `/opt/IBM/WebSphere/AppServer/profiles/wodmServer1/bin/startNode.sh`. Ignore esta etapa se a mensagem `ADMU0508I: O Servidor de Aplicativos "nodeagent" está INICIADO.` for exibida. Se foi necessário iniciar o nodeagent, uma mensagem semelhante à seguinte será exibida: `ADMU3000I: Servidor nodeagent aberto para e-business; o ID do processo é 26654.`

- a. Se a mensagem ADMU0509I: O Servidor de Aplicativos "wodmServer1" não pode ser acessado. Ele parece estar interrompido. For exibida, inicie o wodmServer1 usando o seguinte comando: `/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/startServer.sh wodmServer1`. Ignore esta etapa se a mensagem ADMU0508I: O Servidor de Aplicativos "wodmServer1" está INICIADO. For exibida. Se você teve que iniciar o wodmServer1, uma mensagem semelhante à seguinte será exibida: ADMU3000I: Servidor wodmServer1 aberto para e-business; o ID do processo é 26654.

Importante: Os servidores devem ser iniciados e parados em uma ordem específica.

Inicie os servidores nesta ordem:




- a. nodeagent
- b. wodmServer1

Pare os servidores nesta ordem:

- a. wodmServer1
- b. nodeagent

O servidor wodmServer1 é interrompido executando o seguinte comando em uma janela de comando no servidor de aplicativos: `/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/stopServer.sh wodmServer1 -username waswebadmin -password WAS_ADMIN_PWD`, em que `WAS_ADMIN_PWD` é a senha do administrador do WebSphere.

O nodeagent é interrompido executando o seguinte comando em uma janela de comando no servidor de aplicativos: `/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD`, em que `WAS_ADMIN_PWD` é a senha do administrador do WebSphere.

4. Verifique se o Rule Execution Server está iniciado. A verificação pode ser feita usando o WebSphere Application Server Administrative Console ou por etapas manuais. A seguir estão as etapas que usam o WebSphere Application Server Administrative Console:
 - a. Efetue logon no WebSphere Application Server Administrative Console em `http://APPLICATION_SERVER_HOST:9060/admin` usando o ID `admin` e a senha do WebSphere Application Server Administrative. `APPLICATION_SERVER_HOST` é o nome do host para o servidor de aplicativos.
 - b. Visualize o status do servidor wodmProfile clicando em **Servidores > Tipos de Servidores > Servidores de Aplicativos WebSphere**.
 - O ícone  significa que o servidor está iniciado. Se necessário, selecione o servidor e clique em **Reiniciar** para reiniciar o servidor.
 - O ícone  significa que o servidor está interrompido. Selecione o servidor e clique em **Iniciar** para iniciar o servidor.
 - O ícone  significa que o status de servidor é indisponível. O Agente do Nó pode não estar em execução. Para iniciar o Agente do Nó, execute o comando `/opt/IBM/WebSphere/AppServer/profiles/wodmServer1/bin/startNode.sh` em uma janela de comando.

Importante: Os servidores devem ser iniciados e parados em uma ordem específica.

Inicie os servidores nesta ordem:

- a. nodeagent
- b. wodmServer1

Pare os servidores nesta ordem:

- a. wodmServer1
- b. nodeagent

Para parar o servidor wodmProfile, selecione o servidor e clique em **Parar**.

O nodeagent é interrompido executando o seguinte comando em uma janela de comando no servidor de aplicativos: `/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD`, em que `WAS_ADMIN_PWD` é a senha do administrador do WebSphere.

5. Verifique se o Console do Rule Execution Server pode ser acessado a partir do servidor de aplicativos em `http://APPLICATION_SERVER_HOST:9083/res`, em que `APPLICATION_SERVER_HOST` é o nome do host do servidor de aplicativos. Efetue login usando o ID do usuário `resAdmin1`.
6. No Console do Rule Execution Server, abra a guia Diagnósticos. Clique em **Executar Diagnósticos**. Um relatório será exibido com os testes executados. Clique em **Expandir Todos** para ver os detalhes sobre cada teste.

O que Fazer Depois

Resolva quaisquer problemas ou erros localizados e tente novamente o teste.

Collaboration (Console do Lotus Domino)Teste

O teste do Collaboration (Console do Lotus Domino) determina se o Domino Directory está acessível por meio de sua URL.

Recursos

O teste do Collaboration (Console do Lotus Domino) usa o seguinte recurso:

- Domino Server (no).

Determinação de problemas

Se o teste do Collaboration (Console do Lotus Domino) falhar, faça o seguinte para localizar e resolver o problema.

Procedimento

1. Revise os arquivos de log para as exceções de tempo de execução.
 - a. No revise os seguintes logs do Lotus Domino:
 - `/local/notesdata/console.out`
 - `/local/notesdata/log.nsf`
 - Todos os logs no diretório `/local/notesdata/IBM_TECHNICAL_SUPPORT/`.
2. Verifique se os sistemas de arquivos no sistema não atingiram a capacidade. Isto pode ser determinado usando o comando **df -h**.
3. Verifique se os componentes do Processo do Lotus Domino estão em execução.
 - a. Efetue login no console do Lotus Domino Directory em `http://EVENT_SERVER_HOST:84/names.nsf`, em que `EVENT_SERVER_HOST` é o nome do host do . Efetue login usando o nome de usuário e senha do Domino Administrator.
 - b. Se o console não puder ser acessado, no , execute o comando `ps -ef | grep notes` para determinar se os processos do Lotus Domino estão em execução. Os processos do Lotus Domino são:
 - servidor
 - ocorrência
 - atualizar
 - réplica
 - router
 - adminp
 - calconn
 - sched

- http
 - rnmgr
 - staddin
4. Se alguns, mas não todos os processos estiverem em execução, pare os processos em execução antes de reiniciar todos os processos.
 - a. No , efetue login como o usuário do notes.
 - b. Altere para o diretório /local/notesdata.
 - c. Execute o comando "nohup /opt/IBM/lotus/bin/server -q >console.out 2>&1 &" para parar todos os processos do Lotus Domino em execução.
 - d. Verifique se todos os processos foram interrompidos, executando o comando ps -ef | grep notes.
 - e. Se alguns processos do Lotus Domino ainda estiverem em execução, pare-os usando **kill -9 pid**, em que *pid* é o identificador de processo do processo do Lotus Domino.
 5. Se os processos do Lotus Domino não estiverem em execução, inicie os componentes do Lotus Domino Server.
 - a. No , efetue login como o usuário do notes.
 - b. Altere para o diretório /local/notesdata.
 - c. Execute o comando "nohup /opt/IBM/lotus/bin/server > console.out 2>&1 &" para iniciar todos os componentes do Lotus Domino Server.

O que Fazer Depois

Resolva quaisquer problemas ou erros localizados e tente novamente o teste.

Collaboration (Console do Lotus Sametime)Teste

O teste do Collaboration (Console do Lotus Sametime) determina se o Sametime Console está acessível por meio de sua URL.

Recursos

O teste do Collaboration (Console do Lotus Sametime) usa o seguinte recurso:

- Sametime Server (no).

Determinação de problemas

Se o teste do Collaboration (Console do Lotus Sametime) falhar, faça o seguinte para localizar e resolver o problema.

Procedimento

1. Colete e revise os arquivos de configuração e de log do Sametime Community Server.
 - a. Efetue logon no como um usuário *notes*.
 - b. Altere para o diretório /local/notesdata.
 - c. Execute o comando sh stdiagzip.sh. Este comando coletará todos os arquivos de log pertinentes e os gravará no diretório /local/notesdata/.
 - d. Revise os logs no diretório /local/notesdata/.
2. Verifique se os sistemas de arquivos no sistema não atingiram a capacidade. Isto pode ser determinado usando o comando **df -h**.
3. Verifique se os componentes do Processo do Sametime estão em execução.
 - a. Efetue login na página Inicial do Sametime em http://EVENT_SERVER_HOST:84/stcenter.nsf, em que *EVENT_SERVER_HOST* é o nome do host do . Efetue login usando o nome de usuário e senha do Domino Administrator.
 - b. Na página Inicial do Sametime, clique em **Administrar o Servidor**.

- c. Na página Servidor - Visão Geral, certifique-se de que todos os serviços do Sametime estejam em execução.
4. Se alguns, mas não todos os processos estiverem em execução, pare os processos em execução antes de reiniciar todos os processos.
 - a. No , efetue login como o usuário do notes.
 - b. Altere para o diretório /local/notesdata.
 - c. Execute o comando "nohup /opt/IBM/lotus/bin/server -q >console.out 2>&1 &" para parar todos os processos do Sametime em execução.
 - d. Verifique se todos os processos foram interrompidos, executando o comando ps -ef | grep notes.
 - e. Se alguns processos ainda estiverem em execução, pare-os usando **kill -9 pid**, em que *pid* é o identificador de processo do processo do Lotus Domino.
5. Se os processos do Sametime não estiverem em execução, inicie os componentes do Lotus Sametime Server.
 - a. No , efetue login como o usuário do notes.
 - b. Altere para o diretório /local/notesdata.
 - c. Execute o comando "nohup /opt/IBM/lotus/bin/server > console.out 2>&1 &" para iniciar todos os componentes do Lotus Sametime Server.

O que Fazer Depois

Resolva quaisquer problemas ou erros localizados e tente novamente o teste.

Collaboration (Proxy Lotus Sametime)Teste

O teste do Collaboration (Proxy Lotus Sametime) determina se o Lotus Sametime Proxy Web Application pode ser acessado pela URL do Lotus Sametime Proxy Web Application.

Recursos

O teste do Collaboration (Proxy Lotus Sametime) usa o seguinte recurso:

- Sametime Proxy (no servidor de aplicativos).

Determinação de problemas

Se o teste do Collaboration (Proxy Lotus Sametime) falhar, faça o seguinte para localizar e resolver o problema de acesso.

Procedimento

1. Revise os arquivos de log para as exceções de tempo de execução.
 - a. No servidor de aplicativos revise os seguintes logs do WebSphere Portal:
 - /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log
 - /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log
 - b. No servidor de aplicativos revise os seguintes logs do Sametime Proxy Server:
 - /opt/IBM/WebSphere/AppServer/profiles/STPAppProfile1/logs/STProxyServer1/SystemOut.log
 - /opt/IBM/WebSphere/AppServer/profiles/STPAppProfile1/logs/STProxyServer1/SystemErr.log
2. Verifique se os sistemas de arquivos no sistema servidor de aplicativos não atingiram a capacidade. Isto pode ser determinado usando o comando **df -h**.
3. Verifique se o Sametime Proxy Server está iniciado. A verificação pode ser feita usando o WebSphere Application Server Administrative Console ou por etapas manuais. A seguir estão as etapas manuais:
 - a. No sistema servidor de aplicativos, efetue logon como **ibmadmin**.
 - b. Em uma janela de comando, execute: `/opt/IBM/WebSphere/AppServer/profiles/STPAppProfile1/bin/serverStatus.sh -all -username waswebadmin -password WAS_ADMIN_PWD`, em que **WAS_ADMIN_PWD** é a senha do administrador do WebSphere Application Server.

- c. Se a mensagem ADMU0509I: O Servidor de Aplicativos "nodeagent" não pode ser atingido. Ele parece estar interrompido. for exibida, inicie o nodeagent usando o seguinte comando: `/opt/IBM/WebSphere/AppServer/profiles/STProxyServer1/bin/startNode.sh` . Ignore esta etapa se a mensagem ADMU0508I: O Servidor de Aplicativos "nodeagent" está INICIADO. for exibida. Se você precisava iniciar o agente do nó, uma mensagem semelhante à seguinte será exibida: ADMU3000I: Agente do nó do servidor aberto para e-business; o ID do processo é 26654.
- d. Se a mensagem ADMU0509I: O Servidor de Aplicativos "STProxyServer1" não pode ser acessado. Ele parece estar parado. for exibida, inicie o STProxyServer1 usando o seguinte comando: `/opt/IBM/WebSphere/AppServer/profiles/STAppProfile1/bin/startServer.sh STProxyServer1`. Ignore esta etapa se a mensagem ADMU0508I: O Servidor de Aplicativos "STProxyServer1" está INICIADO. for exibida. Se você teve que iniciar o STProxyServer1, uma mensagem semelhante à seguinte será exibida: ADMU3000I: Servidor STProxyServer1 aberto para e-business; o ID do processo é 26654.

Importante: Os servidores devem ser iniciados e interrompidos em uma ordem específica.

Inicie os servidores nesta ordem:

- a. nodeagent
- b. STProxyServer1

Pare os servidores nesta ordem:


- a. STProxyServer1
- b. nodeagent

O servidor STProxyServer1 é interrompido executando o seguinte comando em uma janela de comando no Servidor de Aplicativos: `/opt/IBM/WebSphere/AppServer/profiles/STAppProfile1/bin/stopServer.sh STProxyServer1 -username waswebadmin -password WAS_ADMIN_PWD`, em que `WAS_ADMIN_PWD` é a senha do administrador do WebSphere.


O nodeagent é interrompido executando o seguinte comando em uma janela de comando no Servidor de Aplicativos: `/opt/IBM/WebSphere/AppServer/profiles/STAppProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD`, em que `WAS_ADMIN_PWD` é a senha do administrador do WebSphere.

4. Verifique se o Sametime Proxy Server está iniciado. A verificação pode ser feita usando o WebSphere Application Server Administrative Console ou por etapas manuais. A seguir estão as etapas que usam o WebSphere Application Server Administrative Console:

- a. Efetue logon no WebSphere Application Server Administrative Console em `http://APPLICATION_SERVER_HOST:9060/admin` usando o ID admin e a senha do WebSphere Application Server Administrative. `APPLICATION_SERVER_HOST` é o nome do host para o servidor de aplicativos.
- b. Visualize o status do servidor STProxyServer1 clicando em **Servidores > Tipos de Servidores > Servidores de Aplicativos WebSphere**.

O ícone  significa que o servidor está iniciado. Se necessário, selecione o servidor e clique em **Reiniciar** para reiniciá-lo.

O ícone  significa que o servidor está interrompido. Selecione o servidor e clique em **Iniciar** para iniciá-lo.

O ícone  significa que o status de servidor é indisponível. O Agente do Nó pode não estar em execução. Para iniciar o Agente do Nó, execute o comando `/opt/IBM/WebSphere/AppServer/profiles/STProxyServer1/bin/startNode.sh` em uma janela de comando.

Importante: Os servidores devem ser iniciados e interrompidos em uma ordem específica.

Inicie os servidores nesta ordem:

- a. nodeagent

b. STProxyServer1

Pare os servidores nesta ordem:

a. STProxyServer1

b. nodeagent

Para parar o servidor STProxyServer1, selecione o servidor e clique em **Parar**.

O nodeagent é interrompido executando o seguinte comando em uma janela de comando no Servidor de Aplicativos: `/opt/IBM/WebSphere/AppServer/profiles/STPAppProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD`, em que `WAS_ADMIN_PWD` é a senha do administrador do WebSphere.

5. Verifique se o Sametime Proxy Console pode ser acessado a partir do sistema WebSphere Portal, no servidor de aplicativos, usando a seguinte URL: `http://APPLICATION_SERVER_HOST:9085/stwebclient/popup.jsp`. Em que `APPLICATION_SERVER_HOST` é o nome do host para o servidor de aplicativos.

O que Fazer Depois

Resolva quaisquer problemas ou erros localizados e tente novamente o teste.

Database (DB2)Teste

O teste do Database (DB2) determina se a conexão JDBC pode ser acessada entre o aplicativo da web e o servidor de dados. Uma conexão JDBC tipo 4 é estabelecida e uma consulta SQL dinâmica é emitida contando o número de tabelas presentes no banco de dados.

Recursos

O teste do Database (DB2) usa os seguintes recursos:

- Definição UddiDataSource contendo a conexão para o banco de dados UDDIDB (no servidor de aplicativos).
- Banco de dados UDDIDB (instância db2inst4 no servidor de dados).

Determinação de problemas

Se o teste do Database (DB2) não puder acessar o servidor de dados, faça o seguinte para localizar e resolver o problema de acesso.

Procedimento

1. Verifique se existe conectividade de rede entre o servidor de aplicativos no qual o teste foi iniciado e o servidor de dados no qual o banco de dados reside. Isto pode ser feito enviando comandos **ping** com o nome do host abreviado e completo do servidor de dados a partir do servidor de aplicativos. Os resultados dos comandos **ping** serão mostrados se o nome do host estiver sendo resolvido corretamente pelo DNS ou pelo arquivo `/etc/hosts`.
2. Revise os arquivos de log para as exceções de tempo de execução.
 - a. No servidor de aplicativos revise os seguintes logs do WebSphere Portal:
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
3. Verifique se os sistemas de arquivos no sistema servidor de dados não atingiram a capacidade. Isto pode ser determinado usando o comando **df -h**.
4. Verifique se os bancos de dados usados pelo servidor de dados estão iniciados.
 - a. No servidor de dados, execute o seguinte comando a partir de uma janela de comando, como db2inst4:

```
ps -ef | grep db2 | grep db2inst4
```

Os processos do DB2, incluindo os seguintes, devem estar em execução como o usuário da instância db2inst4:

db2sysc
db2vend
db2acd

5. Se os processos do DB2 não estiverem em execução, inicie-os executando db2start a partir da janela de comando como o usuário db2inst4:
6. Verifique nos logs do DB2 se há erros relacionados à instância de banco de dados usada para este teste. Os logs estão localizados no servidor de dados, no diretório /datahome/db2inst4/sqllib/db2dump.
7. Verifique se no db2diag.log há erros emitidos ao iniciar o banco de dados usado para este teste.
8. Verifique a conexão com os recursos de contêiner da web DataSource usando o console administrativo do WebSphere Application Server.
 - a. No servidor de aplicativos, acesse o console administrativo do WebSphere Application Server em: https://APPLICATION_SERVER_HOST:9043/ibm/console, em que APPLICATION_SERVER_HOST é o nome do host do servidor de aplicativos.
 - b. Clique em **Recursos > JDBC > Origens de dados**.
 - c. Verifique a origem de dados UddiDataSource clicando em **Testar Conexão** para testar a conexão com a origem de dados.

O que Fazer Depois

Resolva quaisquer problemas ou erros localizados e tente novamente o teste.

Database (DB2 Instance - *instance*)Teste

O Database (DB2 Instance - *instance*) testa o status do gerenciador do DB2 da instância do DB2 no servidor de dados executando o script **db2status**.

Recursos

O teste do Database (DB2 Instance - *instance*) usa o seguinte recurso:

- A *instance* do DB2 (no servidor de dados)

Determinação de problemas

Se o teste do Database (DB2 Instance - *instance*) falhar, faça o seguinte para localizar e resolver o problema de acesso.

Procedimento

1. Verifique se existe conectividade de rede entre o servidor de aplicativos no qual o teste foi iniciado e o servidor de dados no qual o banco de dados reside. Isto pode ser feito enviando comandos **ping** com o nome do host abreviado e completo do servidor de dados a partir do servidor de aplicativos. Os resultados dos comandos **ping** serão mostrados se o nome do host estiver sendo resolvido corretamente pelo DNS ou pelo arquivo /etc/hosts.
2. Revise os arquivos de log para as exceções de tempo de execução.
 - a. No servidor de aplicativos revise os seguintes logs do WebSphere Portal:
 - /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log
 - /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log
3. Verifique se o sistema de arquivos no sistema servidor de dados não atingiu a capacidade. Isto pode ser determinado usando o comando **df -h**.
4. Verifique se os bancos de dados usados pelo servidor de dados estão iniciados.

- a. No servidor de dados, execute o seguinte comando a partir de uma janela de comando como o usuário *instance*, em que *instance* é o nome da instância do DB2 indicada no nome do teste:
`db2 get snapshot for dbm | grep status`

Se o gerenciador do banco de dados for iniciado para *instance*, a seguinte mensagem será exibida:
Status do gerenciador do banco de dados = Ativo.

5. Se os processos do DB2 não estiverem em execução, inicie-os executando **su - instance** a partir da janela de comando, se estiver em execução como o usuário root. Caso contrário, execute **db2start** para iniciar o Gerenciador do Banco de Dados.
6. Verifique nos logs do DB2 se há erros relacionados à instância de banco de dados usada para este teste. Os logs estão localizados no servidor de dados, no diretório `/datahome/instance/sql1lib/db2dump`.
7. Verifique se no `db2diag.log` há erros emitidos ao iniciar o banco de dados usado para este teste.

O que Fazer Depois

Resolva quaisquer problemas ou erros localizados e tente novamente o teste.

Directory (UDDI V3 e UDDI V3 HTTPS)Teste

O teste do Directory (UDDI V3 e UDDI V3 HTTPS) determina se o WebSphere UDDI Registry pode ser acessado usando a URL HTTP e HTTPS do WebSphere UDDI Registry.

Recursos

O teste do Directory (UDDI V3 e UDDI V3 HTTPS) usa o seguinte recurso:

- WebSphere Application Server (no servidor de aplicativos).

Determinação de problemas

Se o teste do Directory (UDDI V3 e UDDI V3 HTTPS) falhar, faça o seguinte para localizar e resolver o problema de acesso.

Procedimento

1. Revise os arquivos de log para as exceções de tempo de execução.
 - a. No servidor de aplicativos revise os seguintes logs do WebSphere Portal:
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
 - b. No servidor de aplicativos revise os seguintes logs de configuração do WebSphere UDDI Registry:
 - `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/logs/cpudServer1/SystemOut.log`
 - `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/logs/cpudServer1/SystemErr.log`
2. Verifique se os sistemas de arquivos no sistema servidor de aplicativos não atingiram a capacidade. Isto pode ser determinado usando o comando **df -h**.
3. Verifique se o servidor `cpudServer1` está iniciado. A verificação pode ser feita usando o WebSphere Application Server Administrative Console ou por etapas manuais. A seguir estão as etapas manuais:
 - a. No sistema servidor de aplicativos, efetue logon como `ibmadmin`.
 - b. Em uma janela de comando, execute: `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/serverStatus.sh -all -username waswebadmin -password WAS_ADMIN_PWD`, em que `WAS_ADMIN_PWD` é a senha do administrador do WebSphere Application Server.
 - c. Se a mensagem `ADMU0509I: O Servidor de Aplicativos "nodeagent" não pode ser acessado. Ele parece estar interrompido.` for exibida, inicie o `nodeagent` usando o seguinte comando: `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/startNode.sh`. Ignore esta etapa se a mensagem `ADMU0508I: O Servidor de Aplicativos "nodeagent" está INICIADO.` for exibida. Se foi

necessário iniciar o nodeagent, uma mensagem semelhante à seguinte será exibida: ADMU3000I: Servidor nodeagent aberto para e-business; o ID do processo é 26654.

- a. Se a mensagem ADMU0509I: O Servidor de Aplicativos "cpudServer1" não pode ser acessado. Ele parece estar interrompido. for exibida, inicie o cpudServer1 usando o seguinte comando: /opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/startServer.sh cpudServer1. Ignore esta etapa se a mensagem ADMU0508I: O Servidor de Aplicativos "cpudServer1" está INICIADO. for exibida. Se você teve que iniciar o cpudServer1, uma mensagem semelhante à seguinte será exibida: ADMU3000I: Servidor cpudServer1 aberto para e-business; o ID do processo é 26654.

Importante: Os servidores devem ser iniciados e parados em uma ordem específica.

Inicie os servidores nesta ordem:

- a. nodeagent
- b. cpudServer1

Pare os servidores nesta ordem:

- a. cpudServer1
- b. nodeagent


O servidor cpudServer1 é interrompido executando o seguinte comando em uma janela de comando no servidor de aplicativos: /opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/stopServer.sh cpudServer1 -username waswebadmin -password WAS_ADMIN_PWD, em que WAS_ADMIN_PWD é a senha do administrador do WebSphere.

O nodeagent é interrompido executando o seguinte comando em uma janela de comando no servidor de aplicativos: /opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD, em que WAS_ADMIN_PWD é a senha do administrador do WebSphere.


4. Verifique se o servidor cpudServer1 está iniciado. A verificação pode ser feita usando o WebSphere Application Server Administrative Console ou por etapas manuais. A seguir estão as etapas que usam o WebSphere Application Server Administrative Console:

- a. Efetue login no WebSphere Application Server Administrative Console em `http://APPLICATION_SERVER_HOST:9060/admin` usando o ID admin e a senha do WebSphere Application Server Administrative. APPLICATION_SERVER_HOST é o nome do host para o Servidor de Aplicativos.

- b. Visualize o status do servidor cpudServer1 clicando em **Servidores > Tipos de Servidores > Servidores de Aplicativos WebSphere**.

O ícone  significa que o servidor está iniciado. Se necessário, selecione o servidor e clique em **Reiniciar** para reiniciar o servidor.

O ícone  significa que o servidor está interrompido. Selecione o servidor e clique em **Iniciar** para iniciar o servidor.

O ícone  significa que o status de servidor é indisponível. O Agente do Nó pode não estar em execução. Para iniciar o Agente do Nó, execute o comando /opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/startNode.sh em uma janela de comando.

Importante: Os servidores devem ser iniciados e parados em uma ordem específica.

Inicie os servidores nesta ordem:

- a. nodeagent
- b. cpudServer1

Pare os servidores nesta ordem:

- a. cpudServer1

b. nodeagent

Para parar o servidor cpudServer, selecione o servidor e clique em **Parar**.

O nodeagent é interrompido executando o seguinte comando em uma janela de comando no servidor de aplicativos: `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD`, em que `WAS_ADMIN_PWD` é a senha do administrador do WebSphere.

5. Verifique se o console do usuário do WebSphere UDDI Registry pode ser acessado a partir do sistema WebSphere Portal, no servidor de aplicativos, usando a seguinte URL: `http://APPLICATION_SERVER_HOST:9080/uddigui/`. Em que `APPLICATION_SERVER_HOST` é o nome do host para o servidor de aplicativos.

O que Fazer Depois

Resolva quaisquer problemas ou erros localizados e tente novamente o teste.

Internal Diagnostic (Echo REST remoto)Teste

O teste do Internal Diagnostic (Echo REST remoto) testa o acesso ao Remote Responder acessando a URL. Este é um diagnóstico do Verificação do Sistema e verifica os links entre módulos do Verificação do Sistema.

Recursos

O Internal Diagnostic (Echo REST remoto) usa o seguinte recurso:

- WebSphere Application Server (no servidor de aplicativos).

Determinação de problemas

Se o teste do Internal Diagnostic (Echo REST remoto) falhar, faça o seguinte para localizar e resolver o problema.

Procedimento

1. Revise os arquivos de log para as exceções de tempo de execução.
 - a. No servidor de aplicativos revise os seguintes logs do WebSphere Portal:
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
 - b. No servidor de aplicativos revise os seguintes logs de configuração do WebSphere UDDI Registry:
 - `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/logs/cpudServer1/SystemOut.log`
 - `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/logs/cpudServer1/SystemErr.log`
2. Verifique se o sistema de arquivo no servidor de aplicativos não atingiu a capacidade. Isto pode ser determinado usando o comando **df -h**.
3. Verifique se o servidor cpudServer1 está iniciado. A verificação pode ser feita usando o WebSphere Application Server Administrative Console ou por etapas manuais. A seguir estão as etapas manuais:
 - a. No sistema servidor de aplicativos, efetue logon como `ibmadmin`.
 - b. Em uma janela de comando, execute: `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/serverStatus.sh -all -username waswebadmin -password WAS_ADMIN_PWD`, em que `WAS_ADMIN_PWD` é a senha do administrador do WebSphere Application Server.
 - c. Se a mensagem `ADMU0509I: O Servidor de Aplicativos "nodeagent" não pode ser acessado. Ele parece estar interrompido.` for exibida, inicie o nodeagent usando o seguinte comando: `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/startNode.sh`. Ignore esta etapa se a mensagem `ADMU0508I: O Servidor de Aplicativos "nodeagent" está INICIADO.` for exibida. Se foi necessário iniciar o nodeagent, uma mensagem semelhante à seguinte será exibida: `ADMU3000I: Servidor nodeagent aberto para e-business; o ID do processo é 26654.`

- a. Se a mensagem ADMU0509I: O Servidor de Aplicativos "cpudServer1" não pode ser acessado. Ele parece estar interrompido. For exibida, inicie o cpudServer1 usando o seguinte comando: `/opt/IBM/WebSphere/AppServer/profiles/cpodProfile1/bin/startServer.sh cpudServer1`. Ignore esta etapa se a mensagem ADMU0508I: O Servidor de Aplicativos "cpudServer1" está INICIADO. For exibida. Se você teve que iniciar o cpudServer1, uma mensagem semelhante à seguinte será exibida: ADMU3000I: Servidor cpudServer1 aberto para e-business; o ID do processo é 26654.

Importante: Os servidores devem ser iniciados e parados em uma ordem específica.

Inicie os servidores nesta ordem:




- a. nodeagent
- b. cpudServer1

Pare os servidores nesta ordem:

- a. cpudServer1
- b. nodeagent

O servidor cpudServer1 é interrompido executando o seguinte comando em uma janela de comando no servidor de aplicativos: `/opt/IBM/WebSphere/AppServer/profiles/cpodProfile1/bin/stopServer.sh cpudServer1 -username waswebadmin -password WAS_ADMIN_PWD`, em que `WAS_ADMIN_PWD` é a senha do administrador do WebSphere.

O nodeagent é interrompido executando o seguinte comando em uma janela de comando no servidor de aplicativos: `/opt/IBM/WebSphere/AppServer/profiles/cpodProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD`, em que `WAS_ADMIN_PWD` é a senha do administrador do WebSphere.

4. Verifique se o servidor cpudServer1 está iniciado. A verificação pode ser feita usando o WebSphere Application Server Administrative Console ou por etapas manuais. A seguir estão as etapas que usam o WebSphere Application Server Administrative Console:
 - a. Efetue logon no WebSphere Application Server Administrative Console em `http://APPLICATION_SERVER_HOST:9060/admin` usando o ID `admin` e a senha do WebSphere Application Server Administrative. `APPLICATION_SERVER_HOST` é o nome do host para o Servidor de Aplicativos.
 - b. Visualize o status do servidor cpudServer1 clicando em **Servidores > Tipos de Servidores > Servidores de Aplicativos WebSphere**.
 - O ícone  significa que o servidor está iniciado. Se necessário, selecione o servidor e clique em **Reiniciar** para reiniciar o servidor.
 - O ícone  significa que o servidor está interrompido. Selecione o servidor e clique em **Iniciar** para iniciar o servidor.
 - O ícone  significa que o status de servidor é indisponível. O Agente do Nó pode não estar em execução. Para iniciar o Agente do Nó, execute o comando `/opt/IBM/WebSphere/AppServer/profiles/cpodProfile1/bin/startNode.sh` em uma janela de comando.

Importante: Os servidores devem ser iniciados e parados em uma ordem específica.

Inicie os servidores nesta ordem:

- a. nodeagent
- b. cpudServer1

Pare os servidores nesta ordem:

- a. cpudServer1
- b. nodeagent

Para parar o servidor cpudServer, selecione o servidor e clique em **Parar**.

O nodeagent é interrompido executando o seguinte comando em uma janela de comando no servidor de aplicativos: `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD`, em que `WAS_ADMIN_PWD` é a senha do administrador do WebSphere.

5. Verifique se WebSphere UDDI User Console pode ser acessado.
 - a. No servidor de aplicativos, acesse: `https://APPLICATION_SERVER_HOST:9080/uddigui/`, em que `APPLICATION_SERVER_HOST` é o nome do host do servidor de aplicativos.

O que Fazer Depois

Resolva quaisquer problemas ou erros localizados e tente novamente o teste.

Messaging (Tópico de Publicação/Assinatura do WebSphere Message Broker) Teste

O teste do Messaging (Tópico de Publicação/Assinatura do WebSphere Message Broker) testa as funções de publicação e assinatura do WebSphere Message Broker. O teste publica uma mensagem para o tópico com o nome JNDI listado nas propriedades como `.jms/IopCatWmbPub`. O WebSphere Message Broker recebe a mensagem, em seguida, ele publica uma mensagem de retorno no tópico `IOP.CAT.PUB`. O teste será bem-sucedido se a mensagem de resposta for recebida. O teste falhará se houver um erro ou se a mensagem de resposta não for recebida dentro do período de tempo limite especificado no arquivo de propriedades.

Recursos

O teste do Messaging (Tópico de Publicação/Assinatura do WebSphere Message Broker) usa os seguintes recursos:

- WebSphere Portal Server (no servidor de aplicativos).
- WebSphere Message Queue (no).
- WebSphere Message Broker (no).

Determinação de problemas

Se o teste do Messaging (Tópico de Publicação/Assinatura do WebSphere Message Broker) falhar, faça o seguinte para localizar e resolver o problema.

Procedimento

1. Verifique se existe conectividade de rede entre o servidor de aplicativos e o . Isto pode ser feito enviando comandos **ping** com o nome do host abreviado e completo para e a partir de cada servidor. Os resultados dos comandos **ping** serão mostrados se o nome do host estiver sendo resolvido corretamente pelo DNS ou pelo arquivo `/etc/hosts`.
2. Revise os arquivos de log para as exceções de tempo de execução.
 - a. No servidor de aplicativos revise os seguintes logs do WebSphere Portal:
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
3. Verifique se os sistemas de arquivos no e no servidor de aplicativos não atingiram a capacidade. Isto pode ser determinado usando o comando **df -h**.
4. Verifique se o gerenciador de filas do WebSphere Message Queue e o broker do WebSphere Message Broker estão em execução.
 - a. No , efetue logon como o administrador do WebSphere Message Queue. Por exemplo, `mqm`.
 - b. Em uma janela de comando, execute **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; dspmq**. Você deverá ver uma mensagem semelhante à seguinte:
`QMNAME(IOC.MB.QM) STATUS(Running)`

- c. Se um status diferente de Em Execução foi retornado, inicie o gerenciador de filas do WebSphere Message Queue usando o seguinte comando: **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; strmqm IOC.MB.QM.**
 - d. No , efetue logon como o administrador do WebSphere Message Broker. Por exemplo, mqm.
 - e. Em uma janela de comando, execute **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; mqsilist**
Você deverá ver uma mensagem semelhante à seguinte:
BIP1284I: O Broker 'IOC_BROKER' no gerenciador de filas 'IOC.MB.QM' está em execução.
 - f. Se um status diferente de Em Execução foi retornado, inicie o broker do WebSphere Message Broker usando o seguinte comando: **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; mqsisstart IOC_BROKER.**
5. Verifique se existem erros nos logs. Os logs estão localizados no no diretório /var/log/messages. Procure mensagens com o prefixo 'BIP'. Procure também nomes de filas e registros de data e hora quando o teste foi executado.
 6. Se o broker ou os gerenciadores de filas não parecerem estar iniciados, eles também podem ser iniciados iniciando o e executando os scripts de inicialização para o sistema.

O que Fazer Depois

Resolva quaisquer problemas ou erros localizados e tente novamente o teste.

Messaging (Tópico de Publicação/Assinatura do WebSphere Message Queue)Teste

O teste do Messaging (Tópico de Publicação/Assinatura do WebSphere Message Queue) testa as funções de publicação e assinatura do WebSphere Message Queue. O teste cria um tópico especificado nas propriedades. Em seguida, ele publica uma mensagem no tópico e tenta ler imediatamente a mensagem publicada. O teste será bem-sucedido se a mensagem enviada puder ser lida. O teste falhará se houver algum erro ou se a mensagem não puder ser lida dentro de 15 segundos (15000 milissegundos).

Recursos

O teste do Messaging (Tópico de Publicação/Assinatura do WebSphere Message Queue) usa os seguintes recursos:

- WebSphere Portal Server (no servidor de aplicativos).
- WebSphere Message Queue (no).

Determinação de problemas

Se o teste do Messaging (Tópico de Publicação/Assinatura do WebSphere Message Queue) falhar, faça o seguinte para localizar e resolver o problema.

Procedimento

1. Verifique se existe conectividade de rede entre o servidor de aplicativos e o . Isto pode ser feito enviando comandos **ping** com o nome do host abreviado e completo para e a partir de cada servidor. Os resultados dos comandos **ping** serão mostrados se o nome do host estiver sendo resolvido corretamente pelo DNS ou pelo arquivo /etc/hosts.
2. Revise os arquivos de log para as exceções de tempo de execução.
 - a. No servidor de aplicativos revise os seguintes logs do WebSphere Portal:
 - /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log
 - /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log
3. Verifique se os sistemas de arquivos nos servidores não atingiram a capacidade. Isto pode ser determinado usando o comando **df -h**.
4. Verifique se o gerenciador de filas do WebSphere Message Queue está em execução.
 - a. No , efetue logon como o administrador do WebSphere Message Queue. Por exemplo, mqm.

- b. Em uma janela de comando, execute **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; dspmq**. Você deverá ver uma mensagem semelhante à seguinte:
`QMNAME(IOC.MB.QM) STATUS(Running)`
 - c. Se um status diferente de Em Execução foi retornado, inicie o gerenciador de filas do WebSphere Message Queue usando o seguinte comando: **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; strmqm IOC.MB.QM**.
5. Verifique se existem erros nos logs. Os logs estão localizados no no diretório `/var/log/messages`. Procure mensagens com o prefixo 'BIP'. Procure também nomes de filas e registros de data e hora quando o teste foi executado.
 6. Se o gerenciador de filas não parecer estar iniciado, ele também pode ser iniciado iniciando o e executando os scripts de inicialização para o sistema.

O que Fazer Depois

Resolva quaisquer problemas ou erros localizados e tente novamente o teste.

Messaging (Verificação de instalação do WebSphere Message Broker/Queue)Teste

O teste do Messaging (Verificação de instalação do WebSphere Message Broker/Queue) determina se o WebSphere Message Queue e o Message Broker podem ser acessados. Isto é feito executando o comando **mqsilist** do WebSphere Message Broker no sistema que está executando o WebSphere Message Broker.

Recursos

O Messaging (Verificação de instalação do WebSphere Message Broker/Queue) usa os seguintes recursos:

- WebSphere Portal Server (no servidor de aplicativos).
- WebSphere Message Queue e Message Broker (no).

Determinação de problemas

Se o teste do Messaging (Verificação de instalação do WebSphere Message Broker/Queue) falhar, faça o seguinte para localizar e resolver o problema.

Procedimento

1. Verifique se há conectividade de rede entre o sistema WebSphere Portal (no servidor de aplicativos) e o sistema WebSphere Message Broker (no). Isto pode ser feito enviando comandos **ping** com o nome do host abreviado e completo do a partir do servidor de aplicativos e vice-versa. Os resultados dos comandos **ping** serão mostrados se o nome do host estiver sendo resolvido corretamente pelo DNS ou pelo arquivo `/etc/hosts`.
2. Revise os arquivos de log para as exceções de tempo de execução.
 - a. No servidor de aplicativos revise os seguintes logs do WebSphere Portal:
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
3. Verifique se os arquivos nos sistemas servidor de aplicativos e não atingiram a capacidade. Isto pode ser determinado usando o comando **df -h**.
4. Verifique se o gerenciador de filas do WebSphere Message Queue e o broker do WebSphere Message Broker estão em execução.
 - a. No , efetue logon como o administrador do WebSphere Message Queue. Por exemplo, `mqm`.
 - b. Em uma janela de comando, execute **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; dspmq**. Você deverá ver uma mensagem semelhante à seguinte:
`QMNAME(IOC.MB.QM) STATUS(Running)`
 - c. Se um status diferente de Em Execução foi retornado, inicie o gerenciador de filas do WebSphere Message Queue usando o seguinte comando: **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; strmqm IOC.MB.QM**.

- d. No , efetue logon como o administrador do WebSphere Message Broker. Por exemplo, mqm.
 - e. Em uma janela de comando, execute **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; mqsilist**
Você deverá ver uma mensagem semelhante à seguinte:
BIP1284I: O Broker 'IOC_BROKER' no gerenciador de filas 'IOC.MB.QM' está em execução.
 - f. Se um status diferente de Em Execução foi retornado, inicie o broker do WebSphere Message Broker usando o seguinte comando: **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; mqsisstart IOC_BROKER.**
5. Verifique se existem erros nos logs. Os logs estão localizados no no diretório /var/log/messages. Procure mensagens com o prefixo 'BIP'. Procure também nomes de filas e registros de data e hora quando o teste foi executado.
 6. Se o broker ou os gerenciadores de filas não parecerem estar iniciados, eles também podem ser iniciados iniciando o e executando os scripts de inicialização para o sistema.

O que Fazer Depois

Resolva quaisquer problemas ou erros localizados e tente novamente o teste.

Messaging (Fila do WebSphere Message Broker/Queue)Teste

O teste do Messaging (Fila do WebSphere Message Broker/Queue) testa o WebSphere Message Queue colocando uma mensagem em uma fila.

Recursos

O teste do Messaging (Fila do WebSphere Message Broker/Queue) usa os seguintes recursos:

- WebSphere Portal Server (no servidor de aplicativos).
- WebSphere Message Queue (no).
- WebSphere Message Broker (no).

Determinação de problemas

Se o teste do Messaging (Fila do WebSphere Message Broker/Queue) falhar, faça o seguinte para localizar e resolver o problema.

Procedimento

1. Verifique se existe conectividade de rede entre o servidor de aplicativos e o . Isto pode ser feito enviando comandos **ping** com o nome do host abreviado e completo para e a partir de cada servidor. Os resultados dos comandos **ping** serão mostrados se o nome do host estiver sendo resolvido corretamente pelo DNS ou pelo arquivo /etc/hosts.
2. Revise os arquivos de log para as exceções de tempo de execução.
 - a. No servidor de aplicativos revise os seguintes logs do WebSphere Portal:
 - /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log
 - /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log
3. Verifique se os arquivos nos sistemas servidor de aplicativos e não atingiram a capacidade. Isto pode ser determinado usando o comando **df -h**.
4. Verifique se o gerenciador de filas do WebSphere Message Queue e o broker do WebSphere Message Broker estão em execução.
 - a. No , efetue logon como o administrador do WebSphere Message Queue. Por exemplo, mqm.
 - b. Em uma janela de comando, execute **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; dspmq.**
Você deverá ver uma mensagem semelhante à seguinte:
QMNAME(IOC.MB.QM) STATUS(Running)
 - c. Se um status diferente de Em Execução foi retornado, inicie o gerenciador de filas do WebSphere Message Queue usando o seguinte comando: **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; strmqm IOC.MB.QM.**

- d. No , efetue logon como o administrador do WebSphere Message Broker. Por exemplo, mqm.
 - e. Em uma janela de comando, execute **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; mqsilist**
Você deverá ver uma mensagem semelhante à seguinte:
BIP1284I: O Broker 'IOC_BROKER' no gerenciador de filas 'IOC.MB.QM' está em execução.
 - f. Se um status diferente de Em Execução foi retornado, inicie o broker do WebSphere Message Broker usando o seguinte comando: **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; mqsisstart IOC_BROKER.**
5. Verifique se existem erros nos logs. Os logs estão localizados no no diretório /var/log/messages. Procure mensagens com o prefixo 'BIP'. Procure também nomes de filas e registros de data e hora quando o teste foi executado.
 6. Se o broker ou os gerenciadores de filas não parecerem estar iniciados, eles também podem ser iniciados iniciando o e executando os scripts de inicialização para o sistema.

O que Fazer Depois

Resolva quaisquer problemas ou erros localizados e tente novamente o teste.

Monitoring (Console do Netcool Impact)Teste

O teste do Monitoring (Console do Netcool Impact) determina se o Netcool Impact Console está em execução e acessível pela URL do Netcool Impact Console.

Recursos

O teste do Monitoring (Console do Netcool Impact) usa o seguinte recurso:

- Netcool Impact Server (no)

Determinação de problemas

Se o teste do Monitoring (Console do Netcool Impact) falhar, faça o seguinte para localizar e resolver o problema.

Procedimento

1. Revise os arquivos de log para as exceções de tempo de execução.
 - a. No servidor de aplicativos revise os seguintes logs do WebSphere Portal:
 - /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log
 - /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log
 - b. No revise os seguintes logs do Netcool Impact:
 - /opt/IBM/netcool/eWAS/profiles/ImpactProfile/logs/server1/SystemOut.log
 - /opt/IBM/netcool/eWAS/profiles/ImpactProfile/logs/server1/SystemErr.log
2. Verifique se os sistemas de arquivos no sistema não atingiram a capacidade. Isto pode ser determinado usando o comando **df -h**.
3. Verifique se o servidor server1 está iniciado.
 - a. No sistema , efetue logon como wasadmin.
 - b. Em uma janela de comando, execute: /opt/IBM/netcool/eWAS/profiles/ImpactProfile/bin/serverStatus.sh -all -username wasadmin -password WAS_ADMIN_PWD, em que WAS_ADMIN_PWD é a senha do administrador do WebSphere Application Server.
 - c. Se a mensagem ADMU0509I: O Servidor de Aplicativos "server1" não pode ser acessado. Ele parece estar parado. for exibida, inicie o servidor server1, que também iniciará o Netcool Impact Console Server, usando o seguinte comando: /opt/IBM/netcool/eWAS/profiles/ImpactProfile/bin/startServer.sh server1. Ignore esta etapa se a mensagem ADMU0508I: O Servidor de Aplicativos "server1" está INICIADO for exibida. Se você teve que iniciar o servidor server1, uma mensagem semelhante à seguinte será exibida: ADMU3000I: Servidor server1 aberto para e-business; o ID do processo é 26654.

O servidor `server1` é interrompido executando o seguinte comando em uma janela de comando no :
`/opt/IBM/netcool/eWAS/profiles/ImpactProfile/bin/stopServer.sh server1 -username wasadmin -password WAS_ADMIN_PWD`, em que `WAS_ADMIN_PWD` é a senha do administrador do WebSphere.

4. Verifique se o Console do Netcool Impact pode ser acessado a partir do : `http://EVENT_SERVER_HOST:9080/nci`, em que `EVENT_SERVER_HOST` é o nome do host do .

O que Fazer Depois

Resolva quaisquer problemas ou erros localizados e tente novamente o teste.

Monitoring (Netcool Omnibus) Teste

O teste do Monitoring (Netcool Omnibus) determina se o Netcool Omnibus está disponível. Isso é feito executando o comando `nco_pa_status -server NCO_PA`.

Recursos

O teste do Monitoring (Netcool Omnibus) usa o seguinte recurso:

- Netcool Omnibus Server (no)

Determinação de problemas

Se o teste do Monitoring (Netcool Omnibus) falhar, faça o seguinte para localizar e resolver o problema.

Procedimento

1. Verifique se existe conectividade de rede entre o servidor de aplicativos e o . Isto pode ser feito enviando comandos **ping** com o nome do host abreviado e completo do a partir do servidor de aplicativos. Os resultados dos comandos **ping** serão mostrados se o nome do host estiver sendo resolvido corretamente pelo DNS ou pelo arquivo `/etc/hosts`.
2. Verifique se os serviços e o agente do servidor de Controle de Processo estão em execução.
 - a. Em uma janela de comando no , execute o comando `$NCHOME/omnibus/bin/nco_pa_status -server NCO_PA` como um usuário `netcool` do Linux.
 - b. Se os serviços não estiverem iniciados ou em execução, inicie o servidor executando o comando `/etc/init.d/nco start` no como um usuário `root` do Linux.
 - c. Se o agente de processo não estiver em execução, inicie o agente executando o comando `$NCHOME/omnibus/bin/nco_pad` no como um usuário `netcool` do Linux.
3. Revise os arquivos de log para as exceções de tempo de execução.
 - a. No servidor de aplicativos revise os seguintes logs do WebSphere Portal:
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
 - b. No , revise todos os logs que começam com NCO nos seguintes diretórios:
 - `/opt/IBM/netcool/log`
 - `/opt/IBM/netcool/omnibus/log`
4. Verifique se os sistemas de arquivos no sistema não atingiram a capacidade. Isto pode ser determinado usando o comando `df -h`.
5. Verifique se o portlet do Netcool Omnibus pode ser acessado a partir do servidor de aplicativos: `http://EVENT_SERVER_HOST:9060/ibm/console`, em que `EVENT_SERVER_HOST` é o nome do host do .

O que Fazer Depois

Resolva quaisquer problemas ou erros localizados e tente novamente o teste.

Monitoring (Tivoli Composite Application Manager Agents - *server*)Teste

O teste do Monitoring (Tivoli Composite Application Manager Agents - *server*) testa se os agentes do Tivoli Composite Application Manager estão em execução executando o comando **cinfo**.

Recursos

O teste do Monitoring (Tivoli Composite Application Manager Agents - *server*) usa os seguintes recursos:

- Tivoli Composite Application Manager
 - Agentes Tivoli Composite Application Manager (no servidor de aplicativos)
 - Agentes Tivoli Composite Application Manager (no)
 - Agentes Tivoli Composite Application Manager (no servidor de dados)
 - Agentes Tivoli Composite Application Manager (no Servidor de Gerenciamento)

Determinação de problemas

Se o teste do Monitoring (Tivoli Composite Application Manager Agents - *server*) falhar, faça o seguinte para localizar e resolver o problema.

Procedimento

1. Verifique se há conectividade de rede entre o servidor de aplicativos, o Servidor de Gerenciamento, o e o servidor de dados. Isto pode ser feito enviando comandos **ping** com o nome do host abreviado e completo do Servidor de Gerenciamento, do e do servidor de dados a partir do servidor de aplicativos. Os resultados dos comandos **ping** serão mostrados se o nome do host estiver sendo resolvido corretamente pelo DNS ou pelo arquivo `/etc/hosts`.
 2. Revise os arquivos de log para as exceções de tempo de execução.
 - a. No servidor de aplicativos revise os seguintes logs do WebSphere Portal:
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
 3. Verifique se os sistemas de arquivos no servidor de aplicativos, no Servidor de Gerenciamento, no e no servidor de dados não atingiram a capacidade. Isto pode ser determinado usando o comando **df -h**.
 4. Repita esta etapa no servidor de aplicativos, no Servidor de Gerenciamento, no e no servidor de dados para verificar se os componentes do Tivoli Monitoring estão em execução.
 - a. Efetue logon em uma sessão do terminal no servidor como raiz.
 - b. Execute o comando `/opt/IBM/ITM/bin/cinfo -r`. Serão exibidos resultados semelhantes ao seguinte. Os agentes serão diferentes nos servidores diferentes. Os agentes devem ter um status em execução.

```
***** Sun May 13 02:13:26 EDT 2012 *****
User: root Groups: root bin daemon sys adm disk wheel idslldap tdsproxy ivmgr tivoli
Host name : baapp2 Installer Lvl:06.22.01.00
CandleHome: /opt/IBM/ITM
*****
Host  Prod  PID  Owner  Start  ID  ..Status
baapp2  lz    31042  root   May09  None  ...running
baapp2  ht    18755  root   May09  None  ...running
baapp2  yn    4190  root   02:11  None  ...running
```
 - c. Inicie quaisquer agentes Tivoli Composite Application Manager que não estão em execução.
 - 1) Efetue logon em uma sessão do terminal no servidor como raiz.
 - 2) Execute `/opt/IBM/ITM/bin/itmcmd agent start PRODUCT_CODE`, em que `PRODUCT_CODE` é o valor PID para um agente localizado nos resultados do comando `/opt/IBM/ITM/bin/cinfo -o`.
5. Revise os arquivos de log para obter exceções.
 - a. No Servidor de Gerenciamento revise os seguintes logs do Tivoli Enterprise Monitoring Server e do Tivoli Enterprise Portal Server:
 - Tivoli Enterprise Monitoring Server: `/opt/IBM/ITM/logs/*_PRODUCT_CODE_{nnnnnn}.log`

- Tivoli Enterprise Portal Server: `/opt/IBM/ITM/logs/*_PRODUCT_CODE_{nnnnnn}.log`
em que `PRODUCT_CODE` é o PID retornado pelo comando `/opt/IBM/ITM/bin/cinfo -o`.

O que Fazer Depois

Resolva quaisquer problemas ou erros localizados e tente novamente o teste.

Monitoring (Tivoli Enterprise Monitoring Server) Teste

O teste do Monitoring (Tivoli Enterprise Monitoring Server) determina se o Tivoli Enterprise Monitoring Server em execução no Servidor de Gerenciamento está disponível. Uma consulta que solicita o status do componente é enviada para o servidor SOAP do Tivoli Monitoring Web Services. A consulta inclui um ID do usuário e senha inválidos para o sistema. A resposta deve indicar que um ID ou uma senha inválida foi usada. O erro indica que o Tivoli Enterprise Monitoring Server está operando corretamente.

Recursos

O teste do Monitoring (Tivoli Enterprise Monitoring Server) usa os seguintes recursos:

- Tivoli Enterprise Monitoring System (no Servidor de Gerenciamento)
 - Tivoli Monitoring Web Services SOAP Server
 - Tivoli Enterprise Portal Server
 - Banco de dados DB2 do Tivoli Enterprise Portal Server

Determinação de problemas

Se o teste do Monitoring (Tivoli Enterprise Monitoring Server) falhar, faça o seguinte para localizar e resolver o problema.

Procedimento

1. Verifique se existe conectividade de rede entre o servidor de aplicativos e o Servidor de Gerenciamento. Isto pode ser feito enviando comandos **ping** com o nome do host abreviado e completo do Servidor de Gerenciamento a partir do servidor de aplicativos. Os resultados dos comandos **ping** serão mostrados se o nome do host estiver sendo resolvido corretamente pelo DNS ou pelo arquivo `/etc/hosts`.
2. Revise os arquivos de log para as exceções de tempo de execução.
 - a. No servidor de aplicativos revise os seguintes logs do WebSphere Portal:
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
 - b. No Servidor de Gerenciamento, revise os seguintes logs do Servidor de Gerenciamento:
 - Tivoli Event Monitoring Server: `/opt/IBM/ITM/logs/{MGMT_SERVER_HOST}_ms_{nnnnnn}.log`
 - Tivoli Event Portal Server: `/opt/IBM/ITM/logs/{MGMT_SERVER_HOST}_cq_{nnnnnn}.log`
 - Logs do Embedded WebSphere Application Server:
 - Log de erro: `/opt/IBM/ITM/li6263/iw/profiles/ITMProfile/logs/ITMServer/SystemErr.log`
 - Log de saída: `/opt/IBM/ITM/li6263/iw/profiles/ITMProfile/logs/ITMServer/SystemOut.log`
 - Log de início: `/opt/IBM/ITM/li6263/iw/profiles/ITMProfile/logs/ITMServer/startServer.log`
3. Verifique se os sistemas de arquivos no Servidor de Gerenciamento não atingiram a capacidade. Isto pode ser determinado usando o comando **df -h**.
4. Verifique se os componentes Tivoli Monitoring estão em execução no Servidor de Gerenciamento.
 - a. Efetue logon em uma sessão do terminal no Servidor de Gerenciamento como raiz.
 - b. Execute o comando `/opt/IBM/ITM/bin/cinfo -r`.
5. Verifique se os bancos de dados do componente do Tivoli estão operacionais.

- a. Efetue logon em uma sessão do terminal no Servidor de Gerenciamento como db2inst1.
 - b. Execute o comando **ps -ef | grep db2inst1**.
 - c. Verifique se os processos do DB2 estão em execução. Eles incluem db2sysc, db2vend e db2acd.
 - d. Se os processos do DB2 não estiverem em execução, execute o comando **\$> db2start**.
 - e. Verifique nos logs do DB2 no servidor de dados se existem erros do banco de dados relacionados ao início de bancos de dados usados por componentes Tivoli. Os arquivos de log podem ser localizados no diretório /datahome/db2inst1/sqllib/db2dump no servidor de dados.
6. Nos resultados, verifique se o Tivoli Enterprise Monitoring Server está em execução, procurando uma entrada para ms. Se a entrada não estiver listada, o Tivoli Enterprise Monitoring Server não está em execução.
 7. Se o Tivoli Enterprise Monitoring Server não estiver em execução, inicie o servidor.
 - a. Efetue logon em uma sessão do terminal no Servidor de Gerenciamento como raiz.
 - b. Execute o comando **/opt/IBM/ITM/bin/itmcmd server start HUB_MWOS**.
 8. Nos resultados da etapa 4 na página 244, verifique se o Tivoli Enterprise Portal Server está em execução, procurando uma entrada para cq. Se a entrada não estiver listada, o Tivoli Enterprise Portal Server não está em execução.
 9. Se o Tivoli Enterprise Portal Server não estiver em execução, inicie o servidor.
 - a. Efetue logon em uma sessão do terminal no Servidor de Gerenciamento como raiz.
 - b. Execute o comando **/opt/IBM/ITM/bin/itmcmd agent start cq**.
 10. Nos resultados da etapa 4 na página 244, verifique se outros subcomponentes válidos estão em execução.

Tabela 79. Componentes do Tivoli Monitoring

Componente	Descrição
kf	Eclipse Help Server
cq	Tivoli Enterprise Portal Server
lz	Monitoring Agent para Linux OS
mlissegundos	Tivoli Enterprise Monitoring Server
yn	IBM Tivoli Composite Application Manager Agent for WebSphere Applications

O que Fazer Depois

Resolva quaisquer problemas ou erros localizados e tente novamente o teste.

Monitoring (Console do WebSphere Business Monitor Business Space) Teste

O teste do Monitoring (Console do WebSphere Business Monitor Business Space) determina se o WebSphere Business Monitor Business Space pode ser acessado usando a URL HTTP do WebSphere Business Monitor Business Space.

Recursos

O teste do Monitoring (Console do WebSphere Business Monitor Business Space) usa o seguinte recurso:

- WebSphere Application Server (no servidor de aplicativos).

Determinação de problemas

Se o teste do Monitoring (Console do WebSphere Business Monitor Business Space) falhar, faça o seguinte para localizar e resolver o problema de acesso.

Procedimento

1. Revise os arquivos de log para as exceções de tempo de execução.
 - a. No servidor de aplicativos revise os seguintes logs do WebSphere Portal:
 - /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log
 - /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log
 - b. No servidor de aplicativos revise os seguintes logs do WebSphere Business Monitor:
 - /opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/logs/WBM_DE.AppTarget.WBMNode1.0/SystemOut.log
 - /opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/logs/WBM_DE.AppTarget.WBMNode1.0/SystemErr.log
2. Verifique se os sistemas de arquivos no sistema servidor de aplicativos não atingiram a capacidade. Isto pode ser determinado usando o comando **df -h**.
3. Verifique se o servidor WebSphere Business Monitor foi iniciado. A verificação pode ser feita usando o WebSphere Application Server Administrative Console ou por etapas manuais. A seguir estão as etapas manuais:
 - a. No sistema servidor de aplicativos, efetue logon como **ibmadmin**.
 - b. Em uma janela de comando, execute: `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/serverStatus.sh -all -username waswebadmin -password WAS_ADMIN_PWD` em que **WAS_ADMIN_PWD** é a senha do administrador do WebSphere Application Server.
 - c. Se a mensagem **ADMU0509I: O Servidor de Aplicativos "nodeagent" não pode ser acessado. Ele parece estar interrompido.** for exibida, inicie o **nodeagent** usando o seguinte comando: `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/startNode.sh`. Ignore esta etapa se a mensagem **ADMU0508I: O Servidor de Aplicativos "nodeagent" está INICIADO.** for exibida. Se foi necessário iniciar o **nodeagent**, uma mensagem semelhante à seguinte será exibida: **ADMU3000I: Servidor nodeagent aberto para e-business; o ID do processo é 26654.**
 - a. Se a mensagem **ADMU0509I: O Servidor de Aplicativos "WBM_DE.AppTarget.WBMNode1.0" não pode ser acessado. Ele parece estar interrompido.** for exibida, inicie **WBM_DE.AppTarget.WBMNode1.0** usando o seguinte comando: `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/startServer.sh WBM_DE.AppTarget.WBMNode1.0`. Ignore esta etapa se a mensagem **ADMU0508I: O Servidor de Aplicativos "WBM_DE.AppTarget.WBMNode1.0" está INICIADO.** for exibida. Se você teve que iniciar o **WBM_DE.AppTarget.WBMNode1.0**, uma mensagem semelhante à seguinte será exibida: **ADMU3000I: Servidor WBM_DE.AppTarget.WBMNode1.0 aberto para e-business; o ID do processo é 26654.**

Importante: Os servidores devem ser iniciados e parados em uma ordem específica.

Inicie os servidores nesta ordem:




- a. **nodeagent**
- b. **WBM_DE.AppTarget.WBMNode1.0**

Pare os servidores nesta ordem:

- a. **WBM_DE.AppTarget.WBMNode1.0**
- b. **nodeagent**

O servidor **WBM_DE.AppTarget.WBMNode1.0** é interrompido executando o seguinte comando em uma janela de comando no servidor de aplicativos: `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/stopServer.sh WBM_DE.AppTarget.WBMNode1.0 -username waswebadmin -password WAS_ADMIN_PWD` em que **WAS_ADMIN_PWD** é a senha do administrador do WebSphere.

O **nodeagent** é interrompido executando o seguinte comando em uma janela de comando no servidor de aplicativos: `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` em que **WAS_ADMIN_PWD** é a senha do administrador do WebSphere.

4. Verifique se o servidor WebSphere Business Monitor foi iniciado. A verificação pode ser feita usando o WebSphere Application Server Administrative Console ou por etapas manuais. A seguir estão as etapas que usam o WebSphere Application Server Administrative Console:
 - a. Efetue login no WebSphere Application Server Administrative Console em `http://APPLICATION_SERVER_HOST:9060/admin` usando o ID `admin` e a senha do WebSphere Application Server Administrative. `APPLICATION_SERVER_HOST` é o nome do host para o servidor de aplicativos.
 - b. Visualize o status do servidor `WBM_DE.AppTarget.WBMNode1.0` clicando em **Servidores > Tipos de Servidores > Servidores de Aplicativos WebSphere**.
 - O ícone  significa que o servidor está iniciado. Se necessário, selecione o servidor e clique em **Reiniciar** para reiniciar o servidor.
 - O ícone  significa que o servidor está interrompido. Selecione o servidor e clique em **Iniciar** para iniciar o servidor.
 - O ícone  significa que o status de servidor é indisponível. O Agente do Nó pode não estar em execução. Para iniciar o Agente do Nó, execute o comando `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/startNode.sh` em uma janela de comando.

Importante: Os servidores devem ser iniciados e parados em uma ordem específica.

Inicie os servidores nesta ordem:

- a. `nodeagent`
- b. `WBM_DE.AppTarget.WBMNode1.0`

Pare os servidores nesta ordem:

- a. `WBM_DE.AppTarget.WBMNode1.0`
- b. `nodeagent`

Para parar o servidor `WBM_DE.AppTarget.WBMNode1.0`, selecione o servidor e clique em **Parar**.

O `nodeagent` é interrompido executando o seguinte comando em uma janela de comando no servidor de aplicativos: `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` em que `WAS_ADMIN_PWD` é a senha do administrador do WebSphere.

5. Verifique se o WebSphere Business Monitor Business Space pode ser acessado a partir do sistema WebSphere Portal, no servidor de aplicativos, usando a seguinte URL: `http://APPLICATION_SERVER_HOST:9084/BusinessSpace`. Em que `APPLICATION_SERVER_HOST` é o nome do host para o servidor de aplicativos.

O que Fazer Depois

Resolva quaisquer problemas ou erros localizados e tente novamente o teste.

Monitoring (Console do WebSphere Business Monitor Mobile Device) Teste

O teste do Monitoring (Console do WebSphere Business Monitor Mobile Device) determina se o WebSphere Business Monitor Mobile pode ser acessado usando a URL HTTP do WebSphere Business Monitor Mobile.

Recursos

O teste do Monitoring (Console do WebSphere Business Monitor Mobile Device) usa o seguinte recurso:

- WebSphere Application Server (no servidor de aplicativos).

Determinação de problemas

Se o teste do Monitoring (Console do WebSphere Business Monitor Mobile Device) falhar, faça o seguinte para localizar e resolver o problema de acesso.

Procedimento

1. Revise os arquivos de log para as exceções de tempo de execução.
 - a. No servidor de aplicativos revise os seguintes logs do WebSphere Portal:
 - /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log
 - /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log
 - b. No servidor de aplicativos revise os seguintes logs do WebSphere Business Monitor:
 - /opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/logs/WBM_DE.AppTarget.WBMNode1.0/SystemOut.log
 - /opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/logs/WBM_DE.AppTarget.WBMNode1.0/SystemErr.log
2. Verifique se os sistemas de arquivos no sistema servidor de aplicativos não atingiram a capacidade. Isto pode ser determinado usando o comando **df -h**.
3. Verifique se o servidor WebSphere Business Monitor foi iniciado. A verificação pode ser feita usando o WebSphere Application Server Administrative Console ou por etapas manuais. A seguir estão as etapas manuais:
 - a. No sistema servidor de aplicativos, efetue logon como **ibmadmin**.
 - b. Em uma janela de comando, execute: `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/serverStatus.sh -all -username waswebadmin -password WAS_ADMIN_PWD` em que **WAS_ADMIN_PWD** é a senha do administrador do WebSphere Application Server.
 - c. Se a mensagem **ADMU0509I: O Servidor de Aplicativos "nodeagent" não pode ser acessado. Ele parece estar interrompido.** for exibida, inicie o **nodeagent** usando o seguinte comando: `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/startNode.sh`. Ignore esta etapa se a mensagem **ADMU0508I: O Servidor de Aplicativos "nodeagent" está INICIADO.** for exibida. Se foi necessário iniciar o **nodeagent**, uma mensagem semelhante à seguinte será exibida: **ADMU3000I: Servidor nodeagent aberto para e-business; o ID do processo é 26654.**
 - a. Se a mensagem **ADMU0509I: O Servidor de Aplicativos "WBM_DE.AppTarget.WBMNode1.0" não pode ser acessado. Ele parece estar interrompido.** for exibida, inicie **WBM_DE.AppTarget.WBMNode1.0** usando o seguinte comando: `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/startServer.sh WBM_DE.AppTarget.WBMNode1.0`. Ignore esta etapa se a mensagem **ADMU0508I: O Servidor de Aplicativos "WBM_DE.AppTarget.WBMNode1.0" está INICIADO.** for exibida. Se você teve que iniciar o **WBM_DE.AppTarget.WBMNode1.0**, uma mensagem semelhante à seguinte será exibida: **ADMU3000I: Servidor WBM_DE.AppTarget.WBMNode1.0 aberto para e-business; o ID do processo é 26654.**

Importante: Os servidores devem ser iniciados e parados em uma ordem específica.

Inicie os servidores nesta ordem:




- a. **nodeagent**
- b. **WBM_DE.AppTarget.WBMNode1.0**

Pare os servidores nesta ordem:

- a. **WBM_DE.AppTarget.WBMNode1.0**
- b. **nodeagent**

O servidor **WBM_DE.AppTarget.WBMNode1.0** é interrompido executando o seguinte comando em uma janela de comando no servidor de aplicativos: `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/stopServer.sh WBM_DE.AppTarget.WBMNode1.0 -username waswebadmin -password WAS_ADMIN_PWD` em que **WAS_ADMIN_PWD** é a senha do administrador do WebSphere.

O **nodeagent** é interrompido executando o seguinte comando em uma janela de comando no servidor de aplicativos: `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` em que **WAS_ADMIN_PWD** é a senha do administrador do WebSphere.

4. Verifique se o servidor WebSphere Business Monitor foi iniciado. A verificação pode ser feita usando o WebSphere Application Server Administrative Console ou por etapas manuais. A seguir estão as etapas que usam o WebSphere Application Server Administrative Console:
 - a. Efetue login no WebSphere Application Server Administrative Console em `http://APPLICATION_SERVER_HOST:9060/admin` usando o ID `admin` e a senha do WebSphere Application Server Administrative. `APPLICATION_SERVER_HOST` é o nome do host para o servidor de aplicativos.
 - b. Visualize o status do servidor `WBM_DE.AppTarget.WBMNode1.0` clicando em **Servidores > Tipos de Servidores > Servidores de Aplicativos WebSphere**.
 - O ícone  significa que o servidor está iniciado. Se necessário, selecione o servidor e clique em **Reiniciar** para reiniciar o servidor.
 - O ícone  significa que o servidor está interrompido. Selecione o servidor e clique em **Iniciar** para iniciar o servidor.
 - O ícone  significa que o status de servidor é indisponível. O Agente do Nó pode não estar em execução. Para iniciar o Agente do Nó, execute o comando `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/startNode.sh` em uma janela de comando.

Importante: Os servidores devem ser iniciados e parados em uma ordem específica.

Inicie os servidores nesta ordem:

- a. `nodeagent`
- b. `WBM_DE.AppTarget.WBMNode1.0`

Pare os servidores nesta ordem:

- a. `WBM_DE.AppTarget.WBMNode1.0`
- b. `nodeagent`

Para parar o servidor `WBM_DE.AppTarget.WBMNode1.0`, selecione o servidor e clique em **Parar**.

O `nodeagent` é interrompido executando o seguinte comando em uma janela de comando no servidor de aplicativos: `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` em que `WAS_ADMIN_PWD` é a senha do administrador do WebSphere.

5. Verifique se o WebSphere Business Monitor Mobile pode ser acessado a partir do sistema WebSphere Portal, no servidor de aplicativos, usando a seguinte URL: `http://APPLICATION_SERVER_HOST:9084/mobile`. Em que `APPLICATION_SERVER_HOST` é o nome do host para o servidor de aplicativos.

O que Fazer Depois

Resolva quaisquer problemas ou erros localizados e tente novamente o teste.

Policy (Console do Tivoli Service Request Manager Maximo) Teste

O teste do Policy (Console do Tivoli Service Request Manager Maximo) determina se o Tivoli Service Request Manager Maximo pode ser acessado usando a página do Tivoli Service Request Manager Maximo Start Center.

Recursos

O teste do Policy (Console do Tivoli Service Request Manager Maximo) usa o seguinte recurso:

- Tivoli Service Request Manager Maximo (no).

Determinação de problemas

Se o teste do Policy (Console do Tivoli Service Request Manager Maximo) falhar, faça o seguinte para localizar e resolver o problema de acesso.

Procedimento

1. Revise os arquivos de log para as exceções de tempo de execução.
 - a. No servidor de aplicativos revise os seguintes logs do WebSphere Portal:
 - /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log
 - /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log
 - b. No revise os seguintes logs do Tivoli Service Request Manager:
 - /opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/logs/MXServer1/SystemOut.log
 - /opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/logs/MXServer1/SystemErr.log
2. Verifique se os sistemas de arquivos nos sistemas e servidor de aplicativos não atingiram a capacidade. Isto pode ser determinado usando o comando **df -h**.
3. Verifique se o servidor Tivoli Service Request Manager foi iniciado. A verificação pode ser feita usando o WebSphere Application Server Administrative Console ou por etapas manuais. A seguir estão as etapas manuais:
 - a. No sistema , efetue logon como `ibmadmin`.
 - b. Em uma janela de comando, execute: `/opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/bin/serverStatus.sh -all -username waswebadmin -password WAS_ADMIN_PWD` em que `WAS_ADMIN_PWD` é a senha do administrador do WebSphere Application Server.
 - c. Se a mensagem `ADMU0509I: O Servidor de Aplicativos "nodeagent" não pode ser acessado. Ele parece estar interrompido.` for exibida, inicie o `nodeagent` usando o seguinte comando: `/opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/bin/startNode.sh`. Ignore esta etapa se a mensagem `ADMU0508I: O Servidor de Aplicativos "nodeagent" está INICIADO.` for exibida. Se foi necessário iniciar o `nodeagent`, uma mensagem semelhante à seguinte será exibida: `ADMU3000I: Servidor nodeagent aberto para e-business; o ID do processo é 26654.`
 - a. Se a mensagem `ADMU0509I: O Servidor de Aplicativos "MXServer1" não pode ser acessado. Ele parece estar interrompido.` for exibida, inicie o `MXServer1` usando o seguinte comando: `/opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/bin/startServer.sh MXServer1`. Ignore esta etapa se a mensagem `ADMU0508I: O Servidor de Aplicativos "MXServer1" está INICIADO.` for exibida. Se você teve que iniciar o `MXServer1`, uma mensagem semelhante à seguinte será exibida: `ADMU3000I: Servidor MXServer1 aberto para e-business; o ID do processo é 26654.`

Importante: Os servidores devem ser iniciados e parados em uma ordem específica.

Inicie os servidores nesta ordem:

- a. `nodeagent`
- b. `MXServer1`




Pare os servidores nesta ordem:

- a. `MXServer1`
- b. `nodeagent`

O servidor `MXServer1` é interrompido executando o seguinte comando em uma janela de comando no : `/opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/bin/stopServer.sh MXServer1 -username waswebadmin -password WAS_ADMIN_PWD` em que `WAS_ADMIN_PWD` é a senha do administrador do WebSphere.

O `nodeagent` é interrompido executando o seguinte comando em uma janela de comando no : `/opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` em que `WAS_ADMIN_PWD` é a senha do administrador do WebSphere.

4. Verifique se o servidor Tivoli Service Request Manager foi iniciado. A verificação pode ser feita usando o WebSphere Application Server Administrative Console ou por etapas manuais. A seguir estão as etapas que usam o WebSphere Application Server Administrative Console:

- a. Efetue login no WebSphere Application Server Administrative Console em `http://EVENT_SERVER_HOST:9061/admin` usando o ID `admin` e a senha do WebSphere Application Server Administrative. `EVENT_SERVER_HOST` é o nome do host para o .
- b. Visualize o status do servidor MXServer1 clicando em **Servidores > Tipos de Servidores > Servidores de Aplicativos WebSphere**.
 - O ícone  significa que o servidor está iniciado. Se necessário, selecione o servidor e clique em **Reiniciar** para reiniciar o servidor.
 - O ícone  significa que o servidor está interrompido. Selecione o servidor e clique em **Iniciar** para iniciar o servidor.
 - O ícone  significa que o status de servidor é indisponível. O Agente do Nó pode não estar em execução. Para iniciar o Agente do Nó, execute o comando `/opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/bin/startNode.sh` em uma janela de comando.

Importante: Os servidores devem ser iniciados e parados em uma ordem específica.

Inicie os servidores nesta ordem:

- a. nodeagent
- b. MXServer1

Pare os servidores nesta ordem:

- a. MXServer1
- b. nodeagent

Para parar o servidor MXServer1, selecione o servidor e clique em **Parar**.

O nodeagent é interrompido executando o seguinte comando em uma janela de comando no :
`/opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` em que `WAS_ADMIN_PWD` é a senha do administrador do WebSphere.

5. Verifique se a página do Tivoli Service Request Manager Maximo Start Center pode ser acessada a partir do sistema WebSphere Portal, no , usando a seguinte URL: `http://EVENT_SERVER_HOST:31015/maximo/ui/login`. Em que `EVENT_SERVER_HOST` é o nome do host para o . O ID do usuário é `maxadmin`.

O que Fazer Depois

Resolva quaisquer problemas ou erros localizados e tente novamente o teste.

Security (Tivoli Access Manager)Teste

O teste do Security (Tivoli Access Manager) determina se o Tivoli Access Manager está em execução enviando um comando `pd_start` a partir do Servidor de Gerenciamento e verificando os resultados.

Recursos

O teste do Security (Tivoli Access Manager) usa o seguinte recurso:

- Tivoli Access Manager, incluindo a Política e Servidores de Autorização (no Servidor de Gerenciamento)

Determinação de problemas

Se o teste do Security (Tivoli Access Manager) falhar, faça o seguinte para localizar e resolver o problema.

Sobre Esta Tarefa

Nas etapas a seguir, `pdmgrd` é o Servidor de Autorização do Gerenciador de Acesso do Tivoli, `pdmgrproxyd` é o Servidor Proxy da Política, e `webseald-default` é o Servidor WebSEAL do Gerenciador de Acesso Tivoli.

Procedimento

1. Revise os arquivos de log para as exceções de tempo de execução.
 - a. No Servidor de Gerenciamento revise os seguintes logs do Tivoli Access Manager:
 - /var/PolicyDirector/log/msg__pdmgrd_utf8.log
 - /var/PolicyDirector/log/msg__pdacld_utf8.log
 - b. No servidor de aplicativos revise os seguintes logs do Tivoli Access Manager:
 - /var/pdweb/log/msg_*.log, em que * é qualquer valor.
 - /var/pdweb/log/config_data_*.log, em que * é qualquer valor.
2. Verifique se os sistemas de arquivos nos sistemas Servidor de Gerenciamento e servidor de aplicativos não atingiram a capacidade. Isto pode ser determinado usando o comando **df -h**.
3. Verifique se os componentes necessários do Tivoli Access Manager estão executando.
 - a. Efetue login em uma sessão do terminal no Servidor de Gerenciamento como raiz.
 - b. Execute o comando **pd_start status**. Os resultados serão semelhantes ao seguinte:

Tivoli Access Manager servers

Server	Enabled	Running

pdmgrd	yes	yes
pdacld	yes	yes
pdmgrproxyd	no	no

- c. Se os servidores pdmgrd ou pdacld não estiverem em execução, inicie-os executando o comando **pd_start start**.

Nota: Somente os servidores pdmgrd e pdacld são ativados no Servidor de Gerenciamento. Ambos são iniciados com o comando **pd_start start** e podem ser interrompidos com o comando **pd_start stop**.

4. Verifique se os componentes necessários do Tivoli Access Manager WebSEAL estão executando.
 - a. Efetue login em uma sessão do terminal no servidor de aplicativos como raiz.
 - b. Execute o comando **pd_start status**. Os resultados serão semelhantes ao seguinte:

Tivoli Access Manager servers

Server	Enabled	Running

pdmgrd	no	no
pdacld	no	no
pdmgrproxyd	no	no
webseald-default	yes	yes

- c. Se o servidor webseald-default não estiver em execução, inicie-o executando o comando **pd_start start**.

Nota: Apenas o servidor webseald-default é ativado no servidor de aplicativos. Ele é iniciado com o comando **pd_start start** e pode ser interrompido com o comando **pd_start stop**.

O que Fazer Depois

Resolva quaisquer problemas ou erros localizados e tente novamente o teste.

Security (Tivoli Access Manager Web Portal Manager)Teste

O teste do Security (Tivoli Access Manager Web Portal Manager) determina se o aplicativo Tivoli Access Manager Web Portal pode ser acessado pela URL do aplicativo Tivoli Access Manager Web Portal.

Recursos

O teste do Security (Tivoli Access Manager Web Portal Manager) usa o seguinte recurso:

- Tivoli Access Manager - Web Portal Manager (no Servidor de Gerenciamento).

Determinação de problemas

Se o teste do Security (Tivoli Access Manager Web Portal Manager) falhar, faça o seguinte para localizar e resolver o problema de acesso.

Procedimento

1. Revise os arquivos de log para as exceções de tempo de execução.
 - a. No servidor de aplicativos revise os seguintes logs do WebSphere Portal:
 - /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log
 - /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log
 - b. No Servidor de Gerenciamento revise os seguintes logs do Tivoli Access Manager - WebSphere Portal Manager:
 - /opt/IBM/WebSphere/AppServer/profiles/dmgr/logs/dmgr/SystemOut.log
 - /opt/IBM/WebSphere/AppServer/profiles/dmgr/logs/dmgr/SystemErr.log
2. Verifique se os sistemas de arquivos no sistema Servidor de Gerenciamento não atingiram a capacidade. Isto pode ser determinado usando o comando **df -h**.
3. Verifique se o Tivoli Access Manager - Web Portal Manager está iniciado.
 - a. No Servidor de Gerenciamento, efetue login como `ibmadmin`.
 - b. Em uma janela de comando, execute: `/opt/IBM/WebSphere/AppServer/profiles/dmgr/bin/serverStatus.sh -all waswebadmin -username-password WAS_ADMIN_PWD`, em que `WAS_ADMIN_PWD` é a senha do administrador do WebSphere Application Server.
 - c. Se a mensagem `ADMU0509I: O Servidor de Aplicativos "dmgr" não pode ser acessado. Ele parece estar parado.` for exibida, inicie o `dmgr` usando o seguinte comando: `/opt/IBM/WebSphere/AppServer/profiles/dmgr/bin/startManager.sh`. Ignore esta etapa se a mensagem `ADMU0508I: O Servidor de Aplicativos "dmgr" está INICIADO.` for exibida. Se você teve que iniciar o `dmgr`, uma mensagem semelhante à seguinte será exibida: `ADMU3000I: Servidor dmgr aberto para e-business; o ID do processo é 26654.`

O WebSphere Application Server Deployment Manager, incluindo o Tivoli Access Manager - Web Portal Manager, é interrompido executando o seguinte comando em uma janela de comando no Servidor de Gerenciamento: `/opt/IBM/WebSphere/AppServer/profiles/dmgr/bin/stopManager.sh -username waswebadmin -password WAS_ADMIN_PWD`, em que `WAS_ADMIN_PWD` é a senha do administrador do WebSphere.
4. Verifique se o Tivoli Access Manager - Web Portal Manager pode ser acessado a partir do sistema WebSphere Portal.
 - a. No Servidor de Gerenciamento, acesse a seguinte URL: `http://MANAGEMENT_SERVER_HOST9060/admin`. Em que `MANAGEMENT_SERVER_HOST` é o nome do host para Servidor de Gerenciamento.
 - b. Clique em **Tivoli Access Manager > Web Portal Manager > Usuários > Procurar Usuários**.
 - c. Efetue login usando como usuário `sec_master`.

O que Fazer Depois

Resolva quaisquer problemas ou erros localizados e tente novamente o teste.

Security (Console do WebSEAL)Teste

O teste do Security (Console do WebSEAL) determina se o Tivoli Access Manager e o Tivoli Access Manager WebSEAL estão em execução com os recursos necessários, acessando a URL HTTP do WebSEAL na Porta 80 e verificando a página retornada para a sequência "Intelligent Operations Center".

Recursos

O teste do Security (Console do WebSEAL) usa os seguintes recursos:

- Tivoli Access Manager, incluindo a Política e Servidores de Autorização (no Servidor de Gerenciamento)
- Tivoli Access Manager WebSEAL (no servidor de aplicativos)

Determinação de problemas

Se o teste do Security (Console do WebSEAL) falhar, faça o seguinte para localizar e resolver o problema.

Sobre Esta Tarefa

Nas etapas a seguir, pdmgrd é o Servidor de Autorização do Gerenciador de Acesso do Tivoli, pdmgrproxyd é o Servidor Proxy da Política, e webseald-default é o Servidor WebSEAL do Gerenciador de Acesso Tivoli.

Procedimento

1. Revise os arquivos de log para as exceções de tempo de execução.
 - a. No Servidor de Gerenciamento revise os seguintes logs do Tivoli Access Manager:
 - /var/PolicyDirector/log/msg__pdmgrd_utf8.log
 - /var/PolicyDirector/log/msg__pdaclد_utf8.log
 - b. No servidor de aplicativos revise os seguintes logs do Tivoli Access Manager:
 - /var/pdweb/log/msg__*.log, em que * é qualquer valor.
 - /var/pdweb/log/config_data__*.log, em que * é qualquer valor.
2. Verifique se os sistemas de arquivos nos sistemas Servidor de Gerenciamento e servidor de aplicativos não atingiram a capacidade. Isto pode ser determinado usando o comando **df -h**.
3. Verifique se os componentes necessários do Tivoli Access Manager estão executando.
 - a. Efetue logon em uma sessão do terminal no Servidor de Gerenciamento como raiz.
 - b. Execute o comando **pd_start status**. Os resultados serão semelhantes ao seguinte:
Tivoli Access Manager servers

Server	Enabled	Running
pdmgrd	yes	yes
pdaclد	yes	yes
pdmgrproxyd	no	no
 - c. Se os servidores pdmgrd ou pdaclد não estiverem em execução, inicie-os executando o comando **pd_start start**.

Nota: Somente os servidores pdmgrd e pdaclد são ativados no Servidor de Gerenciamento. Ambos são iniciados com o comando **pd_start start** e podem ser interrompidos com o comando **pd_start stop**.

4. Verifique se os componentes necessários do Tivoli Access Manager WebSEAL estão executando.
 - a. Efetue logon em uma sessão do terminal no servidor de aplicativos como raiz.
 - b. Execute o comando **pd_start status**. Os resultados serão semelhantes ao seguinte:
Tivoli Access Manager servers

Server	Enabled	Running
pdmgrd	no	no
pdaclد	no	no
pdmgrproxyd	no	no
webseald-default	yes	yes

- c. Se o servidor `webseald-default` não estiver em execução, inicie-o executando o comando **pd_start start**.

Nota: Apenas o servidor `webseald-default` é ativado no servidor de aplicativos. Ele é iniciado com o comando **pd_start start** e pode ser interrompido com o comando **pd_start stop**.

O que Fazer Depois

Resolva quaisquer problemas ou erros localizados e tente novamente o teste.

Web Server (Console do IBM HTTP Server) Teste

O teste do Web Server (Console do IBM HTTP Server) testa o acesso ao IBM HTTP Server acessando a URL do IBM HTTP Server.

Recursos

O Web Server (Console do IBM HTTP Server) usa o seguinte recurso:

- IBM HTTP Server (no servidor de aplicativos).

Determinação de problemas

Se o teste do Web Server (Console do IBM HTTP Server) falhar, faça o seguinte para localizar e resolver o problema.

Procedimento

1. Verifique se há conectividade de rede com o servidor de aplicativos. Isto pode ser feito enviando comandos **ping** com o nome do host abreviado e completo do servidor de aplicativos. Os resultados dos comandos **ping** serão mostrados se o nome do host estiver sendo resolvido corretamente pelo DNS ou pelo arquivo `/etc/hosts`.
2. Revise os arquivos de log para as exceções de tempo de execução.
 - a. No servidor de aplicativos revise os seguintes logs do IBM HTTP:
 - `/opt/IBM/HTTPServer/logs/error_log`
 - `/opt/IBM/HTTPServer/logs/access_log`
3. Verifique se o sistema de arquivo no servidor de aplicativos não atingiu a capacidade. Isto pode ser determinado usando o comando **df -h**.
4. Verifique se a página padrão do IBM HTTP Server pode ser acessada a partir do sistema WebSphere Portal.
 - a. No servidor de aplicativos, acesse: `https://APPLICATION_SERVER_HOST:82/`, em que `APPLICATION_SERVER_HOST` é o nome do host do servidor de aplicativos.
 - b. Se a página padrão não puder ser acessada, execute o comando **ps -ef | grep HTTPServer** para determinar se os processos do IBM HTTP Server estão em execução. Os processos do IBM HTTP Server começam com `/opt/IBM/HTTPServer/bin/httpd`. Haverá sete processos.
 - c. Se alguns, mas não todos os processos estiverem em execução, pare os processos em execução antes de reiniciar todos os processos.
 - 1) No servidor de aplicativos, efetue login como `root`.
 - 2) Altere para o diretório `/opt/IBM/HTTPServer/bin`.
 - 3) Execute os seguintes comandos para parar todos os processos do IBM HTTP em execução:

```
./apachectl stop
./adminctl stop
```
 - 4) Verifique se todos os processos foram interrompidos, executando o comando **ps -ef | grep HTTPServer**.
 - 5) Se alguns dos processos do IBM HTTP Server ainda estiverem em execução, pare-os usando **kill -9 pid**, em que `pid` é o identificador de processo do processo do IBM HTTP Server.

- d. Se os processos do HTTP Server não estiverem em execução, inicie os componentes do IBM HTTP Server.
 - 1) No servidor de aplicativos, efetue logon como root.
 - 2) Altere para o diretório `/opt/IBM/HTTPServer/bin`.
 - 3) Execute os seguintes comandos para iniciar todos os processos do IBM HTTP em execução:


```
./adminctl start
./apachectl start
```
 - 4) Verifique se todos os processos foram iniciados, executando o comando `ps -ef | grep HTTPServer`.

O que Fazer Depois

Resolva quaisquer problemas ou erros localizados e tente novamente o teste.

Fluxo de Eventos do Intelligent Operations CenterTeste

O teste do Fluxo de Eventos do Intelligent Operations Center verifica se os componentes críticos relacionados a processos de eventos do IBM Intelligent Operations Center estão funcionando conforme o esperado. Isto é feito simulando eventos externos e determinando se os resultados são os esperados.

Recursos

O teste do Fluxo de Eventos do Intelligent Operations Center usa o seguinte recurso:

- IBM WebSphere Message Broker (no servidor de aplicativos).
- IBM WebSphere Message Queue (no servidor de aplicativos).
- IBM Netcool/OMNIBus (no).
- IBM Netcool/Impact (no).
- IBM DB2 (no servidor de dados).

Determinação de problemas

Se o teste do Fluxo de Eventos do Intelligent Operations Center falhar, faça o seguinte para localizar e resolver o problema de acesso.

Procedimento

1. Verifique se os componentes do IBM Intelligent Operations Center estão em execução.
 - a. Em uma janela de comando no Servidor de Gerenciamento, execute `/opt/IBM/ISP/mgmt/scripts/IOControl.sh status all password`, em que *password* é a senha do administrador do IBM Intelligent Operations Center definida quando o IBM Intelligent Operations Center foi implementado.
 - b. Se houver componentes que não estão em execução, inicie esses componentes executando `/opt/IBM/ISP/mgmt/scripts/IOControl.sh start component_ID password`, em que *password* é a senha do administrador do IBM Intelligent Operations Center definida quando o IBM Intelligent Operations Center foi implementado e *component_ID* é um ID listado em Opções de Destino ao executar `/opt/IBM/ISP/mgmt/scripts/IOControl.sh help`.
2. Revise o log do Netcool/OMNIBus (`/opt/IBM/netcool/omnibus/log/ioc_xml.log`) no em busca de erros.
3. Se necessário, inicie a análise do Tivoli Netcool/OMNIBus executando o seguinte no.

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

O que Fazer Depois

Resolva quaisquer problemas ou erros localizados e tente novamente o teste.

Fluxo de Notificações do Intelligent Operations CenterTeste

O teste do Fluxo de Notificações do Intelligent Operations Center verifica se os componentes críticos relacionados a processos de notificação do IBM Intelligent Operations Center estão funcionando conforme o esperado. Isto é feito simulando notificações externas e determinando se os resultados são os esperados.

Recursos

O teste do Fluxo de Notificações do Intelligent Operations Center usa o seguinte recurso:

- IBM WebSphere Message Queue (no servidor de aplicativos).
- IBM Netcool/OMNIBus (no).
- IBM Netcool/Impact (no).
- IBM DB2 (no servidor de dados).

Determinação de problemas

Se o teste do Fluxo de Notificações do Intelligent Operations Center falhar, faça o seguinte para localizar e resolver o problema de acesso.

Procedimento

1. Verifique se os componentes do IBM Intelligent Operations Center estão em execução.
 - a. Em uma janela de comando no Servidor de Gerenciamento, execute **/opt/IBM/ISP/mgmt/scripts/IOControl.sh status all *password***, em que *password* é a senha do administrador do IBM Intelligent Operations Center definida quando o IBM Intelligent Operations Center foi implementado.
 - b. Se houver componentes que não estão em execução, inicie esses componentes executando **/opt/IBM/ISP/mgmt/scripts/IOControl.sh start *component_ID password***, em que *password* é a senha do administrador do IBM Intelligent Operations Center definida quando o IBM Intelligent Operations Center foi implementado e *component_ID* é um ID listado em Opções de Destino ao executar **/opt/IBM/ISP/mgmt/scripts/IOControl.sh help**.
2. Revise o log do Netcool/OMNIBus (/opt/IBM/netcool/omnibus/log/ioc_xml.log) no em busca de erros.
3. Se necessário, inicie a análise do Tivoli Netcool/OMNIBus executando o seguinte no.

```
mv /opt/IBM/netcool/omnibus/log/ioc_xml.log /opt/IBM/netcool/omnibus/log/old_ioc_xml.log  
/opt/IBM/netcool/omnibus/probes/nco_p_xml -name ioc_xml -propsfile /opt/IBM/netcool/omnibus/probes/linux2x86/ioc_xml.props &
```

O que Fazer Depois

Resolva quaisquer problemas ou erros localizados e tente novamente o teste.

Capítulo 7. Manutenção da Solução

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

Fazendo Backup de Dados

Para evitar a perda de dados importantes no IBM Intelligent Operations Center, faça backup de certos arquivos, diretórios e bancos de dados em intervalos regulares.

Ao estender o IBM Intelligent Operations Center, é uma boa prática desenvolver um procedimento de backup para os itens que você incluiu, por exemplo:

- Relatórios
- Bancos de dados auxiliares
- Tabelas de banco de dados
- Análítica customizada
- Portlets
- Aplicativos Java

Também considere dados que você acumulou, por exemplo:

- Dados do banco de dados Common Access Protocol (CAP)
- Dados do banco de dados IBM WebSphere Business Monitor
- Dados do registro do usuário Lightweight Directory Access Protocol (LDAP)
- Dados do Geographical Information System (GIS)

Adote uma convenção de nomenclatura para facilitar a identificação das extensões que você incluiu. Em geral, rastreie os dados que você criou ou acumulou desde que instalou a solução original. Implemente procedimentos para fazer backup dos dados, assim, ao atualizar a solução, você não perde dados importantes.

Fazendo Backup de Bancos de Dados

A tabela a seguir lista os bancos de dados recomendados para você fazer backup no IBM Intelligent Operations Center.

Tabela 80. Bancos de Dados do IBM Intelligent Operations Center

Serviço ou Componente	Instância do banco de dados	Nomes do banco de dados	Servidor
Banco de dados Intelligent Operations Center	db2inst1	<ul style="list-style-type: none">• IOCDB	servidor de dados
Portal	db2inst2	<ul style="list-style-type: none">• CUSTDB• FDBKDB• LKMDDB• JCRDB• COMMDB• RELDB	servidor de dados
Inteligência de negócios	db2inst3	<ul style="list-style-type: none">• CXLOGDB• CXCONTDB	servidor de dados

Tabela 80. Bancos de Dados do IBM Intelligent Operations Center (continuação)

Serviço ou Componente	Instância do banco de dados	Nomes do banco de dados	Servidor
Monitor de regra de negócios e atividade de negócios	db2inst4	<ul style="list-style-type: none"> • UDDIDB • WODMDCDB • MONITOR • WBMDB • RESDB 	servidor de dados
Modelo semântico	db2inst5	<ul style="list-style-type: none"> • JTS • IIC 	servidor de dados
Gerenciamento de solicitação de serviço	db2inst6	<ul style="list-style-type: none"> • MAXIMO 	servidor de dados
Gerenciamento de identidade	db2inst7	<ul style="list-style-type: none"> • TIMDB 	servidor de dados
Aplicativos	db2inst8	<ul style="list-style-type: none"> • LDAPDB • LDAPDB2B 	servidor de dados

Criando Capturas Instantâneas de Infraestrutura Virtual

A maioria das infraestruturas virtuais tem um recurso de captura instantânea que preserva o estado e os dados do seu ambiente virtual em um ponto específico no tempo. É altamente recomendado que você obtenha uma captura instantânea do seu ambiente antes de executar quaisquer mudanças significativas. Existem muitas ferramentas de gerenciamento de infraestrutura disponíveis, a maioria delas possui sua própria implementação de um recurso de captura instantânea. É importante se familiarizar com os requisitos específicos e as instruções sobre como fazer backup adequadamente do seu ambiente virtual lendo cuidadosamente as instruções no guia de administração fornecido pelo fornecedor da infraestrutura virtual.

Tarefas relacionadas:

“Faça Backup Antes de Customizar KPIs” na página 172

Faça backup e restaure KPIs que foram criadas ou modificadas com o IBM WebSphere Business Monitor, ou com o portlet Principais Indicadores de Desempenho.

Informações relacionadas:



Redbooks do IBM Smarter Cities Software Solutions

Ajustando o Desempenho

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

Informações relacionadas:



Guia de Ajuste de Desempenho do IBM Websphere Portal V 7.0



Centro de Informações do IBM Websphere Application Server, Network Deployment, Versão 7.0

Ajustando o servidor de aplicativos

Sobre Esta Tarefa

Utilize as diretrizes a seguir, que são baseadas nos resultados dos testes de desempenho, para configurar o tamanho de 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 mais informações, consulte o link relacionado no final do tópico.

Ajustando o WebSphere Application Server

Para obter informações sobre o ajuste de desempenho do WebSphere Application Server Versão 7, consulte o link relacionado no final do tópico.

Gerenciando Arquivos de Log

O IBM Intelligent Operations Center armazena arquivos de log em vários locais diferentes. Para evitar problemas de desempenho do sistema, faça periodicamente archives de arquivos de log e remova os arquivos de log originais.

Se você não gerenciar arquivos de log e o número de arquivos de log aumentar indefinidamente, os arquivos de log poderão eventualmente preencher uma partição de sistema de arquivos. Preencher uma partição do sistema de arquivos pode ter consequências negativas e potencialmente causar interrupção no sistema.

Para obter informações sobre os arquivos de log disponíveis no IBM Intelligent Operations Center, consulte o link no final do tópico.

Conceitos relacionados:

“Resolução de Problemas dos Componentes” na página 300

É possível utilizar a ferramenta de Verificação do Sistema para solucionar problemas dos IBM Intelligent Operations Center.

Atualizando o Token LTPA para Conexão Única

O IBM Intelligent Operations Center utiliza o token Lightweight Third-Party Authentication (LTPA) para ativar a conexão única em muitos serviços. O token e as chaves durante a instalação não expiram. É uma boa prática de segurança utilizá-lo para regenerar periodicamente o token LTPA e atualizar os serviços.

Antes de Iniciar

O produto do IBM Intelligent Operations Center deve ser instalado e todos os serviços iniciados antes de atualizar o token LTPA.

Este procedimento requer que todos os serviços sejam interrompidos e iniciados, para que a atualização não seja feita enquanto o sistema estiver em produção. Todos os usuários conectados ao sistema enfrentarão uma interrupção no serviço e poderão perder dados.

Procedimento

Gerar um novo token LTPA para o servidor de aplicativos

1. No servidor de aplicativos, abra um navegador da web e acesse `http://application_host:9060/ibm/console`, onde `application_host` é o nome do host do servidor de aplicativos.
2. Efetue logon como o usuário `webwasadmin` com a senha especificada no parâmetro `WAS.ADMIN.ACCOUNT.PWD` do arquivo de propriedades de topologia.

3. Clique em **Segurança > Segurança Global > Mecanismos de Autenticação e Expiração > LTPA > Gerar Chaves**.
4. Insira uma senha duas vezes para o novo token LTPA. A senha é utilizada para criptografar o token LTPA. Essa senha será utilizada ao importar o token LTPA. Registre a senha como o parâmetro `WAS.LTPA.PWD` no arquivo de propriedades de topologia.
5. Insira o caminho e o nome do arquivo, onde o token LTPA será salvo, por exemplo, `/tmp/newapp.ltpa`. Se você especificar um caminho diferente ou nome de arquivo, substitua o caminho e nome de arquivo por `/tmp/newapp.ltpa` no restante destas etapas.
6. Clique em **Exportar Chaves**. O novo token LTPA será salvo como `/tmp/newapp.ltpa`.
7. Clique em **Mensagens > Salvar**. As atualizações serão salvas. Ignore todos os avisos sobre o domínio de conexão única que não está sendo definido.

Copie o novo token LTPA para o .

8. No servidor de aplicativos, efetue o logon como usuário raiz e abra uma janela do terminal.
9. Execute o comando `cp /tmp/newapp.ltpa /tmp/stproxy.ltpa`. Isto substituirá o arquivo criado quando o IBM Intelligent Operations Center foi instalado.
10. Execute o comando `scp /tmp/newapp.ltpa root@event_host :/tmp/newapp.ltpa`, onde `event_host` é o nome do host do . Quando solicitado, insira a senha raiz para o . O token LTPA é copiado para o .
 Importe o novo token LTPA
11. No , abra um navegador da web e acesse `http://event_host:9061/ibm/console`, onde `event_host` é o nome completo do .
12. Efetue logon como o usuário `webwasadmin` com a senha especificada no parâmetro `WAS.ADMIN.ACCOUNT.PWD` do arquivo de propriedades de topologia.
13. Clique em **Segurança > Administração Segura, Aplicativos e Infraestrutura > Mecanismos de Autenticação e Expiração**.
14. Insira a senha para o token LTPA e `/tmp/newapp.ltpa` para o nome do arquivo.
15. Clique em **Importar Chaves (Import Keys)**.
16. Clique em **Mensagens > Salvar**. As atualizações serão salvas.

Gere um novo token LTPA para o .

17. Clique em **Mecanismos de autenticação e expiração > Gerar Chaves**.
18. Insira uma senha duas vezes para o token LTPA novo. Essa senha será utilizada ao importar o token LTPA.
19. Insira o caminho e o nome do arquivo onde o token LTPA será salvo, por exemplo, `/tmp/newevent.ltpa`. Se especificar um caminho diferente ou nome do arquivo, substitua o caminho e nome de arquivo por `/tmp/newevent.ltpa`, no restante destas etapas.
20. Clique em **Exportar Chaves**. O novo token LTPA será salvo como `/tmp/newevent.ltpa`.
 Copie o novo token LTPA do para o servidor de aplicativos.

21. No servidor de aplicativos, efetue o logon como usuário raiz e abra uma janela do terminal.
22. Execute o comando `scp /tmp/newevent.ltpa root@event_host :/tmp/newevent.ltpa`, onde `event_host` é o nome do host do . Quando solicitado, insira a senha raiz para o . O token LTPA é copiado para o .
 Atualize o serviço de segurança com o novo token LTPA.

23. No servidor de aplicativos, efetue logon como usuário raiz e abra uma janela do terminal.
24. Execute o comando `cp /tmp/newapp.ltpa /opt/pdweb/etc/`.
25. Execute o comando `cp /tmp/newevent.ltpa /opt/pdweb/etc/`.
26. Crie um nome de comando chamado `/tmp/pd.com` que contenha os seguintes comandos:

```
server task default-webseald-application_host create -t tcp -h application_host -p 9086 -x -b
ignore -i -f -A -F /opt/pdweb/etc/newapp.ltpa -Z appLTPApw /stwebclient
server task default-webseald-application_host create -t tcp -h application_host -p 9086 -x -b
ignore -i -f -A -F /opt/pdweb/etc/newapp.ltpa -Z appLTPApw /stbaseapi
server task default-webseald-application_host create -t tcp -h application_host -p 9086 -x -b
ignore -i -f -A -F /opt/pdweb/etc/newapp.ltpa -Z appLTPApw /stwebapi
server task default-webseald-application_host create -t tcp -h application_host -p 9081 -b
supply -c iv-user,iv-creds -i -j -f -J trailer -A -2 -F /opt/pdweb/etc/newapp.ltpa -Z appLTPApw
/cognosserver task default-webseald-application_host create -t tcp -h event_host -p 82 -i
-j -f -J trailer -A -2 -F /opt/pdweb/etc/newevent.ltpa -Z eventLTPApw /tsm
```


Em que:

application_host

é o nome completo do host do servidor de aplicativos.

event_host

é o nome completo do host do .

appLTPApw

é a senha especificada ao criar o token LTPA para o servidor de aplicativos.

eventLTPApw

é a senha especificada ao criar o token LTPA para o .

27. Execute o comando `/opt/PolicyDirector/bin/pdadmin -a sec_master -p password / tmp/pd.com` em que *password* é a senha definida no parâmetro TAM.WEBSEAL.ADMIN.PWD do arquivo de propriedades de topologia.

Atualize a conexão única para o serviço de colaboração.

28. Siga as etapas do “Configurando Conexão Única para Serviços de Colaboração” na página 52 para atualizar a conexão única para o serviço de colaboração.

Interrompa e reinicie todos os serviços.

29. Utilizando o Ferramenta de Controle de Plataforma, interrompa todos os serviços.

30. Utilizando o Ferramenta de Controle de Plataforma, inicie todos os serviços. Os tokens LTPA serão propagados para todos os serviços.

Dicas de Manutenção

Dicas adicionais para a manutenção da solução são documentadas na forma de notas técnicas individuais no Portal de Suporte IBM.

O seguinte link ativa uma consulta customizada da base de conhecimento de Suporte em tempo real para todas as versões do IBM Intelligent Operations Center: Visualize todas as dicas de manutenção para o IBM Intelligent Operations Center.

Capítulo 8. Usando a Interface da Solução

O IBM Intelligent Operations Center é uma solução baseada na Web usando tecnologia de portal. É possível acessar a solução com qualquer dos navegadores da web suportados.

Para obter informações sobre navegadores da web suportados, consulte o link no final do tópico.

Informações relacionadas:



Navegadores Suportados do IBM Intelligent Operations Center

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 também fornecerá a URL do endereço da web para acessar o portal de soluções.

Sobre Esta Tarefa

Use o procedimento a seguir para iniciar uma nova sessão do navegador e acessar o IBM Intelligent Operations Center. Também é possível acessar a solução a partir de outro IBM Smarter Cities Software Solutions instalado em seu ambiente. Na barra de navegação principal na parte superior do portal, selecione o **Intelligent Operations Center**.

Procedimento

1. Insira a URL no campo de endereço do navegador.

Nota: O nome completo do domínio é necessário na URL, por exemplo, `http://application_server_hostname/wpsv70/wps/myportal`. Se você usar o endereço IP em vez do domínio completo registrado, alguns portlets poderão não ser exibidos corretamente.

2. Na página de login, insira o ID do usuário e a senha.
3. Clique em **Conectar**.

Resultados

Somente as páginas, os recursos e os dados que você tem permissão para acessar serão exibidos. Entre em contato com o administrador se precisar de mais acesso.

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 265

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 81. 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 ter de 5 a 60 caracteres de comprimento. Senhas válidas devem conter somente os caracteres a-z, A-Z, e 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
E-mail	Um endereço de e-mail pode ser inserido pelo administrador ou pelo usuário.	Sim

Nota: Atributos marcados com asterisco são obrigatórios para a criação bem-sucedida de um novo usuário. Atributos não marcados com 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.

Usando Páginas

Uma página consiste em um ou mais portlets complementares. Ao usar o IBM Intelligent Operations Center, é possível interagir com os portlets em uma página para acessar as informações requeridas e responder aos eventos, conforme necessário.

O IBM Intelligent Operations Center fornece seis diferentes visualizações de páginas de amostra.

Administrador

Se você tiver acesso de administrador, na visualização da página será possível acessar o serviço do portal para gerenciar páginas. É possível editar uma página ou criar uma nova. Clique no lado direito da guia do nome da página e selecione uma opção no menu da página. Para obter mais informações, consulte o link no final do tópico.

Tarefas relacionadas:

“Criando ou Customizando uma Página” na página 145

É possível criar novas páginas para que sejam incluídas no IBM Intelligent Operations Center e especificar quais portlets exibir nessas páginas. É possível customizar a aparência e o layout dos portlets incluídos em cada página.

Visualização Supervisor: Status

Use a visualização Supervisor: Status para obter uma visualização consolidada de principais indicadores de desempenho (KPIs) e eventos principais. A visualização Supervisor: Status 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 Supervisor: Status é uma página da Web interativa. A página contém os portlets listados em Tabela 82. Os portlets são seções independentes da página que cooperam uns com os outros para fornecer informações abrangentes e interação no nível executivo.

Tabela 82. Portlet da Visualização Supervisor: Status

Portlet	Descrição
“Status” na página 290	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 275	Para focar em uma categoria de KPI específica no portlet Drill Down de Key Performance Indicator, clique na categoria no portlet Status. Esta categoria é então exibida por si própria no portlet Drill Down de Key Performance Indicator. É possível usar a lista para inspecionar os KPIs subjacentes até acessar os detalhes do KPI que causaram a mudança de status.

Tabela 82. Portlet da Visualização Supervisor: Status (continuação)

Portlet	Descrição
“Notificações” na página 286	O portlet Notificações 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 Notificações.
“Minhas Atividades” na página 284	Um usuário que está conectado pode visualizar as atividades designadas a ele no portlet Minhas Atividades. No portlet Minhas Atividades, as atividades são agrupadas pelos procedimentos padrão de operação pai. Cada procedimento padrão de operação corresponde a um evento individual.
“Contatos” na página 271	O portlet Contatos pode exibir uma lista de seus contatos organizados por categoria. É possível organizar os contatos em categorias baseadas nas pessoas com as quais você precisa se comunicar. Por exemplo, é possível ter uma categoria para contatos de trabalho geral e outra categoria para contatos de trabalho do projeto. Com o portlet Contatos, é possível comunicar-se com pessoas e modificar seu status online, contatos ou grupos.

Visualização Supervisor: Operações

Use a visualização Supervisor: Operações para obter uma visão geral dos eventos à medida que eles ocorrem. A visualização Supervisor: Operações é destinada a supervisores e gerentes que monitoram eventos atuais e planejam eventos futuros.

A visualização Supervisor: Operações é uma página da Web interativa. A página contém os portlets listados em Tabela 83. Os portlets são seções independentes da página que cooperam uns com os outros para fornecer informações abrangentes e interação no nível gerencial.

Tabela 83. Portlet da Visualização Supervisor: Operações

Portlet	Descrição
“Mapa” na página 279	Um mapa da região geográfica, com marcadores de eventos e de recursos. Um formulário de filtro para selecionar as categorias dos eventos a serem mostrados no mapa e nos portlets vinculados ao portlet Mapa. Um formulário de filtro para selecionar as capacidades dos recursos a serem mostrados no mapa e na guia Recursos no portlet vinculado Detalhes. Para visualizar este formulário, primeiro selecione Visualizar Recursos Próximos no portlet Detalhes.
“Detalhes” na página 272	O portlet Detalhes é um portlet de lista interativo. Todos os eventos que você está autorizado a visualizar estão visíveis na lista de eventos e em qualquer portlet de mapa vinculado ao portlet Detalhes.

Tabela 83. Portlet da Visualização Supervisor: Operações (continuação)

Portlet	Descrição
“Notificações” na página 286	O portlet Notificações 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 ocorrem incidentes relacionados dentro de uma área definida, um alerta é enviado para o portlet Notificações.
“Minhas Atividades” na página 284	Um usuário que está conectado pode visualizar as atividades designadas a ele no portlet Minhas Atividades. No portlet Minhas Atividades, as atividades são agrupadas pelos procedimentos padrão de operação pai. Cada procedimento padrão de operação corresponde a um evento individual.
“Contatos” na página 271	O portlet Contatos pode exibir uma lista de seus contatos organizados por categoria. É possível organizar os contatos em categorias baseadas nas pessoas com as quais você precisa se comunicar. Por exemplo, é possível ter uma categoria para contatos de trabalho geral e outra categoria para contatos de trabalho do projeto. Com o portlet Contatos, é possível comunicar-se com pessoas e modificar seu status online, contatos ou grupos.

Visualização Operator: Operações

Use a visualização Operator: Operações para manter o reconhecimento dos eventos e sua localização. A visualização Operator: Operações é destinada a operadores, gerentes ou outras pessoas que monitoram e respondem a eventos atuais.

A visualização Operator: Operações é uma página da Web interativa. A página contém os portlets listados em Tabela 84. Os portlets são seções independentes da página que cooperam uns com os outros para fornecer informações abrangentes e interação no nível de operações.

Tabela 84. Portlets de Visualização do Operator: Operações

Portlet	Descrição
“Mapa” na página 279	Um mapa da região geográfica, com marcadores de eventos e de recursos. Um formulário de filtro para selecionar as categorias dos eventos a serem mostrados no mapa e nos portlets vinculados ao portlet Mapa. Um formulário de filtro para selecionar as capacidades dos recursos a serem mostrados no mapa e na guia Recursos no portlet vinculado Detalhes. Para visualizar este formulário, primeiro selecione Visualizar Recursos Próximos no portlet Detalhes.
“Detalhes” na página 272	O portlet Detalhes é um portlet de lista interativo. Todos os eventos que você está autorizado a visualizar estão visíveis na lista de eventos e em qualquer portlet de mapa vinculado ao portlet Detalhes.
“Notificações” na página 286	O portlet Notificações 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 dois eventos graves ocorrem juntos no mesmo local e horário, é enviado um alerta para o portlet Notificações.

Tabela 84. Portlets de Visualização do Operador: Operações (continuação)

Portlet	Descrição
“Minhas Atividades” na página 284	Um usuário que está conectado pode visualizar as atividades designadas a ele no portlet Minhas Atividades. No portlet Minhas Atividades, as atividades são agrupadas pelos procedimentos padrão de operação pai. Cada procedimento padrão de operação corresponde a um evento individual.
“Contatos” na página 271	O portlet Contatos pode exibir uma lista de seus contatos organizados por categoria. É possível organizar os contatos em categorias baseadas nas pessoas com as quais você precisa se comunicar. Por exemplo, é possível ter uma categoria para contatos de trabalho geral e outra categoria para contatos de trabalho do projeto. Com o portlet Contatos, é possível comunicar-se com pessoas e modificar seu status online, contatos ou grupos.

Supervisor: Relatórios

Use a visualização Supervisor: Relatórios para ver um resumo de dados do evento gerados a partir da execução de relatórios predefinidos. Além disso, é possível usar a visualização Supervisor: Relatórios para criar relatórios personalizados ou configurar relatórios predefinidos. Esses relatórios são destinados a operadores, gerenciadores ou outros eventos de monitoramento atuais e eventos de planejamento futuros.

A visualização Supervisor: Relatórios é uma página da web interativa que contém diferentes relatórios baseados nos dados selecionados para fornecer informações abrangentes e interação em nível de supervisor. Essas informações são exibidas em gráficos que resumem os dados do evento que estão no sistema.

Na visualização Supervisor: Relatórios, você configura e visualiza relatórios em portlets “Relatórios” na página 288. Por padrão, alguns dos portlets Relatórios exibem relatórios de amostra.

Operador: Relatórios

Use a visualização Operador: Relatórios para manter o reconhecimento dos relatórios, eventos e alertas. A visualização Operador: Relatórios é destinada a operadores, gerentes ou outras pessoas que monitoram relatórios.

A visualização Operador: Relatórios fornece um resumo de dados do evento gerados a partir da execução de relatórios predefinidos. Também é possível usar a visualização Operador: Relatórios para visualizar relatórios personalizados. Esses relatórios ajudam a monitorar eventos atuais, tomar ações para manipular eventos e planejar eventos futuros.

A visualização Operador: Relatórios é uma página da Web interativa. É possível escolher a visualização de diversos relatórios diferentes que fornecem informações abrangentes e interação em nível de operador.

Na visualização Operador: Relatórios, você configura e visualiza relatórios em portlets “Relatórios” na página 288. Por padrão, alguns dos portlets Relatórios exibem relatórios de amostra.

Visualização Mapa de Localização

Use a visualização Mapa de Localização para manter o reconhecimento de eventos e suas posições em um mapa de localização. A visualização Mapa de Localização é destinada a operadores, gerentes ou outras pessoas que monitoram e respondem a eventos atuais.

A visualização Mapa de Localização é uma página da Web interativa. A página contém os portlets listados em Tabela 85 na página 271. Os portlets são seções independentes da página que cooperam uns com os outros para fornecer informações abrangentes e interação no nível de operações.

Tabela 85. Portlet da Visualização Mapa de Localização

Portlet	Descrição
“Mapa de Localização” na página 276	Um diagrama do local com marcadores para eventos. Um formulário de filtro para selecionar as categorias do evento mostradas no mapa. Uma lista dos mapas de localização disponíveis organizados por classificação.
“Detalhes” na página 272	O portlet Detalhes é um portlet de lista interativo. Todos os eventos que você está autorizado a visualizar estão visíveis na lista de eventos e em qualquer portlet de mapa vinculado ao portlet Detalhes.

Usando Portlets

Um portlet fornece acesso a informações que podem ser visualizadas e com as quais é possível interagir em uma página de portal.

O IBM Intelligent Operations Center fornece vários portlets diferentes.

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 no menu que é exibido da seguinte forma:

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

Administrador

Customizando um Portlet

Como um administrador, é possível alterar as configurações de portlet clicando no canto superior direito do portlet e selecionando uma opção no menu de portlet.

Há dois modos possíveis de customização, cada um alterando as configurações de portlet para todos os usuários:

- **Editar Configurações Compartilhadas** altera o portlet apenas para a instância do portlet em que você está ao alterar as configurações.
- **Configurar** altera as configurações globais do portlet para todas as instâncias do portlet sempre que elas ocorrem.

Os modos de customização que estão disponíveis dependem das permissões associadas ao seu ID do usuário. As configurações globais são substituídas por configurações compartilhadas.

Os portlets que são fornecidos com o IBM Intelligent Operations Center têm algumas configurações que são específicas para um tipo de portlet, por exemplo, configurar o nível de zoom padrão para um mapa. Além disso, é possível configurar parâmetros genéricos do portlet que são comuns nos portlets fornecidos, por exemplo, o título do portlet.

Contatos

Use o portlet Contatos para enviar mensagens instantâneas na solução.

O portlet Contatos pode exibir uma lista de seus contatos organizados por categoria. É possível organizar os contatos em categorias baseadas nas pessoas com as quais você precisa se comunicar. Por exemplo, é

possível ter uma categoria para contatos de trabalho geral e outra categoria para contatos de trabalho do projeto. Com o portlet Contatos, é possível comunicar-se com pessoas e modificar seu status online, contatos ou grupos.

Clique nos menus na parte superior do portlet:

- **Arquivo** para incluir contatos, modificar grupos ou efetuar logout
- **Ferramentas** para configurar um bate-papo, reunião ou anúncio; ou para alterar suas configurações de privacidade
- **Ajuda** para obter informações mais detalhadas sobre como usar o portlet

Clique no status para modificar status e mensagem. O status padrão indica que você está disponível. É possível alterar o status para indicar que você está fora do computador, em uma reunião ou que não deseja ser incomodado.

O status dos usuários que efetuaram logon é exibido no portlet Contatos. Se um usuário que está conectado fechar a janela do navegador ou efetuar logoff do WebSphere Portal, o status desse usuário ainda será exibido como conectado até que a sessão expire. No entanto, nenhuma mensagem enviada a esse usuário, depois que o usuário fechou a janela do navegador ou efetuou logoff, será entregue. Consequentemente, uma mensagem de erro será entregue ao usuário que está tentando enviar a mensagem. Para assegurar que o status seja atualizado imediatamente no portlet Contatos, efetue logoff clicando em **Arquivo > Efetuar Logout**.

Nota: Para que este portlet funcione conforme o esperado, você deve efetuar logon no portal de soluções usando o nome completo do domínio do servidor de aplicativos do IBM Intelligent Operations Center. Se você efetuar logon no portal usando o endereço IP ou um alias do nome do host em vez do nome completo do domínio registrado, este portlet não será exibido corretamente.

Administrador

Se tiver acesso de administrador, você poderá customizar este portlet. Clique no botão no canto superior direito do portlet para ver as opções de customização do menu de portlet. As configurações compartilhadas afetam o conteúdo desse portlet para todos os usuários, mas apenas para esta ocorrência do portlet.

As configurações que podem ser alteradas para o portlet Contatos são:

- Arquivo de ajuda
- Altura do portlet
- Altura do portlet quando maximizado
- Título do Portlet
- Pacote de Recursos

Referências relacionadas:

“Configurações do Portlet do Contatos” na página 147

Customize o portlet do Contatos alterando as configurações nos campos da janela **Configurações Compartilhadas**.

Detalhes

Use o portlet Detalhes para visualizar, monitorar e gerenciar eventos no IBM Intelligent Operations Center.

O portlet Detalhes é um portlet de lista interativo. Todos os eventos que você está autorizado a visualizar estão visíveis na lista de eventos e em qualquer portlet de mapa vinculado ao portlet Detalhes.

Os recursos na proximidade de um evento podem ser exibidos em uma lista de recursos e em um mapa.

Eventos e Recursos

O portlet Detalhes possui dois elementos de interface interativa, conforme mostrado na tabela a seguir:

Tabela 86. Exibição do Portlet Detalhes

Elemento da interface	Descrição
Eventos e Incidentes	A lista de eventos contém os principais detalhes para cada um dos eventos. É possível exibir uma descrição mais detalhada de um evento passando o mouse sobre a linha na lista.
Recursos	Os principais detalhes para os recursos na proximidade de um evento são listados quando você clica com o botão direito do mouse no evento selecionado. É possível exibir uma descrição mais detalhada de um recurso passando o mouse sobre a linha na lista.

Inicialmente, quando o IBM Intelligent Operations Center é aberto, o portlet Detalhes mostra todos os eventos que são relevantes.

No portlet Mapa, você seleciona as categorias de eventos e as capacidades de recursos a serem mostradas. As categorias de eventos mostradas na guia **Eventos e Incidentes** e no portlet Mapa são as mesmas. As capacidades de recursos mostradas na guia **Recursos** e no portlet Mapa são as mesmas.

A lista de eventos é atualizada regularmente com novos eventos e atualizações, sujeitos aos filtros configurados para limitar as categorias mostradas.

Um contador no canto esquerdo da barra de ação no final da lista indica o número de itens exibidos e o número total de itens. No centro da barra de ação, é possível selecionar o número de itens a serem exibidos de cada vez. Se houver mais linhas do que a quantidade possível de exibir de cada vez, será possível alterar o avanço ou retrocesso de páginas, clicando nos botões no canto direito da barra de ação.

Propriedades de Evento

A tabela a seguir define as propriedades que descrevem um evento:

Tabela 87. Propriedades de Evento

Propriedade	Conteúdo
Quem	
Remetente	Origem ou ID do usuário
Nome do contato	Pessoa com quem entrar em contato para obter informações adicionais
E-mail do contato	Endereço de email da pessoa de contato
Telefone de Contato	Número do telefone da pessoa de contato
O que	
Tipo de evento*	Texto que indica o tipo de evento em <i>Categoria</i>
Status do evento*	Instruções de manipulação de eventos
Escopo do evento*	Público alvo desejado para a mensagem
Restrição	Informações adicionais necessárias quando o <i>Escopo do evento</i> é 'Restrito'
Título*	Breve descrição do evento
Categoria*	Classificação de evento de alto nível
Gravidade*	Intensidade do impacto do evento
Certeza*	Confiança na previsão do evento
Urgência*	Intervalo de tempo para ação em resposta ao evento

Tabela 87. Propriedades de Evento (continuação)

Propriedade	Conteúdo
Quem	
Tipo de mensagem	Natureza da mensagem
Descrição	Descrição adicional do evento
Endereço da Web	Endereço da Web para obter informações adicionais sobre o evento
Quando	
Data e hora de envio	Data e hora em que a mensagem foi enviada
Data e Hora Efetivas	Data e hora em que a mensagem está efetiva
Data e hora marcadas	Data e hora em que o evento está previsto para começar
Data e hora de expiração	Data e hora em que o evento está previsto para terminar
Onde	
Descrição da área	Descrição da área afetada
Latitude / Longitude	Coordenadas da localização do evento

Nota: As propriedades marcadas com um asterisco na tabela são necessárias para a criação bem-sucedida de um novo evento. As propriedades não marcadas com um asterisco são opcionais na criação de um evento.

Gerenciando Eventos e Incidentes

No portlet Detalhes, é possível executar várias ações nos eventos na lista na guia **Eventos e Incidentes**. No portlet Mapa, é possível incluir um evento que é mostrado no mapa e na lista de eventos do portlet Detalhes.

Procedimento

Na guia **Eventos e Incidentes**, clique com o botão direito do mouse em uma linha na lista de eventos e selecione uma opção no menu:

- Para atualizar as informações sobre um evento, clique em **Atualizar Evento**. É possível inserir as mudanças em uma janela com campos que contêm informações sobre o evento. Quando um registro de eventos é atualizado, a propriedade de tipo de mensagem é alterada para *Atualizar*.
- Para alterar um status do evento para o incidente, clique em **Escalar para Incidente** para exibir uma janela e insira seus detalhes de contato. Quando um registro de eventos é escalado, há uma mudança nas propriedades e no ícone no mapa.
- Para remover um evento da lista e do mapa, clique em **Cancelar Evento** para exibir uma janela e insira seus detalhes de contato.
- Para visualizar procedimento padrão de operação (SOP) e atividades do fluxo de trabalho associadas a um evento, clique em **Visualizar Detalhes do Procedimento Padrão de Operação**. Se não houver procedimentos padrão de operação associados a um evento, esta opção não estará disponível. Se houver um procedimento padrão de operação associado, a janela Detalhes de Procedimento Padrão de Operação será exibida. Use o portlet Minhas Atividades para gerenciar as atividades fluxo de trabalho associadas a um procedimento padrão de operação.
- Para visualizar uma lista de recursos na proximidade de um evento, clique em **Visualizar Recursos Próximos** e selecione o raio da área que você deseja focar. Uma lista de recursos é exibida na guia **Recursos**.
- Para visualizar as informações sobre um evento, clique em **Propriedades** para exibir uma janela que contém campos com informações sobre o evento.

Gerenciamento de recursos

É possível executar várias ações nos recursos na lista na guia **Recursos**.

Procedimento

Na guia **Recursos**, clique com o botão direito do mouse em uma linha na lista de recursos e selecione uma opção do menu:

- Para atualizar as informações sobre um recurso, clique em **Atualizar**.
- Para remover um recurso da lista e do mapa, clique em **Excluir**.
- Para visualizar as informações sobre um recurso, clique em **Propriedades**.

Independentemente da opção escolhida, o recurso será exibido no Tivoli Service Request Manager, na guia **Recursos**. Também é possível visualizar capacidades para os recursos na guia Tivoli Service Request Manager **Capacidades**. Para atualizar ou excluir um recurso, selecione o recurso e, em seguida, selecione a opção apropriada da lista **Selecionar Ação**.

Customizando o Portlet Detalhes

Administrador

Se tiver acesso de administrador, você poderá customizar este portlet. Clique no botão no canto superior direito do portlet para ver as opções de customização do menu de portlet. As configurações compartilhadas afetam o conteúdo desse portlet para todos os usuários, mas apenas para esta ocorrência do portlet.

Configure os parâmetros para o portlet Detalhes da seguinte maneira:

Ao configurar os parâmetros para o portlet Detalhes, é possível:

- Especificar o layout da coluna, títulos, ordem de classificação e prioridade.
- Especificar as condições adicionais para filtrar os eventos ou recursos exibidos.
- Mostrar ou ocultar o
 - Botão **Incluir Evento**
 - Botão **Incluir Recursos**
 - Guia **Eventos**
 - Guia **Recursos**
 - barra de ferramentas na parte superior da lista.
- Especifique o nome de um grupo para ativar a comunicação com outro mapa e portlets Detalhes.
- Configure o portlet para reconhecer ou ignorar tipos específicos de mensagem vindos de outros portlets no grupo.

É possível configurar parâmetros de portlet genéricos que são comuns nos portlets: local do arquivo de ajuda, altura do portlet, título do portlet e pacote configurável de recursos.

Referências relacionadas:

“Configurações do Portlet do Detalhes” na página 148

Customize o portlet do Detalhes alterando as configurações nos campos da janela **Configurações Compartilhadas**.

Drill Down de Key Performance Indicator

Use o portlet Drill Down de Key Performance Indicator para consultar informações adicionais sobre a categoria de KPI e o status de seus KPIs subjacentes.

O portlet Drill Down de Key Performance Indicator mostra todos os KPIs subjacentes associados a uma organização ou categoria de KPI mostrada 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 por cor, da mesma forma que a cor é usada para as categorias de KPI exibidas no portlet Status. Os valores dos KPIs subjacentes controlam a cor do KPI pai. Para exibir o status do KPI, passe o mouse sobre o KPI com o cursor.

Para focar em uma categoria de KPI específica no portlet Drill Down de Key Performance Indicator, clique na categoria no portlet Status. Esta categoria é então exibida por si própria no portlet Drill Down de Key Performance Indicator. É possível usar a lista para inspecionar os KPIs subjacentes até acessar os detalhes do KPI que causaram a mudança de status.

Administrador

Customizando o Portlet Drill Down de Key Performance Indicator

Se tiver acesso de administrador, você poderá customizar este portlet. Clique no botão no canto superior direito do portlet para ver as opções de customização do menu de portlet. As configurações compartilhadas afetam o conteúdo desse portlet para todos os usuários, mas apenas para esta ocorrência do portlet.

Ao configurar parâmetros para o portlet Drill Down de Key Performance Indicator, é possível:

- Especifique o layout da coluna, títulos, ordem de classificação e prioridade.
- Customizar cores do KPI.
- Ativar um filtro de KPI adicional.
- Mostre ou oculte a barra de ferramentas na parte superior da lista.
- Especificar um nome do grupo para permitir a comunicação com um portlet Drill Down de Key Performance Indicator.

É possível configurar parâmetros de portlet genéricos que são comuns nos portlets: local do arquivo de ajuda, altura do portlet, título do portlet e pacote configurável de recursos.

Conceitos relacionados:

“Principais Indicadores de Desempenho” na página 168

Use o portlet Principais Indicadores de Desempenho para customizar o Key Performance Indicators (KPIs) e sua exibição hierárquica no IBM Intelligent Operations Center.

Referências relacionadas:

“Configurações do Portlet do Drill Down de Key Performance Indicator” na página 152

Customize o portlet do Drill Down de Key Performance Indicator alterando as configurações nos campos da janela **Configurações Compartilhadas**.

Mapa de Localização

Utilize o portlet do Mapa de Localização para ver os eventos marcados em um mapa de localização. Um mapa de localização no IBM Intelligent Operations Center é um mapa ou plano com áreas pré-definidas para interação, por exemplo, áreas de assentos em um grande estádio esportivo.

O portlet do Mapa de Localização fornece uma representação visual dos eventos na posição que eles se encontram. O portlet do Mapa de Localização juntamente com o Mapa e os portlets do Detalhes permitem identificar problemas, padrões do local, conflitos e sinergias.

O Mapa de Localização, Mapa e os portlets do Detalhes podem estar vinculados para entradas e mudanças para os eventos exibidos. É possível selecionar no portlet do Mapa de Localização as categorias de eventos que deseja visualizar. A seleção afeta os eventos exibidos no portlet do Mapa de Localização e o Mapa, e os portlets do Detalhes vinculados a ela.

Interface do Mapa de Localização

O portlet do Mapa de Localização possui três elementos de interface interativos, conforme mostrados na tabela a seguir:

Tabela 88. Elementos da Interface com o Portlet do Mapa de Localização

Elemento da interface	Descrição
Mapa de Localização	Um diagrama do local com marcadores para eventos.
Selecionar Conteúdo: Categorias de Evento	Um formulário de filtro para selecionar as categorias do evento mostradas no mapa.
Menu do Mapa	Uma lista dos mapas de localização disponíveis organizados por classificação.

Inicialmente, a página do portal é aberta com o portlet do Mapa de Localização e todos os eventos que são relevantes são exibidos no mapa de localização. O mapa é atualizado com novos eventos, sujeito a qualquer filtro configurado para limitar as categorias mostradas. Uma barra de menu listando todos os mapas disponíveis é fornecida à esquerda do mapa.

Um evento que ocorre em uma área é representada por um marcador na posição correspondente no mapa de localização. É possível exibir um título de evento e uma descrição passando o mouse sobre o marcador de evento no mapa. A janela inclui o nome e a descrição da área em que o evento ocorre. Se mais de um evento ocorrer na mesma área, os eventos serão armazenados em cluster e representados por um marcador de cluster. Ao passar o mouse sobre este marcador, o título de cada evento está incluído na janela. É possível também exibir um nome e descrição da área passando o mouse em qualquer área predefinida no mapa que estão sem eventos.

Quando os portlets são vinculados, é possível clicar em um evento neste portlet, e os eventos correspondentes em outros portlets no grupo também são selecionados. Do mesmo modo, selecionando um evento em qualquer um dos resultados de portlets vinculados nesse evento destacado neste portlet.

Nota: Um evento deve ter um identificador de área a ser mostrado no portlet do Mapa de Localização. Além disso, um evento deve ter coordenadas de latitude e longitude a serem exibidas no Mapa de Localização e nos portlets do Mapa. Se um evento não tiver um identificador de área ou coordenadas, ele poderá ser mostrado apenas no portlet do Detalhes .

Marcadores do Mapa

O mapa representa o local de eventos com um dos seguintes tipos de marcador:

Tabela 89. Marcadores do Mapa

Tipo de Marcador	Descrição
Ícone	Identifica no mapa a posição de um evento com um ícone exclusivo para cada categoria de evento.
Cluster	Indica mais de um evento na mesma área com um número que representa o número de eventos nessa área.

O ícone que representa um tipo de evento é definido no campo de categoria dos detalhes do evento no guia **Eventos e Incidentes** no portlet do Detalhes. Quando um evento é escalado para um acidente, o ícone exibido no mapa retém seu símbolo específico da categoria, com a adição de uma margem vermelha em volta do ícone.

Controles do Mapa

É possível mover o cursor ao redor do mapa usando o mouse ou o teclado.

Os controles do mapa estão localizados no canto superior esquerdo do mapa

Os controles de mapa ficam no lado superior esquerdo do mapa. Eles são compostos de:

- Setas de panoramização (para cima, para baixo, à esquerda, à direita)
- Aumentar zoom
- Visualização Mundial (diminuir zoom para a máxima extensão)
- 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 ampliação ou redução da escala do mapa

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

Selecionando Categorias de Evento para o Mapa

Com o filtro Categorias de Evento, é possível selecionar por categoria quais eventos são exibidos no mapa.

Para visualizar o formulário de filtro, clique em **Selecionar Conteúdo**. As categorias de eventos exibidos no mapa, e em portlets associados, podem ser alterados com base na seleção do formulário de filtro aqui. É possível concentrar-se na categorias de evento que deseja analisar, utilizando o filtro para ocultar as categorias de eventos que não são necessárias. O mapa responde a qualquer mudança no formulário de filtro. Quando a seleção é alterada, o mapa é atualizado e apenas as posições dos eventos nas categorias selecionadas são representadas no mapa. Altere as categorias de evento exibidas marcando ou desmarcando as caixas de opções no formulário de filtro. Para fechar o formulário de filtro, clique em **Selecionar Conteúdo**. Se você sair da página do portal e retornar, o filtro será reconfigurado para a seleção padrão.

É possível se concentrar nos eventos individuais que deseja analisar marcando as caixas de seleção no portlet do Detalhes. Esses eventos são também destacados em portlets vinculados.

Customizando o Portlet do Mapa de Localização

Administrador

Se tiver acesso de administrador, você poderá customizar este portlet. Clique no botão no canto superior direito do portlet para ver as opções de customização do menu de portlet. As configurações compartilhadas afetam o conteúdo desse portlet para todos os usuários, mas apenas para esta ocorrência do portlet.

O Mapa e os portlets do Mapa de Localização também podem ser customizados alterando as configurações globais. As configurações globais afetam o conteúdo do portlet para todos os usuários e de todas as ocorrências do portlet. As configurações globais são substituídas pelas configurações compartilhadas.

As configurações que podem ser alteradas para o portlet do Mapa de Localização são as seguintes:

- A seleção padrão no filtro Categorias de Evento
- O nome do mapa de localização padrão a ser exibido
- A cor de destaque da área padrão, ao utilizar o cursos para passar o mouse sobre uma área.
- O nome do grupo que ativa a comunicação com outro mapa e com os portlets do Detalhes

É possível configurar parâmetros de portlet genéricos que são comuns nos portlets: local do arquivo de ajuda, altura do portlet, título do portlet e pacote configurável de recursos.

Customizando Mapas de Localização

É possível utilizar o portlet do Gerenciador de Mapa de Localização para customizar os seguintes aspectos do portlet do Mapa de Localização:

- Nome de classificação a ser exibido no menu à esquerda do portlet.
- Mapa a ser exibido no portlet.
- Áreas dentro de um mapa.

Conceitos relacionados:

“Gerenciador de Mapa de Localização” na página 176

Use o portlet Gerenciador de Mapa de Localização para customizar o portlet Mapa de Localização.

Referências relacionadas:

“Configurações do Portlet do Mapa de Localização” na página 155

Customize o portlet do Mapa de Localização alterando as configurações nos campos da janela

Configurações Compartilhadas.

Mapa

Use o portlet Mapa para ver eventos e recursos em um mapa.

O portlet Mapa fornece uma representação visual dos eventos e recursos em um mapa. Use o portlet Mapa junto com os portlets Mapa de Localização e Detalhes para identificar padrões de local, conflitos, problemas e sinergias.

Os portlets Mapa, Mapa de Localização e Detalhes podem ser vinculados para compartilhar entrada e mudanças nos eventos exibidos. É possível selecionar no portlet Mapa as categorias de eventos e as capacidades de recursos que você deseja visualizar. A seleção afeta o que é exibido no portlet Mapa e nos portlets vinculados Mapa de Localização e Detalhes.

Interface do Mapa

O portlet Mapa possui três elementos de interface interativa, conforme mostrado na tabela a seguir:

Tabela 90. Elementos da interface do portlet Mapa

Elemento da interface	Descrição
Mapa	Um mapa da região geográfica, com marcadores de eventos e de recursos.
Selecione as Categorias Conteúdo: Evento	Um formulário de filtro para selecionar as categorias dos eventos a serem mostrados no mapa e nos portlets vinculados ao portlet Mapa.
Selecionar Conteúdo: Recursos	Um formulário de filtro para selecionar as capacidades dos recursos a serem mostrados no mapa e na guia Recursos no portlet vinculado Detalhes. Para visualizar este formulário, primeiro selecione Visualizar Recursos Próximos no portlet Detalhes.

Inicialmente, a página de portal é aberta com o portlet Mapa e todos os eventos que são relevantes para você no mapa. Se um evento tiver valores de latitude e longitude especificados, é possível ver o local do evento em forma de um marcador de ícone no mapa. É possível exibir um título e descrição do evento passando o mouse sobre o marcador de evento no mapa. Se houver mais de um evento armazenado em cluster no mesmo local, o número de eventos será indicado no marcador. Quando você passa o mouse sobre esse marcador de cluster, o título de cada evento é incluído na janela. O mapa é atualizado com novos eventos, sujeitos a quaisquer filtros configurados para limitar as categorias mostradas.

Quando portlets são vinculados, é possível clicar em um marcador de evento em um portlet, e o evento correspondente nos outros portlets no grupo também são selecionados.

Há um limite para o número de marcadores que podem ser mostrados no mapa. Se o número de marcadores na área na visualização exceder o limite, os marcadores não serão mostrados. Você recebe uma mensagem com o número de marcadores disponíveis e o número do limite. São fornecidas duas opções de exibição de todos os marcadores disponíveis:

- Escolha a opção Aumentar zoom ou Panoramizar em uma área do mapa com o número de marcadores abaixo do limite.
- Clique em **Carregar todos os itens na visualização**.

Se escolher a segunda opção, talvez você veja que os marcadores aparecem no mapa em uma taxa mais lenta. Há uma terceira opção: use o filtro para selecionar menos categorias.

Ao selecionar **Visualizar Recursos Próximos** para um evento no portlet Detalhes, os recursos serão mostrados no mapa com base no raio e nos recursos selecionados.

O mapa o mantém atualizado quando novos eventos são incluídos nele, sujeitos a quaisquer filtros que você tenha configurado para limitar as categorias mostradas.

Nota: Se um evento tiver um identificador de área além das coordenadas de latitude e longitude, ele será mostrado nos portlets Mapa de Localização e Mapa. Todos os eventos podem ser mostrados no portlet Detalhes.

Marcadores do Mapa

O mapa representa o local de eventos ou recursos com um dos seguintes tipos de marcador:

Tabela 91. Marcadores do Mapa

Tipo de Marcador	Descrição
Ícone	indica no mapa a localização de um evento ou um recurso no mapa com um ícone exclusivo para cada tipo de categoria ou recurso

Tabela 91. Marcadores do Mapa (continuação)

Tipo de Marcador	Descrição
Polígono	descreve no mapa a área associada a um evento específico
Cluster	indica mais de um evento no mesmo local
Radius	descreve no mapa a área selecionada para Visualizar Recursos Próximos em relação a um evento

O ícone que representa um tipo de evento é definido no campo de categoria dos detalhes do evento na guia **Eventos e Incidentes** no portlet Detalhes. Quando um evento é escalado para um incidente, o ícone exibido no mapa retém seu símbolo específico de categoria com a adição de uma margem vermelha. Clicar em um marcador de evento no mapa realçará o(s) evento(s) associado(s) no portlet Detalhes.

O ícone que representa um recurso é definido no campo de tipo dos detalhes do recurso na guia **Recursos** no portlet Detalhes. Para visualizar ícones do recurso, primeiro selecione **Visualizar Recursos Próximos** no portlet Detalhes.

Usando os Controles de Mapa

É possível mover o cursor ao redor do mapa usando o mouse ou o teclado.

Os controles do mapa estão localizados no canto superior esquerdo do mapa

Os controles de mapa ficam no lado superior esquerdo do mapa. Eles são compostos de:

- Setas de panoramização (para cima, para baixo, à esquerda, à direita)
- Aumentar zoom
- Visualização Mundial (diminuir zoom para a máxima extensão)
- 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 ampliação ou redução da escala do mapa

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

Selecionando as Categorias de Evento do Mapa

Use o filtro Categorias de Evento para selecionar por categoria quais eventos serão exibidos no mapa.

Para visualizar o formato de filtro, clique em **Selecionar Conteúdo**. As categorias de eventos exibidos no portlet do mapa podem ser alteradas com base na seleção de formulário de filtro feita. É possível manter o foco nas categorias de evento que você deseja analisar, usando o filtro para ocultar as categorias de evento que não são necessárias. O mapa responde a qualquer mudança no formulário de filtro. Uma mudança no formulário de filtro também afeta outros portlets no mesmo grupo. Quando uma seleção é alterada, o mapa é atualizado e apenas os locais de eventos nas categorias selecionadas são demarcados no mapa. Altere a categoria de evento exibida marcando ou desmarcando as caixas de seleção no formulário de filtro. Para fechar o formato de filtro, clique em **Selecionar Conteúdo**. Se você sair da página de portal e retornar, o filtro será reconfigurado para o padrão que é 'todas as categorias selecionadas'.

É possível se concentrar nos eventos individuais que deseja analisar marcando as caixas de seleção no portlet Detalhes. Essas ocorrências são destacadas no mapa.

Selecionando as Capacidades de Recurso do Mapa

Ao selecionar **Visualizar Recursos Próximos** no portlet Detalhes, o filtro Categorias de Evento é substituído pelo filtro Recursos. Use o filtro Recursos para selecionar por capacidade quais recursos serão exibidos no mapa.

Para visualizar o formato de filtro, clique em **Selecionar Conteúdo**. As capacidades de recursos exibidas no mapa e no portlet Detalhes podem ser alteradas com base na seleção de formulário de filtro que é feita. É possível manter o foco na capacidade que você deseja analisar, usando o filtro para ocultar as capacidades que não são necessárias. O mapa responde a qualquer mudança no formulário de filtro. Uma mudança no formulário de filtro também afeta o portlet Detalhes no mesmo grupo. Quando uma seleção é alterada, o mapa é atualizado e apenas os locais dos recursos com capacidades selecionadas são demarcados no mapa. Altere a capacidade de recursos exibida marcando ou desmarcando uma caixa de seleção no formulário de filtro. Para fechar o formato de filtro, clique em **Selecionar Conteúdo**. Se você sair da página de portal e retornar ao formulário de filtro de recursos, o filtro será reconfigurado para o padrão, que é todas as capacidades selecionadas. As capacidades selecionadas por padrão dependem da categoria do evento e de como essa categoria é mapeada para as capacidades.

Reconfigurando o mapa

O portlet Mapa pode ser reconfigurado para a visualização padrão configurada para o IBM Intelligent Operations Center.

Procedimento

1. No portlet Mapa, clique em **Reconfigurar o Mapa** ou clique na seta no canto superior direito.
2. Selecione uma das seguintes opções:
 - **Reconfigurar o Mapa** para aplicar zoom e centralizar o mapa na configuração padrão.
 - **Reconfigurar o Mapa e Limpar Filtros** para aplicar zoom e centralizar o mapa na configuração padrão e reconfigurar os valores definidos em **Selecionar Conteúdo** para os valores padrão.

Resultados

O mapa é reconfigurado de acordo com a opção selecionada, mas apenas para o usuário e a visualização atuais.

Incluindo um Evento

É possível criar um evento, incluindo-o no mapa do portlet Mapa e na lista de portlets Detalhes 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:

Tabela 92. Propriedades de Evento

Propriedade	Conteúdo
Quem	
Remetente	Origem ou ID do usuário
Nome do contato	Pessoa com quem entrar em contato para obter informações adicionais
E-mail do contato	Endereço de email da pessoa de contato
Telefone de Contato	Número do telefone da pessoa de contato
O que	
Tipo de evento*	Texto que indica o tipo de evento em <i>Categoria</i>
Status do evento*	Instruções de manipulação de eventos
Escopo do evento*	Público alvo desejado para a mensagem
Restrição	Informações adicionais necessárias quando o <i>Escopo do evento</i> 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
Quando	
Data e hora de envio	Data e hora em que a mensagem foi enviada
Data e Hora Efetivas	Data e hora em que a mensagem está efetiva
Data e hora marcadas	Data e hora em que o evento está previsto para começar
Data e hora de expiração	Data e hora em que o evento está previsto para terminar
Onde	
Descrição da área	Descrição da área afetada
Latitude / Longitude	Coordenadas da localização do evento

Procedimento

1. Clique com o botão direito do mouse em um local no mapa e clique em **Incluir Evento** para ativar o diálogo **Incluir Evento**. Algumas propriedades da ocorrência são preenchidas automaticamente.
2. Especifique as propriedades de evento restantes nos campos no diálogo. Propriedades marcadas com um asterisco são obrigatórias para a criação bem-sucedida de um novo evento. As propriedades não marcadas com 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 no local solicitado no mapa. É possível ver os detalhes do novo evento na lista de portlets Detalhes vinculada.

Customizando o Portlet Mapa

Administrador

Se tiver acesso de administrador, você poderá customizar este portlet. Clique no botão no canto superior direito do portlet para ver as opções de customização do menu de portlet. As configurações compartilhadas afetam o conteúdo desse portlet para todos os usuários, mas apenas para esta ocorrência do portlet.

O Mapa e os portlets do Mapa de Localização também podem ser customizados alterando as configurações globais. As configurações globais afetam o conteúdo do portlet para todos os usuários e de todas as ocorrências do portlet. As configurações globais são substituídas pelas configurações compartilhadas.

É possível alterar as seguintes configurações específicas no portlet Mapa:

- Reconfigure o ponto central padrão e o nível de zoom do mapa.
- Selecionar um novo mapa de base, o padrão é um mapa ArcGIS fornecido pelo Esri.
- Incluir no mapa a anotação geográfica e camadas de visualização em KML (Keyhole Markup Language), para representar dados adicionais.
- Configure um limite para o número de marcadores que podem ser exibidos sem uma mensagem de aviso.
- Configure a seleção padrão nos filtros do mapa, a ser exibida quando você clica em **Selecionar Conteúdo**.
- Especifique o nome do grupo que ativa a comunicação com outro mapa e portlets Detalhes

É possível configurar parâmetros de portlet genéricos que são comuns nos portlets: local do arquivo de ajuda, altura do portlet, título do portlet e pacote configurável de recursos.

Referências relacionadas:

“Configurações do Portlet do Mapa” na página 157

Customize o portlet do Mapa alterando as configurações nos campos da janela **Configurações Compartilhadas**.

Minhas Atividades

O portlet Minhas Atividades exibe uma lista dinâmica de atividades pertencentes ao grupo do qual o usuário que está conectado à interface é membro.

Cada vez que um evento aciona um procedimento padrão de operação, de acordo com os critérios de seleção definidos no matriz de seleção de procedimento padrão de operação, as atividades associadas são designadas a proprietários. Para obter mais informações sobre procedimentos padrão de operação, consulte o link no final do tópico.

Um usuário que está conectado pode visualizar as atividades designadas a ele no portlet Minhas Atividades. No portlet Minhas Atividades, as atividades são agrupadas pelos procedimentos padrão de operação pai. Cada procedimento padrão de operação corresponde a um evento individual.

Para cada procedimento padrão de operação, o portlet Minhas Atividades exibe apenas atividades abertas e não atividades fechadas ou concluídas. As atividades abertas incluem as atividades que já estão iniciadas e as atividades que são elegíveis para serem iniciadas. Por exemplo, se uma ou mais das atividades especificadas em um procedimento padrão de operação forem ordenadas em uma sequência,

somente a atividade atual na sequência será exibida. Se uma determinada atividade depender da conclusão de uma atividade predecessora, ela não será exibida até que a atividade predecessora seja concluída ou ignorada.

Os seguintes ícones de atividade atrasada são exibidos próximos à parte superior do portlet Minhas Atividades:

Vencido

Atividades cuja conclusão está vencida.

Hoje Atividades que estão atrasadas para serem concluídas hoje.

Futuro

Atividades cuja conclusão vence no futuro.

Quando uma atividade é iniciada, a data de vencimento é calculada incluindo o horário de início na duração da atividade. As datas de vencimento das atividades são usadas para calcular o número exibido em cada um dos ícones de atividades vencidas.

No portlet Minhas Atividades, os procedimentos padrão de operação que tiverem atividades vencidas serão exibidos primeiro e os demais procedimentos padrão de operação serão exibidos em ordem alfabética.

Próximo de cada procedimento padrão de operação na lista contendo atividades vencidas, um ícone vermelho indica o número de atividades vencidas. Os procedimentos padrão de operação com atividades vencidas são classificados de acordo com o número de atividades vencidas que eles contêm. O procedimento padrão de operação com a maioria das atividades vencidas é exibido na parte superior da lista.

Gerenciando Atividades no Portlet Minhas Atividades

Gerencie suas atividades no portlet Minhas Atividades:

- Para visualizar detalhes sobre um procedimento padrão de operação, expanda o nome do procedimento padrão de operação.
 - O nome do evento que acionou o procedimento padrão de operação é exibido. Passe o mouse sobre o nome do evento para visualizar informações da ajuda instantânea que incluem a data e hora de início e a categoria, severidade, certeza e urgência do evento.
 - Se o portlet Detalhes for exibido na página, para visualizar as propriedades do evento, clique no nome do evento. A janela Propriedades do evento é exibida.
 - Etapas que estão em andamento ou elegíveis para serem iniciadas são exibidas. Além disso, são exibidos o status e a data de vencimento de cada etapa.
- Para visualizar detalhes adicionais sobre uma etapa, incluindo comentários e referências que os usuários incluíram na etapa, expanda o nome dessa etapa.
- Para iniciar, concluir ou ignorar uma etapa, expanda o nome da etapa e, em seguida, escolha uma das seguintes opções:
 - Para iniciar uma etapa, na lista, selecione **Iniciar**. Se a etapa for definida como uma tarefa automatizada no procedimento padrão de operação, o fluxo de trabalho designado à tarefa será iniciado automaticamente e a etapa será concluída automaticamente. O usuário que inicia uma etapa se torna o proprietário dessa etapa e o nome do usuário é exibido no campo **Proprietário**.
 - Para ignorar uma etapa, na lista, selecione **Ignorar**.
 - Para concluir uma etapa, na lista, selecione **Concluir**.
- Para incluir um comentário em uma etapa, use as subetapas a seguir:
 1. Expanda o nome da etapa.
 2. Na lista, selecione **Incluir Comentário**.

3. Na janela Incluir Comentário, insira um comentário no campo **Comentário**. **Nome do Comentarista** e **Nome da Atividade** são campos somente leitura e contêm valores inseridos automaticamente.
 4. Clique em **OK**.
 5. Expanda o nome da etapa novamente. O novo comentário é exibido no final da lista de comentários e referências existentes para a etapa.
- Para incluir uma referência em uma etapa, use as subetapas a seguir:
 1. Expanda o nome da etapa.
 2. Na lista, selecione **Incluir Referência**.
 3. Na janela Incluir Referência, insira valores para **Nome da Referência** e **URI da Referência**. **Nome da Atividade** é um campo somente leitura que contém um valor inserido automaticamente.
 4. Clique em **OK**.
 5. Expanda o nome da etapa novamente. A nova referência é exibida como um link no final da lista de comentários e referências existentes para a etapa.
 - Para visualizar os detalhes de um procedimento padrão de operação, clique no ícone **i** próximo ao nome do procedimento padrão de operação. Na janela Detalhes do Procedimento Padrão de Operação, todas as etapas da atividade incluídas no procedimento padrão de operação serão exibidas, incluindo as etapas em andamento, elegíveis para serem iniciadas, concluídas e fechadas. O status e a data de vencimento de cada etapa também são exibidos. Para visualizar detalhes adicionais sobre uma etapa, expanda o nome da etapa.

Administrador

Customizando o Portlet Minhas Atividades

Se tiver acesso de administrador, você poderá customizar este portlet. Clique no botão no canto superior direito do portlet para ver as opções de customização do menu de portlet. As configurações compartilhadas afetam o conteúdo desse portlet para todos os usuários, mas apenas para esta ocorrência do portlet.

Para o portlet Minhas Atividades, é possível especificar um nome de grupo para ativar a comunicação com outros portlets; por exemplo, portlets Detalhes.

É possível configurar parâmetros de portlet genéricos que são comuns nos portlets: local do arquivo de ajuda, altura do portlet, título do portlet e pacote configurável de recursos.

Conceitos relacionados:

“Procedimentos Padrão de Operação” na página 127

É possível definir o procedimentos padrão de operação e atividades para gerenciar eventos que chegam ao IBM Intelligent Operations Center. Use o portlet Procedimentos Padrão de Operação para acessar os aplicativos procedimento padrão de operação, matriz de seleção de procedimento padrão de operação e designer de fluxo de trabalho no Tivoli Service Request Manager.

Referências relacionadas:

“Configurações do Portlet do Minhas Atividades” na página 159

Customize o portlet do Minhas Atividades alterando as configurações nos campos da janela **Configurações Compartilhadas**.

Notificações

Use o portlet Notificações para visualizar as mensagens de alerta e os seus detalhes.

O portlet Notificações é uma janela interativa que contém uma lista de todos os alertas atuais relevantes para você. Você verá somente os alertas enviados aos grupos de usuários dos quais você é membro. 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 principal indicador de desempenho (KPI) predefinido ocorre, onde essa mudança é definida como um acionador de alerta por seu administrador

Também é possível usar o portlet para exibir detalhes adicionais de um alerta.

Lista de Notificações

O portlet Notificações 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 ver todas as informações associadas a esse alerta em uma janela, clique com o botão direito na linha e selecione **Propriedades**.

Inicialmente, ao abrir a página do portal, o portlet 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 para cancelá-la voltar à lista.

Um contador no canto esquerdo da barra de ação no final da lista indica o número de itens exibidos e o número total de itens. No centro da barra de ação, é possível selecionar o número de itens a serem exibidos de cada vez. Se houver mais linhas do que a quantidade possível de exibir de cada vez, será possível alterar o avanço ou retrocesso de páginas, clicando nos botões no canto direito da barra de ação.

Propriedades do Alerta

A janela dos detalhes do alerta exibe as seguintes propriedades:

Tabela 93. 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 evento, se o alerta for causado por eventos correlacionados
Refere-se a KPIs	Nome do KPI, se o alerta for causado por um valor de KPI em mudança

Administrador

Customizando o Portlet Notificações

Se tiver acesso de administrador, você poderá customizar este portlet. Clique no botão no canto superior direito do portlet para ver as opções de customização do menu de portlet. As configurações compartilhadas afetam o conteúdo desse portlet para todos os usuários, mas apenas para esta ocorrência do portlet.

Ao configurar parâmetros para o portlet Notificações, é possível:

- Especifique o layout da coluna, títulos, ordem de classificação e prioridade.

- Mostre ou oculte a barra de ferramentas na parte superior da lista.

É possível configurar parâmetros de portlet genéricos que são comuns nos portlets: local do arquivo de ajuda, altura do portlet, título do portlet e pacote configurável de recursos.

Referências relacionadas:

“Configurações do Portlet do Notificações” na página 160

Customize o portlet do Notificações alterando as configurações nos campos da janela **Configurações Compartilhadas**.

Relatórios

Use o portlet Relatórios para visualizar um relatório de eventos como um gráfico. O portlet fornece opções para agrupar eventos e é possível escolher eventos por uma data ou intervalo de data específico. Estes relatórios ajudam a planejar respostas a eventos atuais e futuros.

Criando Relatórios

É possível criar um relatório customizado para eventos usando o portlet Relatórios. Comece selecionando como deseja agrupar eventos. Por exemplo, para visualizar todos os eventos por uma categoria específica, selecione **Categoria** no campo **Agrupar por**. Em seguida, nos campos **Selecionar Dados**, escolha os dados específicos das informações que deseja visualizar. Também é possível indicar uma data ou intervalo de datas para os eventos no relatório. Clique em **Atualizar** e o gráfico muda para refletir as informações solicitadas.

Para recuperar a URL para o novo relatório, clique em **URL para Este Relatório**.

A Tabela 1 mostra as opções por meio das quais é possível agrupar eventos.

Tabela 94. Relatório customizado

Agrupar por	Descrição
Tipo de Ocorrência	Exibe eventos com base no tipo. Por exemplo, o evento pode ser um tornado se aproximando ou um acidente de trânsito.
Gravidade	Exibe eventos com base na severidade. Por exemplo, os eventos podem ser extremos ou graves.
Certeza	Exibe eventos com base na probabilidade de eles ocorrerem. Por exemplo, se ocorreu um acidente de trânsito, a certeza pode ser "observada."
Urgência	Exibe eventos com base em sua urgência. Por exemplo, o evento pode estar ocorrendo e pode ser descrito como "imediato".
Categoria da Ocorrência	Exibe eventos com base na categoria de evento. Por exemplo, é possível visualizar todos os eventos ambientais, de incêndio ou de transporte.
Tipo de Mensagem	Exibe eventos com base nos tipos de mensagem, como atualizações e alertas.
Status	Exibe eventos por status. Os status são: <ul style="list-style-type: none"> • Aceitável • Cuidado • Execute uma ação
Remetente	Exibe eventos por um determinado emissor. Por exemplo, o evento pode ser um problema de segurança ou um problema que afeta o IBM Intelligent Operations for Water.

Tabela 94. Relatório customizado (continuação)

Agrupar por	Descrição
Incidente	Exibe eventos com base no tipo de incidente. Por exemplo, é possível exibir todos os acidentes de trânsito ou todas as construções de estradas.
Código de Manipulação	Exibe eventos por código de manipulação. Por exemplo, o código de manipulação pode ser "evento."
Nome do Remetente	Exibe eventos por nome do emissor.

A Tabela 2 mostra os dados que podem ser selecionados para o relatório.

Tabela 95. Selecione dados

Selecionar Dados	Descrição
Gravidade	Exibe eventos com base na severidade. Por exemplo, os eventos podem ser extremos ou graves.
Certeza	Exibe eventos com base na probabilidade de eles ocorrerem. Por exemplo, se ocorreu um acidente de trânsito, a certeza pode ser "observada."
Urgência	Exibe eventos com base em sua urgência. Por exemplo, o evento pode estar ocorrendo e pode ser descrito como "imediatos".
Categoria da Ocorrência	Exibe eventos com base na categoria de evento. Por exemplo, é possível visualizar todos os eventos ambientais, de incêndio ou de transporte.
Tipo de Ocorrência	Exibe eventos com base no tipo. Por exemplo, o evento pode ser um tornado se aproximando ou um acidente de trânsito.
Data Inicial	Insira a data para a qual você está visualizando eventos. Para um intervalo de datas, insira a data de início.
À data	Insira a data através da qual você está visualizando eventos.

Nota: Para que este portlet funcione conforme o esperado, você deve efetuar logon no portal de soluções usando o nome completo do domínio do servidor de aplicativos do IBM Intelligent Operations Center. Se você efetuar logon no portal usando o endereço IP ou um alias do nome do host em vez do nome completo do domínio registrado, este portlet não será exibido corretamente.

Copiando a URL de um Relatório

Para copiar a URL de um relatório e fazer o relatório ser exibido em um quadro ao lado desse portlet, clique com o botão direito do mouse na URL e selecione **Copiar Endereço de Link**. O texto para a opção **Copiar Endereço de Link** varia, dependendo do navegador.

Importante:

Para salvar um relatório definido pelo usuário e usar o link que você copiou aqui, insira a data de ontem no campo **De Data** e a data de amanhã no campo **Para Data**. Essas datas garantem que você obtém todos os dados que deseja incluídos no relatório definido pelo usuário. Por exemplo, para o intervalo de data 10/8/2012 até 18/8/2012, insira as seguintes datas para os critérios de filtro:

- De Data - insira 9/8/2012
- Para Data - insira 19/8/2012

Amostras de Relatório

O IBM Intelligent Operations Center possui um portlet Relatórios que contém relatórios gráficos baseados nos dados do portlet Eventos.

O quadro de relatório grande é onde você seleciona os parâmetros para as informações que aparecem no gráfico de relatório.

Os dois quadros no lado direito do portlet são onde os relatórios definidos pelo usuário são copiados.

Os relatórios na parte inferior da página são gráficos predefinidos. Para configurar estes relatórios para mostrar eventos por uma data ou intervalo de data, clique em **Configurar o Relatório**. Insira as datas e clique em **Visualizar o Relatório**.

Integrando seus Relatórios

O portlet Relatórios fornece um IFrame para integrar relatórios ou páginas do IBM Cognos Business Intelligence. Você especifica a URL para o relatório ou página que deseja integrar ao portlet.

Administrador

Customizando o Portlet Relatórios

Se tiver acesso de administrador, você poderá customizar este portlet. Clique no botão no canto superior direito do portlet para ver as opções de customização do menu de portlet. As configurações compartilhadas afetam o conteúdo desse portlet para todos os usuários, mas apenas para esta ocorrência do portlet.

É possível configurar parâmetros de portlet genéricos que são comuns nos portlets: local do arquivo de ajuda, altura do portlet, largura do portlet e título do portlet. Também é possível especificar a URL do relatório a ser exibido.

Referências relacionadas:

“Configurações do Portlet do Relatórios” na página 162

Customize o portlet do Relatórios alterando as configurações nos campos da janela **Configurações Compartilhadas**.

Status

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

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.

Código de Cor do KPI

Cada coluna contém informações de KPI sobre uma organização nomeada na parte superior da coluna. As categorias de KPI associadas a cada organização são representadas por células coloridas. A cor do plano de fundo de uma categoria de KPI reflete seu status. Se houver mais de seis KPIs para serem exibidos em uma coluna, o tamanho de cada célula individual será reduzido para acomodar os KPIs extras.

O código de cor do plano de fundo fornecido com os KPIs de amostra da solução é o seguinte:

- Verde indica que o status é aceitável com base nos parâmetros desse KPI.
- Amarelo indica que é necessário cuidado ou monitoramento.

- Vermelho indica que a ação é recomendada.
- Cinza indica que existem dados insuficientes disponíveis para calcular o status do KPI.

O código de cor é definido na legenda na parte superior do portlet.

Um status indeterminado indica que não há nenhum valor de KPI disponível no período definido para esse KPI. Essa situação ocorre quando a solução não recebe nenhuma mensagem para o KPI no período 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.

Para ver o nome do KPI e uma definição do status representado pela cor de um KPI, passe o mouse sobre a célula com o cursor.

Atualizações 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 Notificações indica que um KPI foi alterado.

Quando a solução recebe uma mensagem relacionada ao cálculo de um KPI, ocorre uma mudança instantânea de cor. Esse recurso é uma vantagem quando a categoria de KPI é aquela com probabilidade de receber mudanças em tempo real, por exemplo, atrasos em aeroportos. Isso não é relevante para as categorias que contêm KPIs históricos, por exemplo, controle de enchente. Para essas categorias de KPI, medidas diárias regulares são tomadas e é improvável que nesse meio tempo ocorra uma mudança repentina que afete o status.

Para cada KPI, é possível ver todos os detalhes e KPIs subjacentes no portlet Drill Down de Key Performance Indicator vinculado ao portlet Status.

Para focalizar apenas um KPI específico no portlet Drill Down de Key Performance Indicator, clique na célula de KPI na tabela no portlet Status. Também é possível clicar no título da organização proprietária; por exemplo, "Water", para ver todos os KPIs relacionados.

Administrador

Customizando o Portlet Status

Se tiver acesso de administrador, você poderá customizar este portlet. Clique no botão no canto superior direito do portlet para ver as opções de customização do menu de portlet. As configurações compartilhadas afetam o conteúdo desse portlet para todos os usuários, mas apenas para esta ocorrência do portlet.

Ao configurar parâmetros para o portlet Status, é possível:

- Customizar cores do KPI.
- Ativar um filtro de KPI adicional.
- Mostrar ou ocultar a legenda do KPI.
- Definir como os KPIs são classificados.
- Especificar um nome do grupo para permitir a comunicação com um portlet Drill Down de Key Performance Indicator.

É possível configurar parâmetros de portlet genéricos que são comuns nos portlets: local do arquivo de ajuda, altura do portlet, título do portlet e pacote configurável de recursos.

Customizando KPIs

Um conjunto de KPIs de amostra é fornecido com a solução. 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.

Conceitos relacionados:

“Principais Indicadores de Desempenho” na página 168

Use o portlet Principais Indicadores de Desempenho para customizar o Key Performance Indicators (KPIs) e sua exibição hierárquica no IBM Intelligent Operations Center.

Referências relacionadas:

“Configurações do Portlet do Status” na página 164

Customize o portlet do Status alterando as configurações nos campos da janela **Configurações Compartilhadas**.

Capítulo 9. 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.

Técnicas para Resolução de Problemas

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 Relacionados

“Procurando Bases de Conhecimento” na página 322

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.

Ativando Rastreios e Visualizando Arquivos de Log

Para resolver um problema no IBM Intelligent Operations Center, pode ser necessário analisar os arquivos de log em vários sistemas. Os tópicos a seguir fornecem algumas orientações sobre como acessar os arquivos de log.

Para iniciar os rastreios e visualizar os logs, insira os comandos no tempo de execução como usuário raiz.

Conceitos relacionados:

“Verificando os Componentes” na página 210

A ferramenta Verificação do Sistema testa componentes dentro do IBM Intelligent Operations Center para determinar se eles estão acessíveis e operacionais.

“Instalando e Usando IBM Support Assistant Lite” na página 303

O IBM Support Assistant Lite (ISA Lite) é uma ferramenta que coleta dados diagnósticos comuns úteis para analisar problemas gerais.

Tarefas relacionadas:

“Executando a Ferramenta de Instalação Coleta de Informações” na página 299

Os arquivos de log são gerados enquanto o IBM Intelligent Operations Center é instalado. Uma ferramenta está disponível para reunir esses arquivos de log para análise.

Arquivos de Log do Servidor de aplicativos

Utilize os procedimentos a seguir para ativar os rastreios e visualizar logs para alguns dos sistemas no servidor de aplicativos.

Os procedimentos a seguir descrevem como ativar rastreios e visualizar logs para os seguintes sistemas:

- WebSphere Portal
- IBM WebSphere Business Monitor

Ativando Rastreo e Visualizar Logs no WebSphere Portal Sobre Esta Tarefa

Os logs do WebSphere Portal estão em `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal`. Siga as etapas no procedimento para iniciar um rastreo e visualizar um log.

Procedimento

1. Efetue logon no console administrativo em `http://app-host:9060/ibm/console`, onde **app-host** é o nome completo do host do servidor de aplicativos.
2. Clique em **Resolução de Problemas > Logs e Rastreo**.
3. Clique em **WebSphere_Portal > Alterar detalhes do nível de log**.
4. Clique na guia **Tempo de Execução** e cole no seguinte comando:

```
*=warning: com.ibm.iss.*=all: com.ibm.ioc.*=all
```
5. Clique em **OK**.
6. Para visualizar um log, insira os seguintes comandos:

```
cd /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal
tail -f trace.log
```

Ativando o Rastreo e Visualizando Logs para IBM WebSphere Business Monitor no servidor de aplicativos

Sobre Esta Tarefa

Os logs para IBM WebSphere Business Monitor no servidor de aplicativos estão localizados em /opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/logs/WBM_DE.AppTarget.WBMNode1.0/. Siga as etapas no procedimento para iniciar um rastreo e visualizar um log.

Procedimento

1. Efetue logon no console administrativo em `http://app-host:9060/ibm/console`, onde **app-host** é o nome completo do host do servidor de aplicativos.
2. Clique em **Resolução de Problemas > Logs e Rastreo**.
3. Clique em **WBM_DE.AppTarget.WBMNode1.0 > Alterar detalhes do nível de log**.
4. Clique na guia **Tempo de Execução** e cole o seguinte código de nível de rastreo: `*=info: com.ibm.wbm.*=finest: com.ibm.events.*=all: com.ibm.wbimonitor.xsp.cei.*=all: com.ibm.wbimonitor.xsp.eventselector.*=all`
5. Clique em **OK**.

Informações relacionadas:



Documentação do Produto IBM WebSphere Portal 7

Arquivos de Log do Servidor de eventos

Utilize os procedimentos a seguir para ativar os rastreios e visualizar logs para alguns dos sistemas no .

Os procedimentos a seguir descrevem como ativar rastreios e visualizar logs para os seguintes sistemas:

- Tivoli Service Request Manager
- WebSphere MQ e WebSphere Message Broker
- Análise de XML do Tivoli Netcool/OMNIBus
- Banco de dados do Tivoli Netcool/OMNIBus (servidor de objeto)
- Banco de dados do Tivoli Netcool/OMNIBus (Agente do Processo)
- Tivoli Netcool/Impact

Ativando Rastreo e Visualizando Arquivos de Log para Tivoli Service Request Manager

Sobre Esta Tarefa

Utilize o seguinte procedimento para depurar o fluxo de informações do Tivoli Service Request Manager para o IBM Intelligent Operations Center.

Procedimento

1. Na interface com o usuário do Tivoli Service Request Manager, clique em **Acessar > Configuração do Sistema > Configuração da Plataforma > Criação de Log**.
2. Em Criadores de Log de Raiz, no campo de filtro, insira **integração**.
3. Expanda **integração**.
4. Configure o criador de logs de integração:
 - a. Para obter o **Nível de Log**, clique no ícone **Selecionar Valor**. Na janela Selecionar Valor, clique em **DEPURAR**.
 - b. Para obter **Anexadores**, clique no ícone **Gerenciar Anexadores**. Na janela Gerenciar Anexadores, marque a caixa de seleção **Dailyrolling** e em seguida clique em **OK**.
 - c. Marque a caixa de seleção **Ativo?**.

- d. Clique no ícone **Salvar Criador de Logs**.
5. A partir da lista **Selecionar Ação** selecione **Configurar Pasta Raiz da Criação de Logs**.
6. Na janela Configurar Pasta Raiz de Criação de Log, para **Pasta de Criação de Log Raiz**, insira `/opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/logs/MXServer1` e clique em **OK**.
7. Clique no ícone **Salvar Criador de Logs**.
8. A partir da lista **Selecionar Ação** selecione **Aplicar Configurações**.
9. Para visualizar o log, em um terminal do servidor do Tivoli Service Request Manager, insira os seguintes comandos:

```
cd /opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/logs/MXServer1/maximo/logs
tail -f event-host_MXServer_maximo_scheduled.log
```

em que *event-host* é o nome do host do .

Tarefas relacionadas:

“Verificando os Arquivos de Log” na página 339

Verifique o arquivo de log de política do Tivoli Netcool/OMNIbus e o arquivo de log do Tivoli Service Request Manager.

Ativando Rastreo e Visualizando Arquivos de Log para WebSphere MQ e WebSphere Message Broker

Sobre Esta Tarefa

Os logs para o WebSphere MQ e WebSphere Message Broker são armazenados nos seguintes locais:

- `/var/mqm/errors`
- `/var/mqm/qmgrs/IOC!MB!QM/errors`

Os arquivos de rastreo são gravados para o diretório `/var/mqm/trace`. É possível ativar o rastreo para um único gerenciador de fila ou para todos os gerenciadores de fila, conforme mostrado no procedimento a seguir.

Procedimento

1. Para iniciar, terminar ou formatar um rastreo, escolha o comando apropriado:
 - Para iniciar um rastreo para todos os processos, insira o seguinte comando: `strmqtrc -e`
 - Para iniciar um rastreo para o gerenciador de fila do IBM Intelligent Operations Center, insira o seguinte comando: `-m strmqtrc IOC.MB.QM`
 - Para iniciar um rastreo elevado de detalhes para o gerenciador de fila do IBM Intelligent Operations Center, insira o seguinte comando: `strmqtrc -t all -t detail -m IOC.MB.QM`
 - Para terminar todo o rastreo, insira o seguinte comando: `endmqtrc -a`
 - Para formatar os arquivos de rastreo binários no formato ASCII, insira o seguinte comando: `dspmqrtrc *.TRC`
2. Para verificar o status do WebSphere Message Broker:
 - a. Insira o seguinte comando: `ps -ef | grep IOC_BROKER`
 - b. Verifique o status dos seguintes processos:
 - `bipservice IOC_BROKER`
 - `bipbroker IOC_BROKER`
 - `biphttplistener IOC_BROKER`
 - `DataFlowEngine IOC_BROKER 5fe69373-2f01-0000-0080-9ab9c3579b15` padrão

Ativando Rastreo e Visualizando Arquivos de Log para Análise de XML do Tivoli Netcool/OMNIBus

Sobre Esta Tarefa

Os logs do WebSphere Portal estão localizados em `/opt/IBM/netcool/omnibus/log/ioc_xml.log`. Siga as etapas no procedimento para iniciar um rastreo e visualizar um log.

Procedimento

1. Abra um terminal no .
2. Insira o seguinte comando: `tail -f /opt/IBM/netcool/omnibus/log/ioc_xml.log`
3. Se a mensagem Status da Conexão OK não for exibida na parte inferior do arquivo, para renomear o arquivo de log atual, insira o seguinte comando: `mv /opt/IBM/netcool/omnibus/log/ioc_xml.log /opt/IBM/netcool/omnibus/log/old_ioc_xml.log`
4. Se a mensagem Status da Conexão OK não for exibida, talvez você veja a mensagem Encerrando Análise. Para reiniciar a análise, insira o seguinte comando:
`/opt/IBM/netcool/omnibus/probes/nco_p_xml -name ioc_xml -propsfile /opt/IBM/netcool/omnibus/probes/linux2x86/ioc_xml.props &`
5. Depois de aproximadamente 1 minuto, insira o seguinte comando novamente: `tail -f /opt/IBM/netcool/omnibus/log/ioc_xml.log`
6. Se a mensagem Status da Conexão OK ainda não for exibida, verifique o arquivo `/opt/IBM/netcool/omnibus/log/ioc_xml.log` em busca de erros. Um problema de conexão pode significar que o servidor de objetos está desativado. Consulte a seção a seguir, *Ativando o Rastreo e Visualizando Logs para o Banco de Dados do Tivoli Netcool/OMNIBus (servidor de objeto)*.

Ativando Rastreo e Visualizando Arquivos de Log para o Banco de Dados do Tivoli Netcool/OMNIBus (Servidor de Objeto)

Sobre Esta Tarefa

Os arquivos de log encontram-se nos seguintes locais:

- `/opt/IBM/netcool/omnibus/log/ioc_xml.log`
- `/opt/IBM/netcool/omnibus/log/NCOMS*.*`, por exemplo:
 - `/opt/IBM/netcool/omnibus/log/NCOMS.log`
 - `/opt/IBM/netcool/omnibus/log/NCOMS_trigger_stats.log1`
 - `/opt/IBM/netcool/omnibus/log/NCOMS_profiler_report.log1`

Siga as etapas no procedimento para iniciar um rastreo e visualizar um log.

Procedimento

1. Efetue logon em um terminal como usuário raiz.
2. Insira o seguinte comando: `/opt/IBM/netcool/omnibus/bin/nco_config &`
3. Se foi perguntado se você deseja importar a partir do `omni.dat`, clique em **sim** e, em seguida, clique em **concluir**.
4. Minimize a janela do agente de processo.
5. Clique com o botão direito do mouse em **NCOMs**.
6. Escolha a opção adequada:
 - Se a opção **Conectar-se Como...** não for exibida, você deverá iniciar o servidor de objeto NCOMS:
 - a. Para iniciar o servidor de objeto NCOMS, feche o `nco_config` e insira o seguinte comando:
`/opt/IBM/netcool/omnibus/bin/nco_objserv -name NCOMS &`
 - b. Se o servidor de objeto NCOMS não iniciar, procure um arquivo `NCOMS.pid` no diretório `/opt/IBM/netcool/omnibus/var` e exclua-o, em seguida, tente iniciar o servidor novamente.
 - Se a opção **Conectar-se Como...** for exibida, clique em **Conectar-se Como...**, em seguida, para o nome do usuário, digite raiz, e insira a senha.

7. Depois de iniciar o servidor NCOMs, para reiniciar a análise, insira o seguinte comando:
`/opt/IBM/netcool/omnibus/probes/nco_p_xml -name ioc_xml -propsfile /opt/IBM/netcool/omnibus/probes/linux2x86/ioc_xml.props &`
8. Para visualizar o arquivo de log, insira o seguinte comando: `tail -f /opt/IBM/netcool/omnibus/log/NCOMS.log`

Arquivo de Log do Banco de Dados do Tivoli Netcool/OMNibus (Agente de Processo)

O arquivo de log do Banco de Dados (Agente do Processo) do Tivoli Netcool/OMNibus encontra-se em `/opt/IBM/netcool/omnibus/log/NCO_PA.log`.

Ativando e Visualizando Arquivos de Log do Tivoli Netcool/Impact Sobre Esta Tarefa

O arquivo de log encontra-se em `opt/IBM/netcool/impact/log/`. Siga as etapas no procedimento para iniciar um rastreamento e visualizar um log.

Procedimento

1. Efetue logon no console administrativo do Tivoli Netcool/Impact em `http://event-host:9080/nci` com o nome de usuário `admin`, em que `event-host` é o nome completo do host do . Se um prompt do login não for exibido, insira os seguintes comandos em uma janela do terminal:

```
su - netcool
/opt/IBM/netcool/bin/ewas.sh start
```
2. Na janela Status do Serviço, role para baixo e certifique-se de que os seguintes serviços estejam em execução, conforme indicado por um símbolo verde:
 - `IOC_CAP_Event_Reader`
 - `IOC_Notification_Reader`
3. Além disso, na janela Status do Serviço, clique no ícone **Visualizar Log** ao lado de **PolicyLogger** para verificar se há quaisquer erros exibidos no log.
4. Se houver um ou mais erros no log, para obter mais detalhes, consulte os arquivos de log no seguinte diretório: `/opt/IBM/netcool/impact/log/`
5. Se precisar de mais detalhes, configure os níveis elevados do log. Clique em **PolicyLogger** e, em seguida, configure o valor de **Nível de Log Elevado** para 3 e marque as caixas de opções apropriadas.

O que Fazer Depois

É possível ativar diversos logs no tempo de execução por meio do console administrativo do WebSphere Application Server. Para obter mais informações sobre ativação do rastreamento do portal e outros rastreios que estão disponíveis no WebSphere Portal, consulte o link próximo ao início do tópico para a documentação do produto do WebSphere Portal e procure por *Criação de Log e Rastreamento*.

Tarefas relacionadas:

“Verificando os Arquivos de Log” na página 339

Verifique o arquivo de log de política do Tivoli Netcool/OMNibus e o arquivo de log do Tivoli Service Request Manager.

Executando a Ferramenta de Instalação Coleta de Informações

Os arquivos de log são gerados enquanto o IBM Intelligent Operations Center é instalado. Uma ferramenta está disponível para reunir esses arquivos de log para análise.

Procedimento

1. Efetue logon no servidor de instalação como raiz e abra uma janela do terminal.
2. Vá para o diretório `install_home/ioc/bin`.

3. Execute o comando `export JAVA_HOME=/opt/ibm/java-x86_64-60/jre` para configurar a variável `JAVA_HOME` para utilizar o Java 6 Runtime JRE.
4. Execute o comando `./mustgather.sh -p password` em que `password` é a senha de topologia. A ferramenta varre o arquivo de propriedades de topologia na primeira vez que é executada. Se o arquivo de propriedades de topologia for alterado após a execução da ferramenta, inclua `-n` no comando para que a ferramenta varra novamente o arquivo de propriedades de topologia. Por exemplo, `./mustgather.sh -n -p password`.

Resultados

Os logs coletados e outras informações serão gravadas no diretório `install_media/mustGather` no servidor de instalação. Haverá um arquivo com extensão `.tar` para cada um dos servidores.

As informações coletadas incluem:

- Logs para todas as fases de instalação, incluindo logs para cada componente instalado em cada nó.
- Logs de instalação da ferramenta Verificação do Sistema.
- Os arquivos XML de topologia.
- Todos os scripts usados durante o processo de instalação.
- Todas as vulnerabilidades tratadas pelo Cyber Hygiene.
- Os scripts do Cyber Hygiene.

Conceitos relacionados:

“Ativando Rastreios e Visualizando Arquivos de Log” na página 295

Para resolver um problema no IBM Intelligent Operations Center, pode ser necessário analisar os arquivos de log em vários sistemas. Os tópicos a seguir fornecem algumas orientações sobre como acessar os arquivos de log.

“Resolução de Problemas dos Componentes”

É possível utilizar a ferramenta do Verificação do Sistema para solucionar problemas dos IBM Intelligent Operations Center.

Tarefas relacionadas:

“Reiniciando a Instalação de Arquitetura do IBM Intelligent Operations Center Durante uma Instalação Passo-a-Passo” na página 47

Se a instalação da arquitetura falhar, a instalação poderá ser reiniciada.

“Trocando Informações com a IBM” na página 326

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.

Resolução de Problemas dos Componentes

É possível utilizar a ferramenta do Verificação do Sistema para solucionar problemas dos IBM Intelligent Operations Center.

Para obter mais informações sobre a ferramenta do Verificação do Sistema, consulte o link no final do tópico.

As tabelas nas seções a seguir listam as localizações do arquivo de log para cada um dos servidores contidos no IBM Intelligent Operations Center. Todos os arquivos de log são criados automaticamente. Visualize-os utilizando os comandos de rodapé apropriados.

Servidor de instalação

Para obter informações sobre a coleta de arquivos de log de instalação, consulte o tópico sobre a execução da ferramenta de coleta de informações. Acesse o link no final do tópico.

Servidor de aplicativos

Tabela 96. Componentes e Arquivos de Log do Servidor de aplicativos

Componente	Arquivos de Log
IBM Cognos Administration	<ul style="list-style-type: none"> • /opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/logs/CognosX_Displ/SystemOut.log • /opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/logs/CognosX_Displ/SystemErr.log • /opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/logs/CognosX_GW1/SystemOut.log • /opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/logs/CognosX_GW1/SystemErr.log • Todos os logs no diretório /opt/IBM/cognos/c10_64/logs/
IBM HTTP Server	<ul style="list-style-type: none"> • /opt/IBM/HTTPServer/logs/error_log • /opt/IBM/HTTPServer/logs/access_log
IBM WebSphere Business Monitor	<ul style="list-style-type: none"> • /opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/logs/WBM_DE.AppTarget.WBMNode1.0/SystemOut.log • /opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/logs/WBM_DE.AppTarget.WBMNode1.0/SystemErr.log
IBM Lotus Sametime Proxy Server	<ul style="list-style-type: none"> • /opt/IBM/WebSphere/AppServer/profiles/STPAppProfile1/logs/STProxyServer1/SystemOut.log • /opt/IBM/WebSphere/AppServer/profiles/STPAppProfile1/logs/STProxyServer1/SystemErr.log
Tivoli Access Manager	<ul style="list-style-type: none"> • /var/pdweb/log/msg_*.log, em que * é qualquer valor. • /var/pdweb/log/config_data_*.log onde * é qualquer valor
Tivoli Access Manager WebSEAL	<ul style="list-style-type: none"> • /var/pdweb/log/msg_webseald-default.log • Todos os logs no diretório /var/pdweb/www-default/log/
Proxy de configuração de log do Tivoli Directory Server	<ul style="list-style-type: none"> • /datahome/proxy/idsslapd-tdsproxy/logs/ibmslapd.log
WebSphere Operational Decision Management	<ul style="list-style-type: none"> • /opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/logs/wodmServer1/SystemOut.log • /opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/logs/wodmServer1/SystemErr.log
WebSphere Portal	<ul style="list-style-type: none"> • /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log • /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log
WebSphere UDDI Registry	<ul style="list-style-type: none"> • /opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/logs/cpudServer1/SystemOut.log • /opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/logs/cpudServer1/SystemErr.log

servidor de dados

Tabela 97. Componentes e Arquivos de Log do servidor de dados

Componente	Arquivos de Log
Tivoli Directory Server	<ul style="list-style-type: none"> • /datahome/dsrdbm01/idsslapd- dsrdbm01/logs/ibmslapd.log • Todos os logs no diretório /datahome/dsrdbm01/idsslapd- dsrdbm01/logs/

Servidor de eventos

Tabela 98. Componentes e Arquivos de Log do Servidor de eventos

Componente	Arquivos de Log
Lotus Domino	<ul style="list-style-type: none"> • /local/notesdata/console.out • /local/notesdata/log.nsf • Todos os logs no diretório /local/notesdata/IBM_TECHNICAL_SUPPORT/.
Lotus Sametime Community Server	Para coletar e gravar todos os arquivos de log pertinentes ao diretório /local/notesdata/, insira o seguinte comando: /local/notesdata/sh stdiagzip.sh
Tivoli Netcool/Impact	<ul style="list-style-type: none"> • /opt/IBM/netcool/eWAS/profiles/ImpactProfile/logs/server1/SystemOut.log • /opt/IBM/netcool/eWAS/profiles/ImpactProfile/logs/server1/SystemErr.log
Tivoli Netcool/OMNIBus	<ul style="list-style-type: none"> • /opt/IBM/netcool/log • /opt/IBM/netcool/omnibus/log
Tivoli Service Request Manager	<ul style="list-style-type: none"> • /opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/logs/MXServer1/SystemOut.log • /opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/logs/MXServer1/SystemErr.log

Servidor de Gerenciamento

Tabela 99. Componentes e Arquivos de Log do Servidor de Gerenciamento

Componente	Arquivos de Log
Servidor de Gerenciamento	<ul style="list-style-type: none"> • Tivoli Event Monitoring Server: /opt/IBM/ITM/logs/{MGMT_SERVER_HOST}_ms_{nnnnnn}.log • Tivoli Event Portal Server: /opt/IBM/ITM/logs/{MGMT_SERVER_HOST}_cq_{nnnnnn}.log • Logs do Embedded WebSphere Application Server: <ul style="list-style-type: none"> – Logs de erro: /opt/IBM/ITM/1i6263/iw/profiles/ITMProfile/logs/ITMServer/SystemErr.log – Log de saída: /opt/IBM/ITM/1i6263/iw/profiles/ITMProfile/logs/ITMServer/SystemOut.log – Log de início: /opt/IBM/ITM/1i6263/iw/profiles/ITMProfile/logs/ITMServer/startServer.log
Tivoli Access Manager e WebSphere Portal Manager	<ul style="list-style-type: none"> • /var/PolicyDirector/log/msg__pdmgrd_utf8.log • /var/PolicyDirector/log/msg__pdacld_utf8.log

Tabela 99. Componentes e Arquivos de Log do Servidor de Gerenciamento (continuação)

Componente	Arquivos de Log
Tivoli Access Manager	<ul style="list-style-type: none"> • /opt/IBM/WebSphere/AppServer/profiles/dmgr/logs/dmgr/SystemOut.log • /opt/IBM/WebSphere/AppServer/profiles/dmgr/logs/dmgr/SystemErr.log
Tivoli Enterprise Monitoring Agent	<ul style="list-style-type: none"> • /opt/IBM/ITM/logs/*_PRODUCT_CODE_{nnnnnn}.log
Tivoli Enterprise Portal	<ul style="list-style-type: none"> • /opt/IBM/ITM/logs/*_PRODUCT_CODE_{nnnnnn}.log
Tivoli Identity Manager	<ul style="list-style-type: none"> • /opt/IBM/WebSphere/AppServer/profiles/timProfile/logs/timServer1/SystemOut.log • /opt/IBM/WebSphere/AppServer/profiles/timProfile/logs/timServer1/SystemErr.log • Todos os logs nos subdiretórios V6 do diretório /var/idsldap/

Conceitos relacionados:

“Gerenciando Arquivos de Log” na página 261

O IBM Intelligent Operations Center armazena arquivos de log em vários locais diferentes. Para evitar problemas de desempenho do sistema, faça periodicamente archives de arquivos de log e remova os arquivos de log originais.

Tarefas relacionadas:

“Executando a Ferramenta de Instalação Coleta de Informações” na página 299

Os arquivos de log são gerados enquanto o IBM Intelligent Operations Center é instalado. Uma ferramenta está disponível para reunir esses arquivos de log para análise.

Informações relacionadas:

Como utilizar a ferramenta Sistema de Verificação

A ferramenta do Verificação do Sistema é usada para determinar o status operacional dos serviços que abrangem o sistema IBM Intelligent Operations Center.

Instalando e Usando IBM Support Assistant Lite

O IBM Support Assistant Lite (ISA Lite) é uma ferramenta que coleta dados diagnósticos comuns úteis para analisar problemas gerais.

O ISA Lite reúne os seguintes tipos de informações:

- Arquivos de determinação de problemas da plataforma
- Arquivos de rastreamento e log do sistema
- Arquivos de provisão de plataforma
- Arquivos de configuração do sistema
- Arquivos dump Java™
- Arquivos de registro internos da estrutura de determinação de problemas

Para fazer o download do ISA Lite para IBM Intelligent Operations Center 1.5, consulte o link no final do tópico.

Para instalar e usar o ISA Lite, siga as instruções do Guia de Iniciação Rápida incluído no pacote de download.

Informações relacionadas:

 Downloading IBM Support Assistant Lite for IBM Intelligent Operations Center 1.5

IBM Intelligent Operations Center Mensagens

Cada tópico da mensagem ajuda a identificar a causa de uma determinada condição de erro no IBM Intelligent Operations Center e recomenda ações a serem tomadas para resolver o erro.

Para ajudá-lo a compreender os erros que podem ser encontrados durante a utilização do IBM Intelligent Operations Center, cada tópico da mensagem é dividido em três seções: a mensagem exibida no IBM Intelligent Operations Center ou seus logs, uma explicação e uma ação.

a mensagem;

Contém dois identificadores, que são a identificação do erro e o texto associado. A identificação de erro é o ID da mensagem. É um número exclusivo que identifica a mensagem. Um caractere E no final indica que a mensagem resultou de um erro, W indica uma mensagem de aviso e I indica uma mensagem informativa.

A explicação

Contém uma explicação adicional da mensagem.

A resposta do usuário

Sugere a ação corretiva para resolução do erro.

Para ajudá-lo a procurar informações sobre uma mensagem de erro, insira o número do ID da mensagem de erro no campo Procurar no centro de informações.

Nota: Os tópicos nesta seção contêm somente mensagens específicas para IBM Intelligent Operations Center. Para todas as outras mensagens, consulte a documentação do produto.

CIYBA0101E O Arquivo de Topologia {0} não é válido.

Explicação: O instalador tentou validar o arquivo de topologia {0} e descobriu que o arquivo de topologia continha erros. Esses erros podem incluir:

- Nem todos os componentes requeridos existem no arquivo de topologia.
- Componentes de pré-requisito não estão listados antes dos componentes dependentes.
- Componentes que devem ser implementados sequencialmente estão na sub-rotina de desenvolvimento paralelo.

Resposta do Usuário: Corrija o arquivo de topologia e execute novamente a instalação.

está configurada para o local correto. O arquivo custom.properties está no subdiretório /resource noservidor de instalação em que o pacote de instalação foi extraído.

CIYBA0103E O script {0} para instalar um componente não existe.

Explicação: O programa de instalação tentou localizar um script para um componente e esse script não foi localizado.

Resposta do Usuário: Verifique se a mídia de instalação foi extraída noservidor de instalação. Verifique se o diretório base foi corretamente configurado no arquivo custom.properties. O diretório base é usada para derivar o local no script de instalação.

CIYBA0102E A topologia ou arquivos de especificação de topologia não foram localizados.

Explicação: Cada topologia de instalação tem um arquivo .xml e especificação. Um ou ambos os arquivos não puderam ser localizados.

Resposta do Usuário: Certifique-se de que todos os arquivos de instalação foram extraídos para o servidor de instalação. Verifique se a propriedade image.basedir.local no arquivo custom.properties

CIYBA0104E O arquivo de Topologia contém entradas inválidas.

Explicação: O instalador encontrou um erro ao ler o arquivo de topologia e ao criar as unidades implementáveis para cada componente. Normalmente esse é um erro interno, a menos que uma topologia customizada esteja sendo instalada.

O arquivo de topologia pode estar corrompido ou incorretamente especificado.

Resposta do Usuário: Verifique o arquivo de topologia para os seguintes problemas:

- IDs de componente duplicados.
- IDs de componente ou atributos de tipo ausentes.
- Especificação de um atributo de conexão no qual nenhum componente pai existe.
- A topologia falha na validação do esquema XML.

CIYBA0105E O arquivo {0} não pôde ser localizado.

Explicação: O programa de instalação não pôde localizar o arquivo {0}.

Resposta do Usuário: Certifique-se de que todos os arquivos de instalação foram extraídos para o servidor de instalação. Verifique se a propriedade `image.basedir.local` no arquivo `custom.properties` está configurada para o local de coleta. O arquivo `custom.propeties` está no subdiretório `/resource` no servidor de instalação em que o pacote de instalação foi extraído.

CIYBA0106E O arquivo {0} não pôde ser salvo.

Explicação: O programa de instalação tentou gravar o arquivo nomeado {0} e um erro de E/S de arquivo foi retornado.

Resposta do Usuário: Verifique se o local especificado pode ser acessado usando o ID de usuário do instalador. Certifique-se de que há espaço suficiente no disco e que a partição não esteja corrompida.

CIYBA0107E A referência de propriedade {0} não foi localizada no arquivo de topologia {1}

Explicação: Durante a instalação, alguns dos componentes requerem valores da propriedade do software de pré-requisito. Esses componentes usam referências de propriedade no arquivo de topologia para determinar os valores de propriedade requeridos. A referência de propriedade não pôde ser localizada no arquivo de topologia.

Resposta do Usuário: O arquivo de topologia está corrompido. Isso pode ser devido a edições manuais que introduziram entradas inválidas ou porque a instalação não gravou um arquivo de topologia com valores corretos. Determine quais componentes foram incorretamente instalados. Remova quaisquer componentes incorretamente instalados, corrija o arquivo de topologia, e instale novamente.

CIYBA0108E O componente {0} não foi localizado no arquivo de topologia {1}.

Explicação: O programa de instalação esperou localizar o ID de componente {0} no arquivo de topologia {1}. O ID de componente não foi localizado. O problema pode ser devido a uma dependência especificada incorretamente em um elemento de

conexão de outro componente.

Resposta do Usuário: Revise o arquivo de topologia para referências a {0}. Corrija quaisquer elementos de conexão para o componente {0} e reinstale.

CIYBA0109E A propriedade {0}.{1} no Arquivo de Topologia {2} é inválida.

Explicação: A propriedade não foi localizada no arquivo de topologia ou em um arquivo de propriedades de especificação.

Resposta do Usuário: Se ausente, inclua a propriedade no arquivo de propriedades de especificação ou no arquivo de topologia. Esse erro também pode ser devido a ortografia errada da propriedade. Corrija o arquivo de topologia ou arquivo de propriedades de especificação e instale novamente.

CIYBA0110E A propriedade {0}.{1} no Arquivo de Topologia {2} não pode ser localizada.

Explicação: Uma unidade implementável referencia outra unidade implementável indicada pela função {1}. A unidade implementável dependente não foi localizada ou há uma incompatibilidade nas funções.

Resposta do Usuário: O arquivo de topologia indicado contém referências à propriedade mostrada, porém, a definição dessa propriedade não pode ser localizada no arquivo de topologia. Essa situação pode surgir se o arquivo de topologia foi editado manualmente e um componente foi removido, porém, as referências a esse componente ainda existam.

CIYBA0111E Não é possível recuperar o host principal para o componente {0}.

Explicação: Um componente de topologia deve ser associado a um host de destino. Um componente de topologia órfão é especificado.

Resposta do Usuário: Verifique o componente de topologia {0} e certifique-se de que tem uma sequência de atributos de conexão que finalmente tem um componente com um atributo do host.

CIYBA0112E Falha ao ler o arquivo de topologia {0}.

Explicação: O programa de instalação não conseguiu ler o arquivo de topologia especificado.

Resposta do Usuário: Verifique se o arquivo de topologia indicado está no diretório de instalação e que o programa de instalação pode acessar o diretório.

CIYBA0113E Falha ao salvar o arquivo {0}.

Explicação: O programa de instalação não conseguiu salvar o arquivo de indicado.

Resposta do Usuário: Verifique se o programa de

instalação tem acesso ao diretório de instalação.

CIYBA0114E A propriedade {0},{1} não pode ser configurada.

Explicação: O programa de instalação não conseguiu atualizar a propriedade indicada.

Resposta do Usuário: O arquivo de topologia está corrompido ou foi editado manualmente e introduziu valores de propriedade inválidos. Corrija o arquivo de topologia e execute novamente a instalação.

CIYBA0115E O Arquivo de Topologia {0} não pode ser localizado.

Explicação: O programa de instalação não conseguiu acessar o arquivo de topologia indicado.

Resposta do Usuário: Verifique se o arquivo de topologia está no diretório especificado pelo programa de instalação e certifique-se de que o programa de instalação pode acessar o diretório.

CIYBA0116E Não é possível gravar no arquivo de propriedades {0}.

Explicação: O programa de instalação não conseguiu gravar o arquivo de propriedades indicado.

Resposta do Usuário: Verifique se o ID de usuário usado pelo programa de instalação tem acesso a todos os diretórios temporários nos servidores de destino. O diretório nos servidores de destino nos quais os scripts de instalação temporária serão gravados é especificado pela propriedade `Unix.script.basedir.remote` no arquivo `custom.properties`. Corrija esse valor de propriedade se estiver especificado incorretamente.

CIYBA0117E O instalador falhou ao criar o keystore.

Explicação: O programa de instalação não pôde criar o armazenamento de chaves.

Resposta do Usuário: Verifique se o ID de usuário usado pelo programa de instalação tem acesso a todos os subdiretórios nos quais a mídia de instalação foi extraída.

CIYBA0118E O instalador não pôde acessar o keystore usando a senha fornecida. A senha está incorreta ou o keystore está corrompido.

Explicação: O programa de instalação não pôde acessar o keystore.

Resposta do Usuário: Verifique se a senha fornecida está correta e se o keystore não foi corrompido. Gere novamente o keystore com uma nova senha por meio da reinstalação da solução.

CIYBA0119E Não é possível decryptografar a propriedade {0} no arquivo de topologia {1}.

Explicação: O programa de instalação tentou criptografar a propriedade indicada usando a senha fornecida no arquivo de topologia e não conseguiu.

Resposta do Usuário: Verifique se o keystore não está corrompido e se a senha para a topologia está correta. Se necessário, recrie o keystore com uma nova senha por meio de reinstalação.

CIYBA0120E Não é possível decryptografar a propriedade {0} no arquivo de topologia {1}

Explicação: Uma tentativa de ler e decryptografar a propriedade indicada falhou.

Resposta do Usuário: Verifique se o ID de usuário usado pelo programa de instalação pode acessar o arquivo de topologia indicado e se o arquivo de topologia está em um local esperado. Verifique se a senha e a chave secreta estão corretas. Execute a instalação novamente.

CIYBA0121E O arquivo de keystore {0} já existe.

Explicação: Esse erro não deve ocorrer ao usar a instalação do IBM Installation Manager. O IBM Installation Manager controla o fluxo de instalação e garante que uma tentativa não seja feita para gerar o keystore novamente.

Resposta do Usuário: Verifique se a instalação já não foi executada. Execute novamente o instalador assim que o keystore existente de uma tentativa de instalação anterior tenha sido removido.

CIYBA0122E O keystore para a Topologia não existe. Execute o comando createSecretKey.

Explicação: Esse erro não deve ocorrer ao executar a instalação do IBM Installation Manager. A instalação do IBM Installation Manager automaticamente aceita a Chave Secreta e gera o keystore.

Resposta do Usuário: Se estiver executado uma instalação passo a passo, siga as etapas para gerar um keystore.

CIYBA0123E A Topologia {0} não está completamente instalada.

Explicação: O programa de instalação determinou que nem todos os componentes na topologia foram instalados.

Resposta do Usuário: Verifique o arquivo de topologia e determine quais componentes não foram instalados. Reinicie a instalação.

CIYBA0124E O arquivo de propriedades {0} não pode ser localizado.

Explicação: O programa de instalação tentou ler o arquivo de propriedades indicado. Porém, o arquivo não pôde ser localizado.

Resposta do Usuário: Verifique se o pacote de instalação foi adequadamente extraído. Verifique se o ID de usuário usado pelo programa de instalação tem acesso a todos os diretórios nos quais o pacote foi extraído.

CIYBA0125E Não é possível gravar no arquivo de propriedades {0}.

Explicação: O programa de instalação tentou atualizar um arquivo com os valores da variável de tempo de execução e uma exceção de E/S foi retornada.

Resposta do Usuário: Verifique se o local especificado pode ser acessado usando o ID de usuário do programa de instalação. Verifique se há espaço suficiente no sistema de arquivos e se a partição de disco não está corrompida.

CIYBA0126E Não é possível configurar o valor para a propriedade {0} do arquivo de topologia.

Explicação: O programa de instalação não pôde configurar o valor da propriedade especificado.

Resposta do Usuário: Verifique se as propriedades no arquivo de topologia indicado tem a sintaxe XML correta. Verifique se o arquivo de topologia não está corrompido ou com defeito. Remova quaisquer caracteres especiais do arquivo e reinicie a instalação.

CIYBA0127E Não é possível ler o arquivo de especificação da solução {0}.

Explicação: O programa de instalação tentou ler o arquivo indicado e um erro de E/S de arquivo foi retornado.

Resposta do Usuário: Verifique se o arquivo existe no local especificado. Verifique se o ID de usuário usado pelo programa de instalação tem acesso a todos os diretórios nos quais o pacote foi extraído.

CIYBA0128E O arquivo {0} não pôde ser salvo.

Explicação: O programa de instalação tentou gravar o arquivo indicado e um erro de E/S de arquivo foi retornado.

Resposta do Usuário: Verifique se o local especificado pode ser acessado pelo ID de usuário usado pelo programa de instalação. Verifique se há espaço suficiente no sistema de arquivos e se a partição de disco não está corrompida.

CIYBA0129E Não é possível ler o arquivo do pacote da solução {0}.

Explicação: O programa de instalação tentou ler o arquivo indicado e um erro de E/S de arquivo foi retornado.

Resposta do Usuário: Verifique se o arquivo existe no local especificado. Verifique se o ID de usuário usado pelo programa de instalação tem acesso a todos os diretórios nos quais o pacote foi extraído.

CIYBA0130E O arquivo do pacote da solução: {0} não existe.

Explicação: O programa de instalação tentou ler o arquivo indicado e um erro de E/S de arquivo foi retornado.

Resposta do Usuário: Verifique as permissões do arquivo indicadas na mensagem. Certifique-se de que o ID de usuário usado pelo programa de instalação tem permissão para ler o arquivo. Modifique as permissões de arquivo, se necessário.

CIYBA0131E O instalador falhou ao carregar o arquivo de topologia {0}. Mensagem de E/S de arquivo foi {1}.

Explicação: O erro indicado foi retornado ao tentar importar o arquivo de topologia especificado.

Resposta do Usuário: Verifique se o arquivo de topologia indicado está no diretório correto. Verifique se o arquivo de topologia não contém nenhum caractere inválido. Verifique se o programa de instalação pode acessar o diretório que contém o arquivo de topologia.

CIYBA0140E Não é possível acessar os arquivos de instalação necessários.

Explicação: O programa de instalação tentou ler um arquivo necessário e não conseguiu.

Resposta do Usuário: Verifique se o local no qual o pacote de instalação foi extraído pode ser acessado pelo ID de usuário usado pelo programa de instalação. Certifique-se de que a partição de disco não está corrompida. Extraia o pacote de instalação de novo e tente novamente a instalação.

CIYBA0141E Não é possível localizar o arquivo de instalação {0}.

Explicação: O programa de instalação tentou ler o arquivo indicado e um erro de E/S de arquivo foi retornado.

Resposta do Usuário: Verifique se o arquivo existe no local especificado. Verifique se o ID de usuário usado pelo programa de instalação pode acessar todos os diretórios que contém o pacote de instalação extraído.

CIYBA0142E Não é possível gravar o arquivo de instalação {0}.

Explicação: O programa de instalação tentou gravar o arquivo indicado e um erro de E/S de arquivo foi retornado.

Resposta do Usuário: Verifique se o ID de usuário usado pelo programa de instalação tem acesso a todos os diretórios que contêm o pacote de instalação extraído. Verifique se a partição de disco não está corrompida ou sem espaço.

CIYBA0143E O programa de instalação falhou ao processar o arquivo de topologia l.

Explicação: O programa de instalação lê o arquivo de topologia e gera arquivos intermediários que contêm valores de tempo de execução. O programa de instalação encontrou um erro durante o processamento do arquivo de topologia e gravação dos arquivos intermediários. Erros de E/S de arquivo são as prováveis causas desse erro.

Resposta do Usuário: Verifique se o ID de usuário usado pelo programa de instalação tem acesso a todos os diretórios nos quais o pacote de instalação foi extraído. Verifique se a partição de disco não está corrompida ou sem espaço.

CIYBA0150E Não é possível ler o arquivo de Especificação de Topologia {0}.

Explicação: O programa de instalação tentou ler o arquivo indicado e um erro de E/S de arquivo foi retornado.

Resposta do Usuário: Verifique se o arquivo existe no local especificado. Verifique se o ID de usuário usado pelo programa de instalação tem direitos de acesso a todos os diretórios nos quais o pacote de instalação foi extraído.

CIYBA0160E O arquivo de especificação de regra não foi localizado no diretório {0}.

Explicação: O programa de instalação tentou carregar o arquivo rule-spec.xml, que define as regras de pré-verificação e não conseguiu.

Resposta do Usuário: Verifique se o diretório indicado existe. Também certifique-se de que o diretório possa ser acessado pelo ID de usuário usado pelo programa de instalação.

CIYBA0161E O nome da regra {0} é inválido.

Explicação: O programa de instalação identificou um nome de valor incorreto no arquivo rule-spec.xml. Esse arquivo define regras usadas pela etapa de pré-verificação.

Resposta do Usuário: Verifique se o nome da regra

está correto no arquivo rule-spec.xml. Consulte uma versão inalterada do arquivo rule-spec.xml para o nome da regra correto.

CIYBA0162E Verificação de pré-requisitos de instalação falhou para a topologia {0}.

Explicação: A etapa de pré-verificação falhou com um ou mais dos destinos de configuração não atendendo aos requisitos do sistema suportados.

Resposta do Usuário: Verifique se a topologia planejada atende aos requisitos suportados mínimos.

CIYBA0163W O tipo de sistema operacional do servido de destino {0} não é {1}.

Explicação: A etapa de pré-verificação detectou um sistema operacional não suportado no servidor de destino indicado.

Resposta do Usuário: Certifique-se de que o sistema operacional no servidor de destino atende aos requisitos do sistema suportados.

CIYBA0164W Espera-se que o servidor {0} tivesse um sistema operacional de {1} bits.

Explicação: A etapa de pré-verificação detectou um sistema operacional incorreto no servidor de destino.

Resposta do Usuário: Verifique se o tipo de sistema operacional no servidor de destino atende aos requisitos do sistema.

CIYBA0165W CPU do servidor de destino {0} não é uma CPU x86 ou s390 de 64 bits.

Explicação: A etapa de pré-verificação detectou um tipo de CPU não suportado para o servidor de destino indicado.

Resposta do Usuário: Verifique se o tipo de CPU para o servidor de destino atende aos requisitos do sistema.

CIYBA0166E Não é possível se conectar ao servidor de destino {0}.

Explicação: O programa de instalação não pôde se conectar ao servidor remoto ao executar a etapa de pré-verificação.

Resposta do Usuário: Verifique a conectividade entre o servidor de instalação e os servidores de destino. Verifique os logs de pré-verificação para outros erros.

CIYBA0167E Não é possível se conectar ao servidor {0} porque o nome do host, conta ou senha errada foi especificada.

Explicação: O programa de instalação falhou ao executar a etapa de pré-verificação. O programa de instalação não pôde se conectar ao servidor de destino.

Resposta do Usuário: Verifique se o nome do host está no formato correto e se os detalhes de login estão corretos para o servidor remoto. Verifique os logs de pré-verificação para obter informações adicionais.

CIYBA0168E A hora ou fuso horário para os servidores {0} e {0} não estão sincronizados.

Explicação: Existe uma diferença entre a configuração de hora ou fusos horários para os servidores.

Resposta do Usuário: Verifique se a hora e fuso horário são os mesmos para todos os servidores.

CIYBA0169W Verifique os tipos e arquitetura de CPU no servidor {0}

Explicação: A etapa de pré-verificação do programa de instalação localizou um sistema operacional e arquitetura de CPU não suportados para um se servidor de destino.

Resposta do Usuário: Certifique-se de que todos os servidores atendem aos requisitos do sistema para a solução.

CIYBA0170W Verifique o fuso horário e a data & hora em todos os servidores

Explicação: Essa mensagem é seguida pela palavra "êxito" ou "falha". O que vem a seguir determina a ação a ser tomada.

Resposta do Usuário: Se a mensagem é seguida por "êxito", nenhuma resposta é necessária. Se a mensagem é seguida por "falha", então os servidores de vem ser sincronizados. O fuso horário, data e parâmetros do sistema de hora devem ser os mesmos para cada nó na topologia.

CIYBA0171I Verificação de pré-requisitos de instalação está iniciando usando a instância {0}.

Explicação: Esta mensagem tem apenas propósitos informativos.

Resposta do Usuário: Nenhuma ação é necessária.

CIYBA0172I Verificação de pré-requisito de instalação concluída com sucesso.

Explicação: Esta mensagem tem apenas propósitos informativos.

Resposta do Usuário: Nenhuma ação é necessária.

CIYBA0173I Verificação de pré-requisito de instalação concluída com {0} avisos e {1} erros:

Explicação: Esta mensagem tem apenas propósitos informativos.

Resposta do Usuário: Nenhuma ação é necessária.

CIYBA0176E As informações de login para o servidor {0} estão incorretas. Verifique o ID do usuário e senha para o servidor.

Explicação: A etapa de pré-verificação do programa de instalação localizou informações de login incorretas para o servidor de destino.

Resposta do Usuário: Verifique se os detalhes da conta para o servidor possuem o ID e senha de usuário corretos.

CIYBA0177W Não é possível se conectar ao servidor remoto. Aguardando para tentar novamente.

Explicação: A etapa de pré-verificação do programa de instalação falhou na conexão com o servidor remoto. A conexão será tentada novamente.

Resposta do Usuário: Nenhuma ação é necessária. O programa de instalação aguardará o período de tempo especificado na propriedade `waiting.time` no arquivo `custom.properties` e então tentará novamente a conexão.

CIYBA0178W Não é possível se conectar ao {0}, aguardando {1} milissegundos antes da próxima tentativa de conexão.

Explicação: Há problemas de conectividade no sistema.

Resposta do Usuário: Se diversas tentativas de conexão falham, entre em contato com o administrador da rede para resolver os problemas de conectividade e tente novamente a instalação.

CIYBA0179E Nenhum valor foi fornecido para a chave {0} no arquivo de propriedades da topologia.

Explicação: A etapa de pré-verificação do programa de instalação não pôde recuperar valores para o nome do host, nome de usuário ou senha do arquivo de propriedades.

Resposta do Usuário: Verifique se o nome do host, nome de usuário e senha estão especificados corretamente o arquivo de propriedades.

CIYBA0180E O ID do usuário inserido para o servidor {0} não tem privilégios de administrador.

Explicação: A etapa de pré-verificação do programa de instalação detectou que a conta usada para o servidor indicado não tem privilégios de administrador.

Resposta do Usuário: Mude o ID de usuário usado para o servidor para um que tenha privilégios de administrador ou inclua privilégios de administrador para o ID especificado para o servidor.

CIYBA0181E Verifique o ID e senha do usuário raiz para o servidor {0}.

Explicação: A etapa de pré-verificação do programa de instalação determinou que o ID do usuário usado para o servidor tem direitos de acesso insuficientes.

Resposta do Usuário: Verifique se a conta tem direitos de acesso suficientes.

CIYBA0182E Verifique a conectividade do servidor de instalação para {0}

Explicação: A etapa de pré-verificação do programa de instalação falhou na conexão entre o servidor de instalação e o servidor de destino.

Resposta do Usuário: Verifique a conectividade entre os servidores. Revise os logs de pré-verificação para informações adicionais.

CIYBA0183E O valor {0} para a chave {1} não é válido, ele deve ser "EM64T" ou "AMD64" ou "S390".

Explicação: O valor da chave deve ser um dos valores especificados.

Resposta do Usuário: Corrija valor e execute novamente a instalação.

CIYBA0184E Valor {0} para a chave {1} não é um nome do host válido

Explicação: A etapa de pré-verificação do programa de instalação determinou que o valor fornecido não é um nome do host válido.

Resposta do Usuário: Verifique se o nome do host está no formato correto e se possui um valor correto.

CIYBA0185E A verificação de pré-requisito de instalação falhou na regra {0}

Explicação: A etapa de pré-verificação do programa de instalação falhou ao verificar a regra especificada.

Resposta do Usuário: Verifique os logs de pré-verificação para mensagens adicionais. Corrija o erro e tente novamente a instalação.

CIYBA0187E Keystore SSH "{0}" foi especificado, mas não pôde ser acessado. O protocolo SSH baseado em certificado estará indisponível. Detalhes: {1}.

Explicação: A etapa de pré-verificação do programa de instalação detectou dados inválidos no keystore SSH ao tentar se conectar com o servidor de destino.

Resposta do Usuário: Revise os detalhes na mensagem e verifique se o keystore fornecido possui entradas adequadas.

CIYBA0190E O componente {0} deve aparecer antes do componente {1} no arquivo de topologia.

Explicação: O arquivo de topologia foi alterado incorretamente. Um componente de pré-requisito aparece após um componente que depende dele.

Resposta do Usuário: Mude o arquivo de topologia para que os componentes que possuem dependências estejam após os componentes que dependem dele.

CIYBA0191E Existe uma dependência entre o componente {0} e o componente {1} no Arquivo de Topologia. Os componentes não podem ser implementados em paralelo.

Explicação: Os componentes não podem ser implementados em paralelo se houver uma dependência entre eles. Por exemplo, se o componente 2 é um pré-requisito do componente 1.

Resposta do Usuário: Remova os componentes da sub-rotina em paralelo do arquivo de topologia.

CIYBA0192E A propriedade {1}.{2} tem um valor de referência inválido de {0} no Arquivo de Topologia.

Explicação: O valor de referência incluído na mensagem não é válido para a propriedade indicada.

Resposta do Usuário: Use o campo de ID para localizar a definição de propriedade e certifique-se de que todas as referências à propriedade possuem o valor correto.

CIYBA0193E O componente {0} tem conexões duplicadas {1} identificadas no Arquivo de Topologia.

Explicação: Conexões duplicadas para o componente são definidas no arquivo de topologia.

Resposta do Usuário: Remova as informações de conexão duplicada no arquivo de topologia e execute novamente o programa de instalação.

CIYBA0194E A propriedade {0} está duplicada no componente {0}

Explicação: Uma propriedade duplicada está definida para o componente.

Resposta do Usuário: Remova a propriedade duplicada para o componente no arquivo de propriedades.

CIYBA0195E O componente {0} no arquivo de topologia tem uma propriedade inválida {0}.

Explicação: A propriedade especificada foi inesperada para o componente indicado. Isso pode ser causado por uma propriedade com ortografia errada ou devido à ausência de uma propriedade da especificação da propriedade.

Resposta do Usuário: Inclua a propriedade especificada no arquivo de propriedades ou na topologia. Se a propriedade tem erro de ortografia, corrija esse erro. Corrija o arquivo de topologia ou arquivo de propriedades de especificação e reinicie a instalação.

CIYBA0196E O componente {1} está ausente da propriedade {0}

Explicação: O componente deve ter a propriedade indicada. O erro poderia ser causado por uma propriedade com ortografia errada ou devido à ausência da propriedade do arquivo de especificação de propriedade.

Resposta do Usuário: Inclua a propriedade no arquivo de propriedades da especificação ou na topologia. Se o erro for devido a ortografia errada, corrija o erro de ortografia. Reinicie a instalação.

CIYBA0197E O componente {1} tem um tipo de componente {1} inválido.

Explicação: Um tipo de componente inválido foi especificado para o componente.

Resposta do Usuário: Verifique se o arquivo de especificação para o componente contém o tipo de componente. Arquivos de especificação de componente estão localizados no subdiretório *install_home/spec/component* no servidor de instalação.

CIYBA0198E A conexão {0} não é válida para o componente {1}

Explicação: A conexão definida não é válida para o componente.

Resposta do Usuário: Verifique a ortografia da conexão no arquivo de topologia para o componente e certifique-se de que está correta.

CIYBA0199E A conexão {0} estava ausente do componente {1}.

Explicação: Nenhuma conexão está definida para o componente indicado.

Resposta do Usuário: Verifique o arquivo de especificação do componente e certifique-se de que as informações de conexão estão incluídas.

CIYBA0200E As informações de conexão para {0} não existem.

Explicação: O ID de conexão está ausente para o componente indicado.

Resposta do Usuário: Verifique se o ID de conexão está especificado no no arquivo de topologia. Verifique se o ID de conexão está com a ortografia correta e se ele se refere a uma sub-rotina no arquivo de topologia que define o componente associado para o ID de conexão.

CIYBA0201E Não é possível se conectar ao servidor remoto {0}.

Explicação: O programa de instalação localizou um problema de conectividade para o servidor indicado.

Resposta do Usuário: Verifique se não há problemas de conexão entre os servidores. Execute a etapa de pré-verificação do programa de instalação e resolva quaisquer problemas de conectividade.

CIYBA0202E Nome ou senha de usuário é inválido para o servidor {0}.

Explicação: O programa de instalação localizou credenciais inválidas para o servidor indicado.

Resposta do Usuário: Verifique se as credenciais do servidor estão corretas no arquivo de topologia.

CIYBA0203E O arquivo {0} não existe.

Explicação: Uma tentativa de carregar o arquivo de propriedades retornou um erro.

Resposta do Usuário: Verifique se o caminho para o arquivo de propriedades está correto e se o arquivo existe.

CIYBA0204E Não é possível ler/gravar o arquivo {0}.

Explicação: O programa de instalação tentou carregar o arquivo de propriedades e um erro foi retornado.

Resposta do Usuário: Verifique se o caminho do arquivo de propriedades está correto e se o arquivo indicado existe.

CIYBA0205E Não é possível criar o diretório {0} no {1}.

Explicação: O programa de instalação não pôde copiar um diretório no servidor remoto.

Resposta do Usuário: Verifique se há espaço suficiente no servidor remoto e se o ID de usuário usado pelo programa de instalação tem direitos de acesso suficientes e permissões adequadas para criar um diretório.

CIYBA0206E Falha ao fazer upload do arquivo {0} para diretório remoto {1} no servidor {2}.

Explicação: O programa de instalação não pôde copiar os arquivos para o diretório indicado no servidor remoto.

Resposta do Usuário: Verifique se há espaço suficiente no servidor remoto e se o ID de usuário usado pelo programa de instalação tem direitos de acesso suficientes e permissão adequada para gravar arquivos no servidor remoto.

CIYBA0207E Nenhuma imagem definida para {0}.

Explicação: O programa de instalação não pôde recuperar dados de imagem para o arquivo de propriedades.

Resposta do Usuário: Verifique se o arquivo de propriedades contém um campo de imagem com o componente de dados.

CIYBA0208E Falha ao fazer upload da imagem do componente {0} para o servidor remoto {1}.

Explicação: O programa de instalação não pôde copiar os arquivos de imagem para um diretório no servidor remoto.

Resposta do Usuário: Verifique se há espaço suficiente no servidor remoto e se o ID de usuário usado pelo programa de instalação tem direitos de acesso suficientes e permissão adequada para gravar no diretório no servidor remoto. Também verifique se o nome do diretório remoto está correto.

CIYBA0209I Nome do host: {0}.

Explicação: Esta mensagem tem apenas propósitos informativos.

Resposta do Usuário: Nenhuma ação é necessária.

CIYBA0210I OSType={0},OSBit={1},CPUArch={2}.

Explicação: Esta mensagem tem apenas propósitos informativos.

Resposta do Usuário: Nenhuma ação é necessária.

CIYBA0211I Caminho remoto: {0}.

Explicação: Esta mensagem tem apenas propósitos informativos.

Resposta do Usuário: Nenhuma ação é necessária.

CIYBA0212I Caminho local: {0}.

Explicação: Esta mensagem tem apenas propósitos informativos.

Resposta do Usuário: Nenhuma ação é necessária.

CIYBA0213E Falha ao fazer download do arquivo {0} do servidor remoto {1}.

Explicação: O programa de instalação não pôde copiar os arquivos de imagem de um servidor de diretório remoto para o servidor local.

Resposta do Usuário: Verifique se há espaço suficiente no servidor local e se o ID de usuário usado pelo programa de instalação tem direitos de acesso suficientes e permissão adequada para gravar no diretório. Também verifique se os nomes do diretório local e remoto estão corretos.

CIYBA0214E Faça download do arquivo {0}.

Explicação: Esta mensagem tem apenas propósitos informativos.

Resposta do Usuário: Nenhuma ação é necessária.

CIYBA0215I Comando: {0}.

Explicação: Esta mensagem tem apenas propósitos informativos.

Resposta do Usuário: Nenhuma ação é necessária.

CIYBA0216I Código de saída de comando: {0}.

Explicação: Esta mensagem tem apenas propósitos informativos.

Resposta do Usuário: Nenhuma ação é necessária.

CIYBA0217I Saída de comando: {0}.

Explicação: Esta mensagem tem apenas propósitos informativos.

Resposta do Usuário: Nenhuma ação é necessária.

CIYBA0218E Comando falhou com código de retorno {0}.

Explicação: O comando não foi concluído com êxito.

Resposta do Usuário: Verifique os arquivos de log para mais detalhes.

CIYBA0219I Faça upload do arquivo {0}.

Explicação: Esta mensagem tem apenas propósitos informativos.

Resposta do Usuário: Nenhuma ação é necessária.

CIYBA0220I Diretório de imagem local: {0}.

Explicação: Esta mensagem tem apenas propósitos informativos.

Resposta do Usuário: Nenhuma ação é necessária.

CIYBA0221I Diretório de imagem remota: {0}.

Explicação: Esta mensagem tem apenas propósitos informativos.

Resposta do Usuário: Nenhuma ação é necessária.

CIYBA0222E Imagem remota {0} já existe.

Explicação: O arquivo já existe no servidor de destino. O processo de instalação inclui a transferência de mídia para servidores de destino. Essa mensagem indica que a imagem requerida já foi transferida.

Resposta do Usuário: Essa mensagem indica que a mídia de uma tentativa de instalação anterior ainda existe nos servidores de destino. Se um usuário pretende iniciar uma nova instalação, a mídia deve ser excluída para que possa ser transferida por upload novamente.

CIYBA0223E Não é possível ativar o comando no servidor {0}.

Explicação: O programa de instalação não pôde executar o comando **IOC** do servidor remoto para o servidor local.

Resposta do Usuário: Verifique a conectividade entre os servidores local e remoto. Verifique se o ID de usuário usado pelo programa de instalação tem direitos de acesso suficientes e permissão adequada para executar o comando.

CIYBA0224E Obtenha arquivos de backup da pasta {0} no servidor {1}.

Explicação: Esta mensagem tem apenas propósitos informativos.

Resposta do Usuário: Nenhuma ação é necessária.

CIYBA0225E Falha ao obter arquivos de backup da pasta {0} no servidor {1}.

Explicação: O programa de instalação não pôde recuperar arquivos de uma pasta de backup remota para uma pasta local.

Resposta do Usuário: Verifique a conectividade entre

os servidores local e remoto. Verifique se o ID de usuário usado pelo programa de instalação tem direitos de acesso suficientes e permissão adequada para acessar as pastas.

CIYBA0226E Nenhuma pasta de backup {0} existe no servidor {1}.

Explicação: O programa de instalação não pôde recuperar arquivos de uma pasta de backup remota para uma pasta local.

Resposta do Usuário: Verifique se o diretório e pasta remotos existem.

CIYBA0227E O valor deve ser fornecido para o atributo do caminho e ID.

Explicação: A instalação não pôde identificar o ID de componente e o atributo do caminho.

Resposta do Usuário: Verifique se os argumentos de ID de componente e caminho são fornecidos dentro dos argumentos de tarefa.

CIYBA0228I Comando executável: {0}.

Explicação: Esta mensagem tem apenas propósitos informativos.

Resposta do Usuário: Nenhuma ação é necessária.

CIYBA0229E Espaço em disco insuficiente no diretório de destino {0}.

Explicação: O programa de instalação não localizou espaço suficiente no diretório de destino.

Resposta do Usuário: Verifique se o diretório indicado possui espaço alocado suficiente e se pode ser acessado pelo ID de usuário usado pelo programa de instalação.

CIYBA0230I Versão da Linha de Comandos IOC: {0}

Explicação: Esta mensagem tem apenas propósitos informativos.

Resposta do Usuário: Nenhuma ação é necessária.

CIYBA0231I Importação de topologia "{0}" bem-sucedida

Explicação: Esta mensagem tem apenas propósitos informativos.

Resposta do Usuário: Nenhuma ação é necessária.

CIYBA0232E Nome da topologia "{0}" não foi localizado na pasta ../topologia

Explicação: O programa de instalação não conseguiu localizar a topologia indicada na pasta ../topologia.

Resposta do Usuário: Verifique se o arquivo de

topologia existe na pasta ../topologia e se ele está em um formato XML válido.

CIYBA0233I Topologia atual é "{0}".

Explicação: Esta mensagem tem apenas propósitos informativos.

Resposta do Usuário: Nenhuma ação é necessária.

CIYBA0234E ANT_HOME não está configurado ou está configurado incorretamente. Configure ANT_HOME.

Explicação: O programa de instalação encontrou um problema na variável de ambiente do ANT_HOME.

Resposta do Usuário: Verifique se a variável ANT_HOME está configurada para uma versão de ANT válida.

CIYBA0237E ID de componente "{0}" é inválido.

Explicação: O programa de instalação localizou um ID de componente incorreto no arquivo de topologia.

Resposta do Usuário: Verifique se o ID de componente existe e se está corretamente nomeado no arquivo de topologia.

CIYBA0238E Ação "{0}" para ID de componente "{1}" é inválida.

Explicação: A ação indicada é incorreta para o componente atual no arquivo de topologia.

Resposta do Usuário: Verifique o arquivo de topologia e certifique-se de que a ação definida é adequada para o componente.

CIYBA0239E Se desejar mais mensagens detalhadas da operação, verifique {0}.

Explicação: O comando não foi concluído com êxito.

Resposta do Usuário: Verifique o arquivo de log indicado por {0} para ações a serem tomadas.

CIYBA0240I Comando concluído com sucesso.

Explicação: Esta mensagem tem apenas propósitos informativos.

Resposta do Usuário: Nenhuma ação é necessária.

CIYBA0241E Falha no comando :

Explicação: O comando exibido falhou.

Resposta do Usuário: A ação a ser tomada dependerá do comando que falhou. Revise o comando e os logs para determinar a causa da falha.

CIYBA0242E Remova o ".xml" do parâmetro "{0}".

Explicação: O parâmetro mostrado inclui a extensão de arquivo .xml.

Resposta do Usuário: Parâmetros de nome de arquivo XML não devem incluir a extensão .xml. Remova o .xml do parâmetro e tente novamente o comando.

CIYBA0243E Variáveis de ambiente IOP_CIPHER_ALG ou IOP_CIPHER_KEYSIZE configuradas incorretamente. Configure JCE apropriados compatíveis com os valores."

Explicação: O programa de instalação não pôde identificar um valor correto para a cifra usada na criptografia.

Resposta do Usuário: Verifique se os valores de ambiente CIPHER_ALG e IOP_CIPHER_KEYSIZE estão configurados corretamente.

CIYBA0244E "{0}" não é um parâmetro válido.

Explicação: O parâmetro indicado não é um parâmetro válido.

Resposta do Usuário: Remova ou corrija o parâmetro e tente novamente o comando.

CIYBA0245E parâmetro "-{0}" ausente.

Explicação: O parâmetro indicado é necessário, mas está ausente do comando.

Resposta do Usuário: Execute novamente o comando com o parâmetro ausente.

CIYBA0249I Preparar scripts de operação.

Explicação: Esta mensagem tem apenas propósitos informativos.

Resposta do Usuário: Nenhuma ação é necessária.

CIYBA0250I Operação concluída.

Explicação: Esta mensagem tem apenas propósitos informativos.

Resposta do Usuário: Nenhuma ação é necessária.

CIYBA0251I Sequência de operações iniciada.

Explicação: Esta mensagem tem apenas propósitos informativos.

Resposta do Usuário: Nenhuma ação é necessária.

CIYBA0252I Sequência de operações concluída.

Explicação: Esta mensagem tem apenas propósitos informativos.

Resposta do Usuário: Nenhuma ação é necessária.

CIYBA0253I Fazer upload de imagens do componente [{0}] no host [{1}]

Explicação: Esta mensagem tem apenas propósitos informativos.

Resposta do Usuário: Nenhuma ação é necessária.

CIYBA0254I Instalar componente [{0}] no host [{1}]

Explicação: Esta mensagem tem apenas propósitos informativos.

Resposta do Usuário: Nenhuma ação é necessária.

CIYBA0255I Desinstalar componente [{0}] no host [{1}]

Explicação: Esta mensagem tem apenas propósitos informativos.

Resposta do Usuário: Nenhuma ação é necessária.

CIYBA0256I Iniciar componente [{0}] no host [{1}]

Explicação: Esta mensagem tem apenas propósitos informativos.

Resposta do Usuário: Nenhuma ação é necessária.

CIYBA0257I Parar componente [{0}] no host [{1}]

Explicação: Esta mensagem tem apenas propósitos informativos.

Resposta do Usuário: Nenhuma ação é necessária.

CIYBA0258I Propagar componente [{0}] no host [{1}]

Explicação: Esta mensagem tem apenas propósitos informativos.

Resposta do Usuário: Nenhuma ação é necessária.

CIYBA0259I OK

Explicação: Esta mensagem tem apenas propósitos informativos.

Resposta do Usuário: Nenhuma ação é necessária.

CIYBA0261I Tarefa(s) {0} estão em execução

Explicação: Esta mensagem tem apenas propósitos informativos.

Resposta do Usuário: Nenhuma ação é necessária.

CIYBA0262I O total de {0} tarefa(s) será executado

Explicação: Esta mensagem tem apenas propósitos informativos.

Resposta do Usuário: Nenhuma ação é necessária.

CIYBA0263I Componente de backup [{0}] no host [{1}]

Explicação: Esta mensagem tem apenas propósitos informativos.

Resposta do Usuário: Nenhuma ação é necessária.

CIYBA0264E Não é possível carregar o arquivo de configuração de log {0}.

Explicação: A função de criação de log não pode localizar o arquivo que contém os parâmetros de configuração de criação de log.

Resposta do Usuário: Verifique se o pacote de instalação foi completamente extraído e se ele é localizado em um sistema de arquivos acessível ao ID de usuário que executa o programa de instalação.

CIYBA0265E Não é possível criar manipulador de arquivo para o log.

Explicação: A função de criação de log tentou abrir um arquivo usando uma manipulação de arquivo do sistema e não conseguiu.

Resposta do Usuário: Peça para o administrador do sistema verificar o número de manipulações de arquivo disponíveis para o sistema. Certifique-se de que o sistema de arquivo do qual o pacote de instalação foi extraído não está corrompido.

CIYBA0266E O pacote de RPM requerido {0} não está instalado no servidor {1}.

Explicação: O pacote de RPM indicado não está instalado no servidor.

Resposta do Usuário: Instale o pacote de RMP suportado no servidor.

CIYBA0267E O servidor {1} não possui espaço em disco suficiente. Espaço em disco {0} é necessário.

Explicação: O servidor não tem espaço em disco suficiente ou o servidor não atende aos requisitos do sistema para espaço em disco.

Resposta do Usuário: Exclua arquivos para criar espaço disponível no servidor para que os requisitos de espaço mínimo sejam atendidos.

CIYBA0268E O servidor {1} não possui memória suficiente. {0} GB de memória é requerido.

Explicação: Não há RAM suficiente no servidor indicado. O servidor não atende aos requisitos do sistema para RAM mínima.

Resposta do Usuário: Inclua RAM no servidor.

CIYBA0269E O diretório {0} não pode ser criado no servidor {1}. O diretório já existe.

Explicação: O diretório especificado já existe no servidor.

Resposta do Usuário: Remova o diretório no servidor.

CIYBA0270E A porta tcp ip {0} já está em uso no servidor {1}. Essa é uma porta necessária e deve estar disponível antes da instalação.

Explicação: O programa ou processo já está configurado para usar a porta TCP/IP requerida no servidor.

Resposta do Usuário: Reconfigure o servidor para que a porta requerida esteja disponível. Execute a instalação novamente.

CIYBA0271E O servidor {1} não possui o Nome Completo do Host esperado. O FQH é {0}.

Explicação: O servidor não possui o nome completo do host esperado.

Resposta do Usuário: Se usar a instalação do IBM Installation Manager, insira o nome completo do host para o servidor. Se usar a instalação passo a passo, insira o nome completo do host na seção SERVERS do arquivo Propriedades da Topologia. Corrija o servidor listado na mensagem de erro.

CIYBA0272E A conexão de rede do servidor {1} para o servidor {0} está quebrada.

Explicação: Não há conectividade de rede entre os dois servidores indicados.

Resposta do Usuário: Verifique a conectividade entre os servidores. Se o problema persistir, entre em contato com o administrador de rede do sistema.

CIYBA0273E O servidor {0} está executando SELinux que não é suportado.

Explicação: SELinux não é suportado por IBM Intelligent Operations Center.

Resposta do Usuário: Instale uma versão de Linux suportada.

CIYBA0274E Um firewall ativo foi detectado no servidor {0}. Todos os firewalls devem ser desativados antes da instalação.

Explicação: O servidor possui um firewall ativo.

Resposta do Usuário: Desative o firewall no servidor durante o processo de instalação.

CIYBA0275E Não é possível localizar uma entrada DNS para o servidor {0}. A consulta DNS por IP ou nome do host falhou.

Explicação: O servidor não está configurado corretamente no DNS, ou o DNS não está funcionando adequadamente. O comando de consulta de DNS falhou para o servidor por endereço IP ou por nome do host.

Resposta do Usuário: Entre em contato com o administrador do sistema para o servidor e corrija a entrada DNS de DNS

CIYBA0276E O servidor {1} tem uma configuração de sistema que não atende aos requisitos de instalação. O número máximo de arquivos abertos [ilimitado] é inferior a {0}.

Explicação: A configuração do sistema para o número máximo de arquivos abertos não atende aos requisitos do sistema.

Resposta do Usuário: A configuração `ulimit` precisa ser modificada para o valor indicado.

CIYBA0277E A solicitação de Linux localizada não atende aos requisitos de instalação. A liberação esperada é {0}.

Explicação: O Linux instalado no servidor indicado não é suportado.

Resposta do Usuário: Instale uma versão de Linux suportada.

CIYBA0278E A distribuição de Linux localizada não atende aos requisitos. A distribuição esperada é {0}

Explicação: O Linux instalado não é suportado.

Resposta do Usuário: Instale uma distribuição de Linux suportada.

CIYBA0279E O perfil do WebSphere Application Server {0} não foi iniciado ou a conta ou senha é inválida no servidor {4}.

Explicação: O perfil WebSphere Application Server não foi iniciado ou uma tentativa foi feita para iniciá-lo com credenciais inválidas.

Resposta do Usuário: Inicie o perfil do WebSphere Application Server usando um ID e senha de usuário corretos.

CIYBA0281E O servidor {0} não possui IPv6 ativado. Ative IPv6 no servidor antes da instalação.

Explicação: O servidor indicado não possui IPv6 configurado.

Resposta do Usuário: Ative o IPv6 no servidor indicado.

CIYBA0282E Alguns dos arquivos localizados no diretório {0} no servidor de mídia estão corrompidos.

Explicação: Todo os arquivos de instalação possuem somas de verificação MD5 que precisam ser verificadas antes da instalação. A soma de verificação MD5 em alguns arquivos localizados no diretório indicado não possuem somas de verificação MD5 válidas.

Resposta do Usuário: Extraia o pacote de instalação novamente ou copie novamente os arquivos no diretório.

CIYBA0283E SSH no servidor {0} não está configurado corretamente. A autenticação de senha usando SSH é necessária, mas não está configurada no servidor.

Explicação: A configuração de SSH no servidor indicado está incorreta.

Resposta do Usuário: Reconfigure o arquivo `/etc/ssh/sshd_config` como a seguir:

- Remova todas as instruções `AllowUsers`.
- Especifique `YES` para `PermitRootLogin`.
- Especifique `YES` para `Autenticação de Senha`.

Essas mudanças permitirão que apenas usuários raiz acessem o servidor usando SSH co autenticação de senha.

CIYBA0284E {0} foi localizado como um link simbólico [soft]. Links simbólicos não são permitidos.

Explicação: Links simbólicos ou soft para arquivos ou diretórios não são suportados.

Resposta do Usuário: Remova os links simbólicos e forneça o caminho direto ou nome do arquivo.

CIYBA0285E A instância do Tivoli Directory Server {0} não foi iniciada no servidor {1}.

Explicação: A instância Tivoli Directory Server indicada precisa ser iniciada.

Resposta do Usuário: Inicie o Tivoli Directory Server.

CIYBA0286E Instância do IBM DB2 {1} não foi iniciada no servidor {1}.

Explicação: A instância do DB2 indicada não foi iniciada.

Resposta do Usuário: Inicie a instância do DB2.

CIYBA0287E WebSphere Application Server {1} no perfil {0} não foi iniciado no servidor {2}.

Explicação: O perfil WebSphere Application Server indicado não foi iniciado no servidor indicado.

Resposta do Usuário: Inicie o perfil WebSphere Application Server.

CIYBA0288E O servidor {0} não tem "host local" mapeado para 127.0.0.1.

Explicação: No arquivo host para cada servidor a entrada `host local` deve ser mapeada para `127.0.0.1`.

Resposta do Usuário: Atualize o arquivo host no servidor para mapear o valor `host local` para `127.0.0.1`.

CIYBA0289E O servidor {0} não tem Recurso de CPU suficiente. Contagem de Recurso de CPU no servidor é {1}

Explicação: O servidor não tem recursos de CPU suficientes para atender aos requisitos.

Resposta do Usuário: Inclua recursos de CPU para o servidor indicado.

CIYBA0301E Um botão foi pressionado para executar um teste, mas nenhuma propriedade correspondente foi localizada no arquivo de propriedades.

Explicação: As propriedades para o teste não foram localizadas no arquivo de propriedades.

Resposta do Usuário: Clique em **Reconfigurar**. Isso fará o programa ler o arquivo de propriedades atual no caso de mudanças serem feitas. Tente o teste novamente.

CIYBA0302E Cada teste deve ter certas propriedades. class é uma delas. Parâmetros: {0}: nome de classe {1}: nome do método {2}: número de sequência

Explicação: A definição está ausente da propriedade de classe.

Resposta do Usuário: Procure o número de sequência no arquivo de propriedades. Inclua uma propriedade de classe para o teste. Esse é o nome de classe do teste. Geralmente, esse é o nome de classe do agente de execução remoto (o código que encaminha a solicitação de teste para IopCatRemoteResponder para execução.

Por exemplo:

```
0070.classname=com.ibm.iop.cat.fw.remote.IopCatRemoter
```

CIYBA0303E Cada teste deve ter certas propriedades. Rótulo de exibição é uma delas. Parâmetros: {0}: nome de classe {1}: nome do método {2}: número de sequência

Explicação: Rótulo de exibição está ausente da definição de teste.

Resposta do Usuário: Procure o número de sequência no arquivo de propriedades. Inclua uma propriedade `displaylabel` para o teste. Esse é o texto que será exibido no botão.

CIYBA0304E Um botão foi pressionado para executar um teste, mas nenhum teste correspondente foi localizado no arquivo de propriedades.

Explicação: O arquivo de propriedades atualmente carregadas não define o teste solicitado.

Resposta do Usuário: Clique em **Reconfigurar**. O arquivo de propriedades atual será recarregado.

CIYBA0305E Um botão foi pressionado para executar um teste, mas nenhuma informação de configuração pode ser localizada para o teste.

Explicação: Informações de configuração não disponíveis para o teste.

Resposta do Usuário: Clique em **Reconfigurar**. O arquivo de propriedades atual será recarregado.

CIYBA0306E O código especificado pela classe não pôde ser localizado. Parâmetro: {0}: nome de classe (não localizado)

Explicação: O `classname` não está especificado corretamente no arquivo de propriedades ou o código não foi localizado.

Resposta do Usuário: Verifique as bibliotecas compartilhadas para o aplicativo

IopCatRemoteResponder para ver se uma ou mais bibliotecas compartilhadas estão ausentes ou não foram especificadas.

CIYBA0307E Variáveis comuns se aplicam a todos os testes. Não é permitido configurar o nome, a classe ou a depuração usando comum. Parâmetros: {0}: nome de classe {1}: nome do método {2}: sequência da chave da propriedade

Explicação: Common foi usado para configurar `name`, `class`, ou `debug`.

Resposta do Usuário: Procure pela chave e remova a linha inválida. Por exemplo, `common.name` usado para nomear todos os testes com o mesmo nome.

CIYBA0308E Uma exceção ocorreu na classe {0}, método {1}. Detalhes {2}

Explicação: Uma exceção ocorreu.

Resposta do Usuário: Examine a sequência de exceção para determinar porque o teste falhou. Isso pode ser uma falha de teste normal. Por exemplo, "Conexão recusada" geralmente significa que nenhum programa estava recebendo na porta, assim, o serviço não está em execução.

CIYBA0309E {0},{1}{0} - Teste[{2}] - Exceção: {3}

Explicação: Uma exceção de tempo de execução ocorreu no teste indicado.

Resposta do Usuário: Revise a mensagem de erro para detalhes.

CIYBA0310E Ocorreu uma exceção inesperada durante a execução deste teste.

Explicação: Ocorreu uma exceção inesperada.

Resposta do Usuário: Revise outras exceções para detalhes adicionais.

CIYBA0311I A sequência retornou de um teste de eco de diagnóstico interno. Parâmetro {0}: propriedades de entrada para o teste.

Explicação: Exibe as propriedades de entrada para o teste.

Resposta do Usuário: Essa é uma mensagem normal e não uma indicação de um erro.

CIYBA0312E O teste da Web recebeu o código de resposta HTTP esperado (nos 200's ou especificado pela propriedade `expectedRcode`). Parâmetros: {0}: nome de classe

Explicação: Indica que o teste foi bem-sucedido.

Resposta do Usuário: Nenhuma ação é necessária.

CIYBA0313E O teste da Web não recebeu o código de resposta HTTP esperado (nos 200's ou especificado pela propriedade expectedRcode). Parâmetros: {0}: nome de classe {1}: código de resposta HTTP

Explicação: Um código de resposta HTTP inesperado foi recebido.

Resposta do Usuário: Verifique a URL especificada pela propriedade hosturl com um navegador ou o comando **wget**.

CIYBA0314E A representação em sequência da resposta do teste. Parâmetros: {0}: código de resposta {1}: texto de resposta {2}: texto adicional texto específico

Explicação: Essa mensagem retorna a resposta do teste como uma sequência.

Resposta do Usuário: Nenhuma ação é necessária.

CIYBA0315E Todos os testes devem ter propriedades. Nenhuma das propriedades passou neste teste.

Explicação: Propriedades estavam ausentes da chamada de teste.

Resposta do Usuário: Esse mensagem não deve ocorrer, pois as propriedades são passadas pela estrutura. Entre em contato com o Suporte de Software IBM.

CIYBA0320E Uma sequência esperada não foi localizada nas propriedades do texto. Nome da classe {0}, texto de saída {1}

Explicação: O SSH testa o login com o servidor, executa os comandos e verifica uma sequência esperada na saída dos comandos. Nenhuma sequência esperada foi especificada nas propriedades para este teste.

Resposta do Usuário: Verifique a chave esperada para o teste. Inclua ou modifique a propriedade para especificar que uma sequência esperada seja contida na saída dos comandos especificados na propriedade `commands`.

CIYBA0322E Sequência esperada não localizada na saída. Nome da classe {0}, texto de saída {1}

Explicação: O SSH testa o logon com o servidor, executa os comandos e verifica uma sequência esperada na saída dos comandos. A sequência esperada não foi localizada na saída.

Resposta do Usuário: Verifique a chave esperada para o teste e o teste de saída. Isso pode indicar que o teste

falhou. Se o texto de saída contiver "teclado interativo não permitido", isso pode significar que o ID ou senha do usuário usado para efetuar login no servidor remoto está incorreto. Verifique as propriedades `user`, `password`, e `hostname` para o teste. A senha é um alias para uma senha no keystore.

CIYBA0323E Exceção inesperada no nome da classe {0}. Exceção: {1}

Explicação: Ocorreu uma exceção inesperada.

Resposta do Usuário: Se o texto de saída contiver "teclado interativo não permitido", isso pode significar que o ID ou senha do usuário usado para efetuar login no servidor remoto está incorreto. Verifique as propriedades `user`, `password`, e `hostname` para o teste. A senha é um alias para uma senha no keystore.

CIYBA0340E O agente de execução de teste (IopCatRemoteResponder) não conseguiu analisar os dados de JSON de entrada. Parâmetros: {0}: nome de classe {1}: nome do método {2}: dados da postagem

Explicação: A interface com o usuário e o agente de execução de teste se comunicam usando JSON. Esse erro significa que o agente de execução de teste (IopCatRemoteResponder) não conseguiu analisar os dados de JSON de entrada.

Resposta do Usuário: Examine os dados da postagem para ver se eles estão no formato JSON correto.

CIYBA0341E Uma exceção foi encontrada durante a execução do teste. Parâmetros: {0}: nome de classe {1}: nome do método {2}: sequência de exceção

Explicação: Uma exceção foi encontrada durante a execução do teste.

Resposta do Usuário: Verifique a sequência de exceção para determinar porque o teste falhou. Isso pode ser uma falha de teste normal. Por exemplo, "Conexão recusada" geralmente significa que nenhum programa estava recebendo na porta, assim, o serviço não está em execução.

CIYBA0342E O agente de execução de teste (IopCatRemoteResponder) não conseguiu enviar uma resposta de volta para a interface com o usuário. Parâmetros: {0}: nome de classe {1}: nome do método {2}: sequência de exceção

Explicação: A interface com o usuário e o agente de execução de teste se comunicam usando JSON. Esse erro significa que o agente de execução de teste (IopCatRemoteResponder) não conseguiu enviar uma resposta de volta para a interface com o usuário.

CIYBA0343E • CIYBA0404E

Resposta do Usuário: Verifique a sequência de exceção para determinar porque a resposta não pôde ser enviada. Isso pode ocorrer se o teste demorou muito e a interface com o usuário não estiver mais aguardando.

CIYBA0343E Um prefixo de chave esperado está ausente. Parâmetros: {0}: nome de classe {1}: nome do método {2}: sequência da chave da propriedade

Explicação: Todas as propriedades para um determinado teste são prefixadas com o mesmo número. Isso fornece um agrupamento, já que arquivos de propriedades não são posicionais.

Resposta do Usuário: Procure pela chave no arquivo de propriedades e inclua o prefixo apropriado. Por exemplo, o seguinte está incorreto:

```
classname      - com.ibm.lbp.cat.fw.remote.IopCatRemoter
0050_rhosturl   - https://$!APP_HOSTNAME_1:9443/IopCatRemoteResponder/IopCatRemoteResponder
0050_remoteclassname= com.ibm.lbp.cat.fw.Echo
0050_displaylabel - Internal Diagnostic (Echo REST remotet)
0050_comment    - Self diagnostic CAT check. Tests link between to CAT modules.
0050_failinfo page - cct_echo_rest_remoted_test.html
```

Deve ser:

```
0050_classname  - com.ibm.lbp.cct.fw.remote.IopCatRemoter
0050_rhosturl   - https://$!APP_HOSTNAME_1:9443/IopCatRemoteResponder/IopCatRemoteResponder
0050_remoteclassname= com.ibm.lbp.cat.fw.Echo
0050_displaylabel - Internal Diagnostic (Echo REST remotet)
0050_comment    - Self diagnostic CAT check. Tests link between to CAT modules.
0050_failinfo page - cct_echo_rest_remoted_test.html
```

CIYBA0345E Chave Inválida - O prefixo da chave não é numérico. Parâmetros: {0}: nome de classe {1}: nome do método {2}: número de sequência CCT_RESULTS_INFO = {0},{1}0 - Classe: {2} Resultados - Código de Resposta[{3}] Texto de Resposta[{4}]

Explicação: Todo teste tem um prefixo numérico que agrupa todas as propriedades para um teste determinado. O prefixo fornecido não é numérico.

Resposta do Usuário: Procure o número de sequência no arquivo de propriedades. Mude o prefixo para ser numérico e use esse mesmo prefixo para o restante das propriedades para o teste.

CIYBA0347E Ocorreu uma exceção. Parâmetros: {0}: nome de classe {1}: nome do método {2}: sequência de exceção

Explicação: Ocorreu uma exceção.

Resposta do Usuário: Examine a sequência de exceção para determinar porque o teste falhou. Isso pode ser uma falha de teste normal. Por exemplo, "Conexão recusada" geralmente significa que nenhum programa estava recebendo na porta, assim, o serviço não está em execução.

CIYBA0348E Um botão foi pressionado para executar um teste, mas nenhuma propriedade correspondente foi localizada no arquivo de propriedades.

Explicação: Nenhuma propriedade foi localizada para

o teste. O arquivo de propriedades pode ter sido alterado.

Resposta do Usuário: Clique em **Reconfigurar**. O arquivo de propriedades atual será recarregado.

CIYBA0349E O código especificado pela classe não pôde ser localizado. Parâmetro: {0}: nome de classe (não localizado)

Explicação: O `classname` não está especificado corretamente no arquivo de propriedades ou o código não foi localizado.

Resposta do Usuário: Verifique as bibliotecas compartilhadas para o `IopCatRemoteResponder` para ver se uma ou mais bibliotecas compartilhadas estão ausentes.

CIYBA0401E O nome o arquivo de modelo de propriedades IOPMGMT não foi especificado ou estava incorreto.

Explicação: O parâmetro para o arquivo de modelo de propriedades IOPMGMT está ausente.

Resposta do Usuário: Insira o nome correto para o arquivo de propriedades IOPMGMT.

CIYBA0402E O nome do arquivo de propriedades de Topologia não foi especificado ou estava incorreto.

Explicação: O parâmetro para o arquivo de propriedades de Topologia está ausente ou incorreto.

Resposta do Usuário: Insira o nome correto para o arquivo de propriedades de topologia.

CIYBA0403E O nome o arquivo de modelo de propriedades IOPMGMT não foi especificado ou estava incorreto.

Explicação: O parâmetro que especifica o arquivo de modelo de propriedades IOPMGMT está ausente.

Resposta do Usuário: Insira o nome do arquivo correto para o arquivo de propriedades de topologia.

CIYBA0404E O arquivo de propriedades de Topologia não pode ser localizado.

Explicação: O arquivo de propriedades de topologia não pode ser localizado.

Resposta do Usuário: Verifique se o arquivos de propriedades de topologia está localizado no diretório `install_home/topology` no servidor de instalação.

CIYBA0405E Senha ausente no Arquivo de Topologia para a propriedade:

Explicação: Uma senha não foi localizada no arquivo de propriedades de topologia indicado.

Resposta do Usuário: Uma senha para o arquivo de topologia é necessária. Insira uma senha para a topologia.

CIYBA0501E O parâmetro requerido para o Base Architecture Cyber Hygiene está ausente.

Explicação: O parâmetro requerido para a mídia do IBM Intelligent Operations Center Cyber Hygiene está ausente.

Resposta do Usuário: Verifique se o script do Cyber Hygiene tem o caminho correto para o local da mídia de instalação.

CIYBA0502E O parâmetro requerido para o arquivo de propriedades de Topologia está ausente.

Explicação: O parâmetro do nome do arquivo para o arquivo de propriedades de Topologia está ausente.

Resposta do Usuário: Forneça o nome do arquivo correto para o arquivo de propriedades de Topologia.

CIYBA0503E O parâmetro requerido para o diretório de destino do Base Architecture Cyber Hygiene está ausente.

Explicação: O parâmetro requerido para o diretório de destino do Cyber Hygiene está ausente.

Resposta do Usuário: Forneça o diretório de destino correto.

CIYCC0002E Corrija os seguintes erros de configuração: {0}

Explicação: Existe um erro na página de configuração Editar Sessões Compartilhadas. O erro é indicador por {0}.

Resposta do Usuário: Corrija o erro e repita o pedido.

CIYCC0005E O evento não pode ser enviado. Tente enviar o evento novamente. Se o problema persistir, entre em contato com um administrador ou helpdesk.

Explicação: Um erro de servlet do publicador ocorreu quando um usuário tentou atualizar, escalar ou cancelar um evento.

Resposta do Usuário: Peça para o administrador ou helpdesk resolver o erro de servlet do publicador.

CIYCC0006W O registro foi atualizado por outro usuário. Atualize a página para buscar o registro atualizado.

Explicação: Uma atualização solicitada pelo usuário está conflitando com outra mudança que ocorreu no servidor. Isso pode ocorrer se dois usuários tentarem mudar o estado de uma atividade ao mesmo tempo.

Resposta do Usuário: Atualize a página. A atualização feita pelo outro usuário será exibida. Depois, faça quaisquer mudanças necessárias.

CIYUI0001E A matriz JSON fornecida contém erros e não pode ser analisada.

Explicação: O usuário inseriu uma sequência JSON em uma janela na qual o script deve ser inserido, mas a sequência possui erros de sintaxe e não pode ser analisada.

Resposta do Usuário: Corrija a sequência JSON.

CIYUI0002E Evento não localizado. As propriedades do evento não podem ser exibidas.

Explicação: A solicitação para exibir as propriedades do evento falhou porque as propriedades não foram localizadas no banco de dados.

Resposta do Usuário: Atualize a página e tente novamente a solicitação.

CIYUI0004E Erro de envio dos dados do gerenciador de mapa de localização.

Explicação: Um problema ocorreu durante a configuração dos dados do gerenciador de mapa de localização.

Resposta do Usuário: Consulte mensagens adicionais para obter mais detalhes.

Mensagens adicionais da guia Classificações.

Erro de Envio de Dados

A nova classificação foi inserida no banco de dados.

Mensagens adicionais da guia Mapas de Localização.

Erro de Envio de Dados

O novo mapa de localização não foi inserido no banco de dados.

Mensagens adicionais da guia Áreas.

O identificador de área inserido não é válido. O identificador de área já existe no mapa.

O usuário está inserindo uma área no mapa que já existe no mapa.

O identificador de área inserido não é válido.

O identificador de área não é válido. Ele está em branco ou o ID da área é igual ao ID da área pai.

Os dados da área inseridos não são válidos.

Os dados da área não são válidos. O cliente deve verificar se inseriu todos os campos necessários para cada área.

O identificador de área pai não deve existir como uma área no mapa atual.

O ID da área pai inserido existe como uma área no mapa. Uma área não pode ter uma área pai que seja uma área no mapa. Ela deve estar em outro mapa.

Há referências circulares entre áreas e suas áreas pai. Remova as referências circulares.

Remova relacionamentos da área pai circulares do banco de dados IBM Intelligent Operations Center.

Erro de envio de dados.

A nova guia Áreas não foi inserida no banco de dados.

CIYUI0003I Dados enviados com sucesso.

Explicação: Esta mensagem tem apenas propósitos informativos. A mensagem indica que o banco de dados IBM Intelligent Operations Center, portlet Gerenciador de Mapa de Localização e portlet Mapa de Localização foram atualizados.

Resposta do Usuário: Nenhuma ação é necessária.

CIYUI0004I Enviado com sucesso.

Explicação: Esta mensagem tem apenas propósitos informativos. A mensagem indica que apenas a UI do portlet Gerenciador de Mapa de Localização é atualizada; mudanças não são armazenadas no banco de dados do IBM Intelligent Operations Center. Se você sair do portlet Gerenciador de Mapa de Localização sem enviar as mudanças, a atualização será cancelada.

Resposta do Usuário: Clique em **Enviar** para atualizar o banco de dados IBM Intelligent Operations Center e o portlet Mapa de Localização.

Usando Bases de Conhecimento e o Suporte IBM

Esta seção contém tópicos para o uso de bases de conhecimento, Fix Central e Suporte IBM para localizar informações sobre resolução de problemas.

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:

- Procure conteúdo usando o IBM Support Assistant Lite (ISA Lite).
O ISA Lite é uma ferramenta de software gratuita que o ajuda a responder questões e resolver problemas com os produtos de software IBM. Para instruções para o download e instalação do ISA Lite, consulte o link no final do tópico.
- 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) 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:
 - Technotes e APARs (relatório 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
 - IBM Smarter Cities Software Solutions Redbooks
- 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.
- 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.

Conceitos relacionados:

“Sobre” na página 195

Use o portlet Sobre para visualizar detalhes da versão do IBM Intelligent Operations Center e IBM Smarter Cities Software Solutions integrado que você instalou. Também é possível visualizar detalhes de quaisquer atualizações aplicadas desde sua instalação.

“Instalando e Usando IBM Support Assistant Lite” na página 303

O IBM Support Assistant Lite (ISA Lite) é uma ferramenta que coleta dados diagnósticos comuns úteis para analisar problemas gerais.

Informações relacionadas:

 Downloading IBM Support Assistant Lite for IBM Intelligent Operations Center 1.5

Obtendo Correções do Fix Central

Você pode utilizar a Central de Correções para localizar as correções recomendadas pelo Suporte IBM para vários produtos, incluindo IBM Intelligent Operations Center. Com o Fix Central, é possível procurar, selecionar, solicitar e fazer o download de correções para o seu sistema com a escolha de opções de entrega. A correção de um produto do IBM Intelligent Operations Center poderá estar disponível para resolver o problema.

Procedimento

Para localizar e instalar correções:

1. Obtenha as ferramentas necessárias para obter a correção. Se não estiver instalado, obtenha o instalador de atualização do produto. É possível fazer o download do instalador do Fix Central. Esse site fornece instruções de download, instalação e configuração para o instalador de atualização.
2. Selecione IBM Intelligent Operations Center como o produto e marque uma ou mais caixas de seleção relevantes ao problema que você deseja resolver.
3. Identifique e selecione a correção que é necessária.
4. Faça download da correção.
 - a. Abra o documento de download e siga o link na seção “Pacote de Download”.


- b. Ao fazer o download do arquivo, assegure-se de que o nome do arquivo de manutenção não esteja alterado. Esta mudança pode ser intencional ou pode ser uma mudança inadvertida causada por certos navegadores da Web ou utilitários de download.
5. Para aplicar a correção, siga as instruções na seção “Instruções de Instalação” do documento de download.
6. Opcional: Assine para receber notificações por e-mail semanais sobre correções e outras atualizações de Suporte IBM.

Tarefas relacionadas:

“Assinando Atualizações de Suporte” na página 325

É possível assinar para obter atualizações para manter-se informado sobre os produtos IBM que você usa.

Informações relacionadas:

 Ajuda do Fix Central

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. Para obter informações sobre como usar o IBM Support Assistant Lite para coletar arquivos de log do IBM Intelligent Operations Center, consulte os links no final do tópico.
3. Envie o problema para o Suporte IBM através de uma das maneiras a seguir:
 - Usando o IBM Support Assistant Lite (ISA Lite). Consulte os links no final do tópico.
 - 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.

Conceitos relacionados:

“Sobre” na página 195

Use o portlet Sobre para visualizar detalhes da versão do IBM Intelligent Operations Center e IBM Smarter Cities Software Solutions integrado que você instalou. Também é possível visualizar detalhes de quaisquer atualizações aplicadas desde sua instalação.

“Instalando e Usando IBM Support Assistant Lite” na página 303

O IBM Support Assistant Lite (ISA Lite) é uma ferramenta que coleta dados diagnósticos comuns úteis para analisar problemas gerais.

Informações relacionadas:

 Downloading IBM Support Assistant Lite for IBM Intelligent Operations Center 1.5

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

O feed RSS a seguir está disponível para o IBM Intelligent Operations Center: *IBM Intelligent Operations Center*.

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 o feed RSS do *IBM Intelligent Operations Center*, utilize as seguintes subetapas:
 - a. Abra o link IBM Intelligent Operations Center feed RSS.
 - 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 subscrever nos feeds RSS, consulte o link de feeds RSS do IBM Software Support 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).

Tarefas relacionadas:

“Obtendo Correções do Fix Central” na página 323

Você pode utilizar a Central de Correções para localizar as correções recomendadas pelo Suporte IBM para vários produtos, incluindo IBM Intelligent Operations Center. Com o Fix Central, é possível procurar, selecionar, solicitar e fazer o download de correções para o seu sistema com a escolha de opções de entrega. A correção de um produto do IBM Intelligent Operations Center poderá estar disponível para resolver o problema.

Informações Relacionados



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

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.

Conceitos relacionados:

“Ativando Rastreios e Visualizando Arquivos de Log” na página 295

Para resolver um problema no IBM Intelligent Operations Center, pode ser necessário analisar os arquivos de log em vários sistemas. Os tópicos a seguir fornecem algumas orientações sobre como acessar os arquivos de log.

“Instalando e Usando IBM Support Assistant Lite” na página 303

O IBM Support Assistant Lite (ISA Lite) é uma ferramenta que coleta dados diagnósticos comuns úteis para analisar problemas gerais.

Tarefas relacionadas:

“Executando a Ferramenta de Instalação Coleta de Informações” na página 299

Os arquivos de log são gerados enquanto o IBM Intelligent Operations Center é instalado. Uma ferramenta está disponível para reunir esses arquivos de log para análise.

Informações relacionadas:

 Downloading IBM Support Assistant Lite for IBM Intelligent Operations Center 1.5

Enviando Informações ao Suporte IBM

Para reduzir o tempo de resolução do problema, é possível enviar informações de rastreo 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 os dados diagnósticos necessários. Os dados de diagnóstico ajudam a reduzir o tempo necessário para resolver seu PMR. É possível coletar os dados diagnósticos de forma automática ou manual:
 - Colete os dados automaticamente usando o IBM Support Assistant Lite (ISA Lite). Consulte os links próximos do início do tópico.
 - Colete os dados manualmente. Para obter informações sobre os arquivos de log do IBM Intelligent Operations Center, consulte os links próximos ao início do tópico.
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`

Problemas Conhecidos e Soluções

Esta seção contém uma lista de problemas comuns de ocorrer e uma solução para cada item.

O processamento do Principal Indicador de Desempenho (KPI) Interrompido após um Período

No IBM Intelligent Operations Center, o processamento do Principal Indicador de Desempenho (KPI) é interrompido ocasionalmente depois de um período, por exemplo, durante a noite. Para obter informações sobre a resolução do problema, consulte o link no final do tópico para a nota técnica de resolução de problema *O processamento do Principal Indicador de Desempenho (KPI) é interrompido após um período de tempo*.

Portlets não Preenchidos com Dados Quando as Configurações de Segurança Mudam

Se portlets não forem preenchidos com o KPI, atividade ou dados de recurso que você espera, verifique as configurações da sua porta. Se usar o tabela de propriedades de sistema para mudar as configurações de HTTPS e não mudar as configurações da porta de acordo, haverá um problema no preenchimento dos portlets com dados.

Erro de Conexão do Relatório do Cognos

Se você receber um erro de conexão de relatório do Cognos, atualize a página.

Relatórios do Cognos Não São Exibidos Corretamente

Se relatórios do Cognos não forem exibidos corretamente quando você abrir a página do Supervisor: Relatórios ou Operador: Relatórios, atualize a página.

Se após a atualização da página os relatórios do Cognos continuarem não sendo exibidos corretamente, os clusters de servidores de aplicativos Cognos podem ter sido interrompidos. Efetue login no console administrativo do WebSphere Application Server e verifique o status dos clusters do WebSphere Application Server. Se o status de um cluster mostrar um X vermelho, selecione esse cluster e pressione **Iniciar**.

Nenhum Dado Localizado para Relatórios do Cognos

Se relatórios do Cognos não forem exibidos corretamente e você receber uma mensagem Nenhum dado localizado, os dados para seu critério de seleção podem não existir no banco de dados. Redefina o critério de seleção. Por exemplo, limpe os campos **Data de Início** e **Data de Conclusão** no relatório customizado e clique em **Atualizar**. Em seguida, copie a URL do relatório e cole no portlet Cognos.

O Relatório não é Exibido Quando Você Copia a URL do Relatório Usando o Botão URL do Relatório

Como um usuário de amostra, se você copiar a URL do relatório usando o botão **URL do Relatório** e depois acessar diretamente a página de portlet Relatórios, o relatório não será exibido. Para corrigir esse problema, pressione F5 para atualizar, e o relatório será exibido corretamente.

O Recurso Editado Não Será Exibido no Portlet do Detalhes

Se você editar um recurso no Tivoli Service Request Manager quando o Tivoli Netcool/Impact não estiver disponível, o recurso não poderá ser exibido no portlet do Detalhes. Por exemplo, se clicar com o botão direito do mouse em um evento na guia **Eventos e Incidentes**, e em seguida, clicar em **Visualizar Recursos Próximos**, o recurso editado não poderá ser exibido. Para resolver o problema, edite o recurso novamente no Tivoli Service Request Manager.

O Status de Usuários que Efetuaram logout Não Exibido Corretamente no Portlet do Contatos

O status dos usuários que efetuaram logon é exibido no portlet Contatos. Se um usuário que está conectado fechar a janela do navegador ou efetuar logoff do WebSphere Portal, o status desse usuário ainda será exibido como conectado até que a sessão expire. No entanto, nenhuma mensagem enviada a esse usuário, depois que o usuário fechou a janela do navegador ou efetuou logoff, será entregue. Consequentemente, uma mensagem de erro será entregue ao usuário que está tentando enviar a mensagem. Para assegurar que o status seja atualizado imediatamente no portlet Contatos, efetue logoff clicando em **Arquivo > Efetuar Logout**.

Selecionando Atualizar Mais de Uma Vez na Página de Relatórios do Supervisor

No Supervisor: a página de relatórios na interface com o usuário do IBM Intelligent Operations Center, ao selecionar **Atualizar** sem fazer nenhuma mudança, os campos **De Data** e **Para Data** são preenchidos com a data de hoje. Se você selecionar **Atualizar** novamente sem fazer nenhuma mudança, a mensagem Nenhum dado localizado será exibida.

Esse comportamento ocorre porque os campos **De Data** e **Para Data** são preenchidos automaticamente.

Títulos Compridos Inutilizam os Gráficos de Relatório

Títulos de evento que excedem 20 a 30 caracteres podem afetar como o relatório de gráfico de pizza **Todos os Eventos, por Título** é exibido, inutilizando o gráfico. Como os títulos de evento rotulam as seções do gráfico de pizza, e o gráfico de pizza é reduzido para acomodar os rótulos, a imagem do gráfico de pizza se torna muito pequena para ser diferenciada entre as várias seções.

Resultados Inesperados na Conversão de Fuso Horário do Navegador

Resultados inesperados na conversão de fuso horário do navegador podem ser causados por codificação de fuso horário incorreta no evento Common Alerting Protocol (CAP). Para obter mais detalhes, consulte o link no final do tópico.

Conceitos relacionados:

“Utilizando CAP para Ocorrências KPI” na página 96

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).

Informações relacionadas:

 O processamento do Principal Indicador de Desempenho (KPI) é interrompido após um período de nota técnica de resolução de problemas

Erros de Conexão ao Instalar o IBM Intelligent Operations Center

O que fazer quando uma mensagem SOAPException é emitida quando o IBM Intelligent Operations Center está sendo instalado.

A conexão com um servidor foi perdida quando uma mensagem similar à seguinte é emitida:

```
[SOAPException: faultCode=SOAP-ENV:Client; msg=Read timed out
```

Se isso ocorrer, pare e reinicie os servidores. Depois, reinicie o instalador ou tente novamente o comando de instalação.

A Rede IPv6 Não é Iniciada

Se a rede IPv6 não é iniciada em um servidor, talvez o arquivo `/etc/modprobe.conf` precise de mudanças.

Sobre Esta Tarefa

Este problema pode ocorrer ao atualizar o VMWare para o release 5.

Procedimento

1. Edite o arquivo `/etc/modprobe.conf`.

2. Altere a seguinte linha:

```
alias ipv6 off
```

para

```
# alias ipv6 off
```

3. Altere a seguinte linha:

```
options ipv6 disable=1
```

para

```
# options ipv6 disable=1
```

4. Salve o arquivo.

5. Inicie novamente o servidor.

O Tivoli Service Request Manager não Inicia

O que fazer se o Tivoli Service Request Manager não puder ser iniciado pelo Ferramenta de Controle de Plataforma e for mostrado pela ferramenta do Verificação do Sistema como em funcionamento.

Sobre Esta Tarefa

Para reiniciar o Tivoli Service Request Manager, faça o seguinte.

Procedimento

1. Pare todos os servidores usando o Ferramenta de Controle de Plataforma.
2. Encerre e reinicie o .
3. Inicie todos os serviços usando o Ferramenta de Controle de Plataforma.

Não É Possível Criar Nova Página para Interface com o Usuário

Resolva um problema que ocorre durante a criação de uma nova página se você estiver trabalhando com o Microsoft Internet Explorer 9.

Sobre Esta Tarefa

Este problema pode ocorrer durante uma tentativa de criar uma nova página a partir da página **Administração** ou de qualquer página do usuário do **Citywide**. A nova página não é carregada. Para eliminar o problema, alterne o navegador para **Visualização de Compatibilidade** temporariamente. Você deve assegurar que desativou a **Visualização de Compatibilidade** após ter criado a nova página, já que o IBM Intelligent Operations Center não suporta Visualização de Compatibilidade no Internet Explorer 8 ou Internet Explorer 9.

Procedimento

1. Abra o Internet Explorer 9.
2. Efetue logon no IBM Intelligent Operations Center como administrador.
3. Clique em **Administração > Interface com o Usuário do Portal > Gerenciar Páginas**.
4. Na barra de ferramentas da parte superior do navegador, clique em **Ferramentas**.
5. No menu, selecione **Visualização de Compatibilidade**.
6. Insira `citywide` na caixa de procura.
7. Quando a procura retornar, clique em `citywide`.
8. Clique em **Nova Página**.
9. Quando a nova página for carregada, retorne para a barra de ferramentas do navegador e cancele a seleção de **Visualização de Compatibilidade**.

Conceitos relacionados:

“Navegadores Suportados” na página 13

A interfaces de soluções do IBM Intelligent Operations Center suporta uma série de navegadores. Alguns navegadores podem ser utilizados com limitações.

Soluções Alternativas de Acessibilidade para Portlets

Há soluções alternativas para problemas de acessibilidade relacionados a alguns dos portlets IBM Intelligent Operations Center:

- No portlet do Detalhes e o portlet do Notificações, para acessar o menu pop-up, utilize os seguintes controles de teclado:

Windows

Pressione a Tecla de Menu Dedicada.

Mac Escolha a opção apropriada dependendo de você ter ou não um teclado numérico:

- Se você tiver um teclado numérico, certifique-se de que Mouse Keys esteja ativado e, em seguida, pressione Ctrl+5.
 - Se você não tiver um teclado numérico, ative o Mouse Keys e, em seguida, pressione Ctrl+I.
- Para abrir a janela Incluir Evento, no portlet do Detalhes, clique na guia **Eventos e Incidentes** ou pressione a tecla Tab; o leitor de tela lê os nomes das guias. Em seguida escolha os controles de teclado apropriados a partir da lista.

Mozilla Firefox
Ctrl+Alt+V

Safari fn+control+option+V

Internet Explorer
Ctrl+Alt+V

- No portlet do Detalhes, na janela Incluir Evento, o leitor de tela não lê os seguintes valores:
 - **Data de vigência**
 - **Horário Efetivo**
 - **Data de Início**
 - **Horário de Início**
 - **Data de Expiração**
 - **Tempo de Expiração**

Solução Alternativa de Acessibilidade para Seleção de Datas no Portlet Relatórios

No portlet Relatórios, não é possível selecionar datas a partir do calendário, utilizando o teclado.

Sobre Esta Tarefa

No portlet Relatórios, para configurar um relatório predefinido, é necessário digitar uma data ou um intervalo de datas. No entanto, o selecionador de datas do calendário não é acessível pelo teclado. O calendário é exibido, mas não é possível selecionar a data a partir do calendário que utiliza o teclado. Selecionar datas a partir do calendário funcionará apenas se você utilizar um mouse.

Para solucionar esse problema, conclua as seguintes etapas para inserir as datas manualmente, utilizando o teclado.

Procedimento

1. No portlet Relatórios, selecione o relatório predefinido ao longo da parte inferior da página e clique em **Configurar o Relatório**.
2. No campo **A Partir da Data**, insira a data em que estiver visualizando as informações. Se estiver inserindo um intervalo de data, essa data será a data de início.
3. No campo **Para a Data**, insira a última data no intervalo de datas para as informações do relatório.
4. Clique em **Visualizar o report**.

Novos Eventos Não São Exibidos no Portlet Detalhes

Se novos eventos não forem exibidos no portlet Detalhes, inúmeras etapas estarão disponíveis para a resolução do problema.

Sobre Esta Tarefa

Se a primeira etapa não resolver o problema, continue na etapa seguinte. Continue em cada etapa até o problema ser resolvido.

Procedimento

1. Verifique o status da análise de XML do IBM Intelligent Operations Center
 - a. Efetue logon no servidor de eventos como raiz e insira o comando:

```
- tail -f /opt/IBM/netcool/omnibus/log/ioc_xml.log
```
 - b. Verifique se Status da conexão OK é exibido na parte inferior do arquivo.

- c. Se uma mensagem Encerrando análise for exibida ou se a data/hora não corresponder ao atual horário do servidor, conclua as seguintes etapas:
- 1) Renomeie o log atual inserindo o seguinte comando:


```
- mv /opt/IBM/netcool/omnibus/log/ioc_xml.log
/opt/IBM/netcool/omnibus/log/old_ioc_xml.log
```
 - 2) Reinicie a análise inserindo o seguinte comando:


```
/opt/IBM/netcool/omnibus/probes/nco_p_xml -name ioc_xml -propsfile /opt/IBM/netcool/omnibus/probes/linux2x86/i
```
 - 3) Espere aproximadamente 1 minuto e insira o comando:


```
- tail -f /opt/IBM/netcool/omnibus/log/ioc_xml.log
```

Procure por Status da conexão OK. Se o status da conexão não for OK, verifique erros no arquivo. Problemas de conexão podem significar que o servidor de objeto está inativo. Consulte a etapa 2.
2. Se a análise de XML do IBM Intelligent Operations Center continuar o encerramento, conclua as etapas a seguir para verificar o status do banco de dados do Tivoli Netcool/OMNIBUS. Se a análise de XML do IBM Intelligent Operations Center não continuar o encerramento, continue na Etapa 3.
- a. Efetue logon no servidor de eventos como `ibmadmin` e insira o comando:


```
- /opt/IBM/netcool/omnibus/bin/nco_config &
```
 - b. Se for solicitada a importação de `omni.dat`, selecione **Sim** e clique em **Concluir**.
 - c. Minimize a janela do agente de processo e clique com o botão direito do mouse em **NCOMS**. Se a opção **Conectar como** estiver disponível, clique nela, conecte-se como raiz e use sua senha de topologia. Se você não vir a opção **Conectar como**, feche `nco_config` e, como `ibmadmin`, digite o seguinte comando para iniciar o servidor de objeto NCOMS:


```
- /opt/IBM/netcool/omnibus/bin/nco_objserv -name NCOMS &
```

Se o servidor de objeto NCOMS não for iniciado, abra `/opt/IBM/netcool/omnibus/var`, localize e remova o arquivo `NCOMS.pid` e digite o comando a seguir:

```
/opt/IBM/netcool/omnibus/bin/nco_objserv -name NCOMS &
```
- Nota:** Após iniciar o servidor de objeto NCOMS, você deve reiniciar a análise de XML do IBM Intelligent Operations Center. Consulte a Etapa 1 na página 332.
3. Verifique o status da Tivoli Netcool/Impact.
- a. Efetue logon no servidor de eventos em `http://EventsHost:9080/nci/login_main.jsp` como `admin`. Se não for possível efetuar logon, execute os comandos a seguir no servidor de eventos:


```
su - netcool
/opt/IBM/netcool/bin/ewas.sh start
```
 - b. Na janela **Status de Serviço**, role para baixo e verifique se os serviços a seguir estão em execução:
 - **EventProcessor**
 - **IOC_CAP_Event_Reader**
 - **IOC_Notification_Reader**

Nota: Um visto verde é exibido ao lado dos serviços que estão em execução.
 - c. Na janela **Status do Serviço**, clique no ícone **Visualizar Log** ao lado de **PolicyLogger** e verifique os erros no arquivo de log. Se você localizar erros no log, é possível visualizar detalhes do arquivo de log em `/opt/IBM/netcool/impact/log/`. Para obter mais detalhes, clique em **PolicyLogger**, configure **Nível de Log Mais Alto** como **3** e selecione as caixas de opção relevantes.
4. Verifique se os eventos estão parados em uma das filas do WebSphere MQ.
- a. Use um cliente VNC para efetuar logon no servidor de eventos e insira os seguintes comandos para abrir o WebSphere MQ Explorer:

```
xhost +
su - mqm
strmqcfg &
```

Nota: Se a página Bem-vindo for aberta, feche-a.

- b. Expanda **IBM WebSphere MQ > Gerenciadores de Filas > IOC.MC.QM > QueuesLocate** e selecione a pasta **Filas**.
- c. Na tabela **Filas**, verifique a **Profundidade da Fila Atual** de todas as filas que começam com **IOC_**. Por exemplo, **IOC_KPI_IN_INTERNAL_USE_ONLY_DO_NOT_MODIFY**.

Uma profundidade de fila maior que 0 para qualquer quantidade de tempo pode indicar um problema.

5. Verifique se os eventos de CAP atingem o banco de dados do IBM Intelligent Operations Center.
 - a. Use um cliente VNC para efetuar logon no servidor de dados e insira os comandos a seguir para abrir o DB2 Control Center:

```
xhost +
su - db2inst1
Db2cc &
```

- b. Clique em **IOCDB > tabelas**, clique com o botão direito do mouse em **Evento** no esquema **IOC_COMMON** e clique em **Abrir**. Você verá uma lista de eventos que são enviados para o sistema.
- c. Verifique se os eventos estão banco de dados.

Nota: Talvez você precise buscar mais linhas, dependendo de quantos eventos estão no sistema.

6. Para configurar o rastreamento no servidor de portal, siga estas etapas:
 - a. Efetue logon no console administrativo em `http://app-host:9060/ibm/console`, em que `app-host` é o nome completo do host do servidor de aplicativos.
 - b. Clique em **Resolução de Problemas > Logs e Rastreamento**.
 - c. Clique em **WebSphere_Portal > Alterar detalhes do nível de log**.
 - d. Clique na guia **Tempo de Execução**, cole o seguinte comando e clique em **OK**.

```
*=warning: com.ibm.iss.*=all: com.ibm.ioc.*=all
```

- e. Para visualizar um log, insira o seguinte comando:

```
cd /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal
tail -f trace.log
```

Para obter mais informações sobre a visualização de logs, consulte o link de conceito relacionado no final do tópico.

Conceitos relacionados:

“Ativando Rastreamento e Visualizando Arquivos de Log” na página 295

Para resolver um problema no IBM Intelligent Operations Center, pode ser necessário analisar os arquivos de log em vários sistemas. Os tópicos a seguir fornecem algumas orientações sobre como acessar os arquivos de log.

Mecanismo de Autenticação não Disponível

Se você receber a mensagem de erro HPDIA0119W O mecanismo de autenticação não está disponível depois de efetuar logon no WebSphere Portal, verifique o status do Tivoli Directory Server e do Proxy Tivoli Directory Server para o servidor de aplicativos.

Procedimento

1. Efetue logon no servidor de gerenciamento como `ibmadmin` e digite os seguintes comandos:

```
su - ibmadmin
cd /opt/IBM/ISP/mgmt/scripts
./iopmgmt.sh status tds topology_password
```

Se o servidor estiver em execução, será exibida uma mensagem semelhante ao seguinte exemplo:


```
Executing query command.....completed.  
IBM Tivoli Directory Server [ on ]  
Command completed successfully.
```

2. Se o servidor não estiver em execução, digite `./iopmgmt.sh start tds topology_password`
3. Se o servidor não estiver em execução após a conclusão das Etapas 1 na página 334 e 2, efetue logon no servidor de gerenciamento como `ibmadmin` e digite os seguintes comandos:

```
su - ibmadmin  
cd /opt/IBM/ISP/mgmt/scripts  
./iopmgmt.sh status tdspxyapp topology_password
```

Se o servidor estiver em execução, será exibida uma mensagem semelhante ao seguinte exemplo:

```
Executing query command.....completed.  
IBM Tivoli Directory Server [ on ]  
Command completed successfully.
```

4. Se o servidor não estiver em execução, digite `./iopmgmt.sh start tdspxyapptopology_password`

Servidor de Terceiros não Está Respondendo

Se você receber a mensagem de erro Servidor de terceiros não está respondendo depois de efetuar logon no portal do WebSphere Portal, verifique o status do WebSphere Portal.

Procedimento

1. Efetue logon no servidor de gerenciamento como `ibmadmin` e digite o seguinte comando:

```
su - ibmadmin  
cd /opt/IBM/ISP/mgmt/scripts  
./iopmgmt.sh status wpe topology_password
```

Se o portal estiver em execução, será exibida uma mensagem semelhante à seguinte:

```
Executing query command.....completed.  
IBM WebSphere Portal Extend [ on ]  
Command completed successfully.
```

2. Se o portal não estiver em execução, digite `./iopmgmt.sh start wpe topology_password`.

Nenhuma Atividade É Exibida no Portlet Minhas Atividades

Se não for possível ver nenhuma atividade no portlet Minhas Atividades, há várias causas possíveis, que são descritas nas seções a seguir.

Resolução de Problemas com Dados de Amostra

Use os dados de amostra para criar um evento e use os resultados para limitar as possíveis causas devido às quais as atividades não estão sendo exibidas.

Procedimento

1. Efetue logon na interface administrativa do IBM Intelligent Operations Center como `wpsadmin`.
2. Crie um evento “Aproximação de Furacão”:
 - a. No portlet Mapa, clique com o botão direito do mouse no mapa e clique em **Incluir Evento**.
 - b. Para **Tipo de Evento**, selecione **Aproximação de Furacão**. Os outros campos são pré-preenchidos automaticamente.
 - c. Para **Urgência**, selecione **Esperado**.
 - d. Mantenha os valores padrão para os outros parâmetros do evento e clique em **OK**.

Os parâmetros para o evento “Aproximação de Furacão” são mapeados para um procedimento padrão de operação de amostra no matriz de seleção de procedimento padrão de operação.

3. Após aproximadamente 5 minutos, verifique se uma nova atividade correspondente ao evento “Aproximação de Furacão” é exibida no portlet Minhas Atividades.

Resultados

- Se uma atividade correspondente ao evento “Aproximação de Furacão” não for exibida no portlet Minhas Atividades, o problema das atividades que não são exibidas para outro usuário pode ser devido a um problema com o Tivoli Service Request Manager.
- Se uma atividade correspondente ao evento “Aproximação de Furacão” for exibida no portlet Minhas Atividades, o problema das atividades que não são exibidas para outro usuário pode ser devido aos seguintes motivos:
 - As permissões do usuário não estão configuradas corretamente.
 - Um procedimento padrão de operação não está configurado corretamente.
 - O matriz de seleção de procedimento padrão de operação não está configurado corretamente.

Referências relacionadas:

“procedimentos padrão de operação, fluxos de trabalho de Amostra e Recursos” na página 138
Os procedimentos padrão de operação, fluxos de trabalho de amostra e recursos são fornecidos ao instalar o IBM Intelligent Operations Center Versão 1.5.

Verificando o Status do Tivoli Service Request Manager

Se nenhuma atividade for exibida no portlet Minhas Atividades quando você criar um evento usando os dados de amostra, use o procedimento a seguir para solucionar o problema do Tivoli Service Request Manager.

Antes de Iniciar

Assegure-se de que senha administrativa do Tivoli Service Request Manager tenha sido criptografada corretamente. Para obter mais informações, consulte o link no final do procedimento.

Sobre Esta Tarefa

Escolha uma das opções a seguir.

Procedimento

- Use Ferramenta de Controle de Plataforma para verificar o status do Tivoli Service Request Manager:
 1. Efetue logon no como `ibmadmin` com o comando `putty`.
 2. Acesse o diretório `opt/IBM/ISP/mgmt/scripts`.
 3. Use Ferramenta de Controle de Plataforma para obter o status do Tivoli Service Request Manager e para parar e iniciar o Tivoli Service Request Manager. Para obter mais informações sobre a execução do Ferramenta de Controle de Plataforma, consulte os links no final do procedimento.
- Alternativamente, para reiniciar manualmente o Tivoli Service Request Manager, execute as seguintes etapas:
 1. Efetue logon no como `ibmadmin` com o comando `putty`.
 2. Para parar o Tivoli Service Request Manager, insira os seguintes comandos:

```
cd /opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/bin
./stopServer.sh MXServer1 -user waswebadmin -password password
./stopNode.sh -user waswebadmin -password password
../../ctgDmgr01/bin/stopManager.sh -user waswebadmin -password password
```

em que `password` é a senha de topologia.
 3. Para iniciar o Tivoli Service Request Manager, insira os seguintes comandos:

```
cd /opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/bin
../../ctgDmgr01/bin/startManager.sh
./startNode.sh -user waswebadmin
./startServer.sh MXServer1
exit
```

Tarefas relacionadas:

“Consultando o Status dos Serviços” na página 202

O Ferramenta de Controle de Plataforma está disponível para determinar o status dos serviços do IBM Intelligent Operations Center.

“Iniciando os Serviços” na página 195

O Ferramenta de Controle de Plataforma está disponível para iniciar os serviços em execução nos servidores IBM Intelligent Operations Center.

“Parando os Serviços” na página 199

O Ferramenta de Controle de Plataforma está disponível para parar os serviços do IBM Intelligent Operations Center.

“Criptografando a Senha Administrativa do Tivoli Service Request Manager” na página 58

Utilize o procedimento a seguir para criptografar a senha administrativa do Tivoli Service Request Manager no Tivoli Netcool/Impact.

Verificando Permissões do Usuário

Verifique se um usuário tem permissão para visualizar atividades associadas a um procedimento padrão de operação.

Procedimento

1. Para abrir o portlet Procedimentos Padrão de Operação na interface de Administração do WebSphere Portal, clique em **Intelligent Operations > Ferramentas de Customização > Procedimentos Padrão de Operação**.
2. Para abrir o aplicativo Matriz de Seleção de Procedimento Padrão de Operação, clique em **Matriz de Seleção de Procedimentos Padrão de Operação**.
3. Na coluna **Nome de SoP**, localize o nome de um procedimento padrão de operação para o qual deseja verificar permissões de usuário.
4. Próximo do campo **Nome de SoP**, clique no ícone **Menu Detalhes** e clique em **Acessar Procedimento Padrão de Operação**.
5. Próximo do campo **Grupo de Proprietários**, clique no ícone **Menu Detalhes** e clique em **Acessar Grupos de Pessoas**.
6. Verifique se o usuário é membro do grupo de pessoas.

O que Fazer Depois

Se o usuário não for membro do grupo de pessoas, execute uma das ações a seguir:

- Não conceda ao usuário permissão para visualizar atividades associadas ao procedimento padrão de operação.
- Inclua o usuário no grupo de pessoas para que ele possa ver todas as atividades designadas ao grupo de pessoas.
- Inclua o usuário em outro grupo de pessoas associado ao procedimento padrão de operação.

Para obter mais informações sobre como configurar usuários, consulte o link no final da tarefa.

Tarefas relacionadas:

“Configurando Novos Usuários no Tivoli Service Request Manager” na página 126

Ao incluir um usuário no IBM Intelligent Operations Center, designe permissões e grupos de pessoas para o usuário no Tivoli Service Request Manager.

Verificando a Associação de um fluxo de trabalho com um procedimento padrão de operação

Crie um evento cujos parâmetros correspondam ao conjunto de critérios de seleção que você definiu em matriz de seleção de procedimento padrão de operação. Verifique se as atividades do fluxo de trabalho associadas são exibidas no portlet Minhas Atividades.

Sobre Esta Tarefa

Para obter mais informações sobre cada uma das etapas a seguir, consulte os links no final do procedimento.

Procedimento

1. Crie um fluxo de trabalho.
2. Crie um procedimento padrão de operação e associe ao fluxo de trabalho que você criou na etapa anterior.
3. Crie uma entrada para o procedimento padrão de operação em matriz de seleção de procedimento padrão de operação.
4. No portlet Mapa, crie um evento que corresponda aos parâmetros que você definiu em matriz de seleção de procedimento padrão de operação.
5. Verifique se as atividades do fluxo de trabalho associadas são exibidas no portlet Minhas Atividades.

O que Fazer Depois

Se nenhuma atividade for exibida no portlet Minhas Atividades, verifique se você configurou fluxo de trabalho, procedimento padrão de operação, a matriz de seleção de procedimento padrão de operação e o evento corretamente. Se a configuração estiver correta, verifique o arquivo de log de política do Tivoli Netcool/OMNIbus e os arquivos de log do Tivoli Service Request Manager.

Conceitos relacionados:

“Mapa” na página 279

Use o portlet Mapa para ver eventos e recursos em um mapa.

“Minhas Atividades” na página 284

O portlet Minhas Atividades exibe uma lista dinâmica de atividades pertencentes ao grupo do qual o usuário que está conectado à interface é membro.

Tarefas relacionadas:

“Criando fluxos de trabalho” na página 128

No Tivoli Service Request Manager, é possível criar o fluxos de trabalho que pode ser incluído como tarefas automatizadas nas atividades do procedimento padrão de operação.

“Criando procedimentos padrão de operação” na página 129

Crie um procedimento padrão de operação e designe-o a um grupo de proprietários. Os usuários são designados a um grupo de proprietários por meio da associação de um grupo de pessoas.

“Definindo Parâmetros na matriz de seleção de procedimento padrão de operação” na página 131

Na matriz de seleção de procedimento padrão de operação, defina os parâmetros de evento que determinam se um procedimento padrão de operação é selecionado para um evento específico.

Verificando os Arquivos de Log

Verifique o arquivo de log de política do Tivoli Netcool/OMNIBus e o arquivo de log do Tivoli Service Request Manager.

Procedimento

- Verifique o arquivo de log de política do Tivoli Netcool/OMNIBus:
 1. Ative o arquivo de log de política do Tivoli Netcool/OMNIBus. Para obter mais informações sobre a ativação e o uso do arquivo de log, consulte o link no final do procedimento.
 2. No arquivo de log de política do Tivoli Netcool/OMNIBus, para localizar um evento, procure por CallMaximoEnterpriseServices. O arquivo de log de política do Tivoli Netcool/OMNIBus analisa eventos por parâmetro, por exemplo, Categoria e Gravidade, e lista cada evento com seu ID de ordem de serviço associado. É possível corresponder eventos com relação ao matriz de seleção de procedimento padrão de operação. Se um evento não estiver listado no arquivo de log de política do Tivoli Netcool/OMNIBus, o motivo mais provável é que nenhum procedimento padrão de operação corresponde aos parâmetros do evento.
 3. Procure erro do servidor 500, que indica um erro do servidor Tivoli Service Request Manager. Se você vir esse erro, verifique o arquivo de log do Tivoli Service Request Manager. Consulte o link no final do procedimento.
- Verifique o arquivo de log do Tivoli Service Request Manager. Para obter mais informações sobre a ativação e o uso do arquivo de log, consulte o link no final do procedimento.

Tarefas relacionadas:

“Ativando e Visualizando Arquivos de Log do Tivoli Netcool/Impact” na página 299

“Ativando Rastreo e Visualizando Arquivos de Log para Tivoli Service Request Manager” na página 296

Dados de KPI Não São Exibidos nos Portlets Status ou Drill Down de Key Performance Indicator

Se dados de KPI não forem exibidos nos portlets Status ou Drill Down de Key Performance Indicator, siga as etapas no procedimento para resolver o problema.

Procedimento

1. Para verificar o status do IBM WebSphere Business Monitor, efetue logon no console de administração do WebSphere Application Server. Para obter mais informações sobre como acessar consoles de administração, acesse o link no final do tópico.

2. Se o IBM WebSphere Business Monitor estiver interrompido, reinicie-o. Se o IBM WebSphere Business Monitor não estiver interrompido, pare-o e depois reinicie-o. Se o problema não for resolvido, execute a etapa 3.
3. Verifique os logs do IBM WebSphere Business Monitor para investigar e resolver quaisquer problemas com o IBM WebSphere Business Monitor. Para obter mais informações sobre como verificar logs, acesse o link no final do tópico.
4. Quando todos os problemas do IBM WebSphere Business Monitor estiverem resolvidos, efetue logon no console de administração do WebSphere Application Server para reiniciar o IBM WebSphere Business Monitor.

Conceitos relacionados:

“Arquivos de Log do Servidor de aplicativos” na página 295

Utilize os procedimentos a seguir para ativar os rastreios e visualizar logs para alguns dos sistemas no servidor de aplicativos.

“Consoles de Administração” na página 203

Utilize o portlet do Consoles de Administração para administrar os serviços fornecidos pela solução.

Eventos Não São Atualizados nos Portlets Status ou Drill Down de Key Performance Indicator

Se dados do evento KPI não forem atualizados nos portlets Status ou Drill Down de Key Performance Indicator, siga as etapas no procedimento até resolver o problema.

Procedimento

1. Para confirmar se atualizações de eventos KPI estão atingindo o IBM Intelligent Operations Center, acesse o link *Novos eventos não são exibidos no portlet Details* no final do tópico e siga as etapas.
2. Confirme se os eventos estão atingindo IBM WebSphere Business Monitor.
 - a. Efetue logon no console de administração do WebSphere Application Server. Para obter mais informações sobre como acessar consoles de administração, acesse o link no final do tópico.
 - b. Clique em **Resolução de Problemas > Modelos de Monitor > Sequências de Eventos com Falha**. Exclua quaisquer eventos KPI exibidos na página.
 - c. Reinicie o IBM WebSphere Business Monitor.
 - d. Clique em **Aplicativos > Serviços de Monitor > Gerenciamento de Eventos Registrados > Ativar/Desativar Registro de Eventos** e ative a gravação de evento.
 - e. Clique em **Aplicativos > Serviços de Monitor > Gerenciamento de Eventos Registrados > Gerenciamento de Eventos**. Verifique nesta página se há pelo menos dois eventos criados para cada evento KPI que é enviado para o IBM Intelligent Operations Center.
3. Confirme se as atualizações de evento KPI estão atingindo o portlet Principais Indicadores de Desempenho. Para obter mais informações sobre o portlet Principais Indicadores de Desempenho, acesse o link no final do tópico. Se você vir valores de KPI atualizados no portlet Principais Indicadores de Desempenho, os valores serão atualizados no IBM WebSphere Business Monitor.

Conceitos relacionados:

“Consoles de Administração” na página 203

Utilize o portlet do Consoles de Administração para administrar os serviços fornecidos pela solução.

“Principais Indicadores de Desempenho” na página 168

Use o portlet Principais Indicadores de Desempenho para customizar o Key Performance Indicators (KPIs) e sua exibição hierárquica no IBM Intelligent Operations Center.

Tarefas relacionadas:

“Novos Eventos Não São Exibidos no Portlet Detalhes” na página 332

Se novos eventos não forem exibidos no portlet Detalhes, inúmeras etapas estarão disponíveis para a resolução do problema.

Capítulo 10. Referência

Esses tópicos contêm informações de referência adicionais para ajudá-lo.

Produtos e Componentes Incluídos no IBM Intelligent Operations Center

A solução do IBM Intelligent Operations Center instala uma série de produtos e componentes de software.

Os produtos e componentes de software e os servidores onde eles estão instalados são mostrados no Tabela 100.

Tabela 100. Produtos Instalados com o IBM Intelligent Operations Center

Produto	Servidor de aplicativos	servidor de dados	Servidor de eventos	Servidor de Gerenciamento
IBM WebSphere Business Monitor 7.5	instalado	não instalado	não instalado	não instalado
IBM Cognos Business Intelligence 10.1.1	instalado	não instalado	não instalado	não instalado
DB2 Enterprise Server Edition com DB2 Spatial Extender 9.7.0.5	não instalado	instalado	não instalado	instalado
Serviços de modelo semântico	não instalado	não instalado	não instalado	instalado
IBM ILOG CPLEX Optimization Studio 12.4	instalado	não instalado	não instalado	não instalado
Jazz Foundation Server (para Serviços de modelo semântico) 3.0.1	não instalado	não instalado	não instalado	instalado
Lotus Domino 8.5.3.1	não instalado	não instalado	instalado	não instalado
Lotus Sametime Standard 8.5.2 + IFR1	não instalado	não instalado	instalado	não instalado
Tivoli Access Manager for e-Business 6.1.1.4	não instalado	não instalado	não instalado	instalado
Tivoli Composite Application Manager 7.1	não instalado	não instalado	não instalado	instalado
Tivoli Directory Integrator 7.1.0.5	não instalado	não instalado	não instalado	instalado
Tivoli Directory Server 6.3.0.8	não instalado	instalado	não instalado	não instalado
Tivoli Identity Manager 5.1	não instalado	não instalado	não instalado	instalado

Tabela 100. Produtos Instalados com o IBM Intelligent Operations Center (continuação)

Produto	Servidor de aplicativos	servidor de dados	Servidor de eventos	Servidor de Gerenciamento
Tivoli Monitoring 6.2.2.1	não instalado	não instalado	não instalado	instalado
Tivoli Netcool/Impact 5.1.1.1 + IF003	não instalado	não instalado	instalado	não instalado
Tivoli Netcool/OMNIBus 7.3.1.2 e análise XML	não instalado	não instalado	instalado	não instalado
Tivoli Service Request Manager 7.2.1.2	não instalado	não instalado	instalado	não instalado
WebSphere Application Server 1.1.0.0 Feature Pack for Web 2.0 and Mobile	instalado	não instalado	não instalado	não instalado
WebSphere Application Server Network Deployment 7.0.0.21	instalado	não instalado	não instalado	instalado
WebSphere Application Server 6.1.0.29 for Tivoli Service Request Manager	não instalado	não instalado	instalado	não instalado
WebSphere Message Broker 8.0	não instalado	não instalado	instalado	não instalado
WebSphere MQ 7.0.1.7	não instalado	não instalado	instalado	não instalado
WebSphere Operational Decision Management 7.5.1 (Mecanismo de Regras)	instalado	não instalado	não instalado	não instalado
WebSphere Portal Enable 7.0.0.2	instalado	não instalado	não instalado	não instalado

Processos em Execução na Conta Raiz

Depois que o cyber hygiene for executado, alguns processos ainda deverão ser executados na conta raiz.

Os processos em execução na conta raiz podem ficar vulneráveis se um usuário ou processo puder obter privilégios de administrador por meio da escalação de privilégio. Normalmente, esse é apenas um problema para serviços que processam solicitações originadas por um usuário. As solicitações originadas pelo usuário podem conter entrada configurada de forma maliciosa que pode comprometer o servidor. Os serviços que processam solicitações do usuário são sistemas que fornecem interfaces com o usuário ou interfaces de programação de aplicativos (APIs) acessíveis.

Os daemons do Linux normalmente não estão em risco, porque geralmente eles apenas iniciam, param ou respondem a eventos do sistema bem-definidos. Em muitos casos, esses daemons devem ser executados como a conta raiz, portanto, eles podem controlar outros processos ou responder a eventos críticos do

sistema. Desde que o próprio servidor acessível pelo usuário não esteja em execução como raiz, os daemons em execução na conta raiz não são apresentados como uma exposição grave.

Com exceção do Tivoli Netcool/OMNIBus, todos os servidores do produto no IBM Intelligent Operations Center estão configurados com IDs que não possuem privilégios no sistema. O Tivoli Netcool/OMNIBus fornece serviços de monitoramento e de gerenciamento em todos os hosts e servidores IBM Intelligent Operations Center.

A Tabela 101 lista os processos que continuam sendo executados como a conta raiz após a execução do cyber hygiene.

Tabela 101. Processos do ambiente do IBM Intelligent Operations Center em execução como raiz

Servidor	Produto	Nome do Processo	Explicação
servidor de dados e Servidor de Gerenciamento	DB2	db2wdog	Esse processo daemon recebe eventos do sistema e propaga-os para diversos processos-filhos. O processo db2wdog gerencia os processos db2sync e requer nível de gerenciamento raiz.
servidor de dados e Servidor de Gerenciamento	DB2	db2chkpwd	Esse daemon autentica o ID do usuário e senha do usuário ou aplicativo que se conecta a um banco de dados. O processo db2chkpwd precisa ler o arquivo de senhas /etc/shadow.
servidor de dados e Servidor de Gerenciamento	DB2	/opt/IBM/DB2/bin/db2fmc	Esse daemon serve como um coordenador de monitoramento de falhas. Ele deve ser executado como raiz para monitorar todas as instâncias do DB2.
servidor de dados e Servidor de Gerenciamento	DB2	/usr/sbin/rcst/bin/rmcd e /usr/sbin/rcst/bin/IBM.ConfigRMd	Esses comandos gerenciam a solução de alta disponibilidade para DB2. Eles precisam de acesso a todos os bancos de dados nos servidores configurados para alta disponibilidade.
	Agentes IBM Tivoli Monitoring para Lotus Domino	kgbagent, kgbclient, kslagent	Esses agentes de monitoramento precisam ser executados como raiz para controlar a atividade do servidor Lotus Domino.
servidor de aplicativos, e Servidor de Gerenciamento	IBM HTTP Server	httpd -d, http -f	O Linux requer acesso raiz para receber em portas menores que 1024. As portas HTTP padrão são 80 a 443. O IBM Intelligent Operations Center usa a porta 82. Os processos httpd -d e http -f devem ser executados como raiz. Qualquer configuração alternativa é de responsabilidade da instalação como parte da política de segurança e da configuração de rede abrangentes.
servidor de dados	Agentes IBM Tivoli Monitoring	klzagent, kcawd	Esses são processos do agente de monitoramento e de gerenciamento. Esses processos monitoram processos e recursos do sistema operacional e do aplicativo.
servidor de aplicativos	Agentes IBM Tivoli Monitoring	klzagent, kcawd, khtagent, kynagent	Esses são processos do agente de monitoramento e de gerenciamento. Esses processos monitoram processos e recursos do sistema operacional e do aplicativo.
	Agentes IBM Tivoli Monitoring	klzagent, kcawd, khtagent, kynagent, kmcrca, kgbagent, kgbstart.sh, kgbclient, kslagent, kmqagent, /opt/IBM/ITM/JRE/1x8266/bin/java	Esses são processos do agente de monitoramento e de gerenciamento. Esses processos monitoram processos e recursos do sistema operacional e do aplicativo.
Servidor de Gerenciamento	Agentes IBM Tivoli Monitoring	cms, kdsmain, KfwServices, klzagent, kcawd, kynagent, /opt/IBM/ITM/1i6263/iw/java/jre/bin/java, /opt/IBM/ITM/1i6263/iw/java/bin/java	Esses são processos do agente de monitoramento e de gerenciamento. Esses processos monitoram processos e recursos do sistema operacional e do aplicativo.
	Tivoli Netcool/OMNIBus	/usr/ibm/common/acsi/jre/bin/java, /opt/IBM/netcool/omnibus/platform/linux2x26/bin/ncp_pad	O processo ncp_pad é o daemon do agente de processo que monitora todos os agentes de processo. O daemon requer acesso a recursos do sistema. O daemon do agente de processo não apresenta uma interface com o usuário. Ele apenas gerencia outros processos.

Exceções do Cyber Hygiene

Quando o cyber hygiene é executado, há exceções conhecidas restantes na configuração de segurança preferencial.

Uma configuração ideal não teria exceções para configurações de melhor prática. No entanto, a maioria dos sistemas possui exceções. Essas exceções não apresentam um risco significativo, mas podem ser problemáticas, se não forem entendidas. Por exemplo, alguns programas talvez precisem ser executados com o conjunto de bits **suid**.

Os administradores de segurança precisam entender as exceções para poderem verificar se seu sistema foi comprometido. Durante a varredura, os administradores de sistema podem entender as exceções desejadas em oposição ao malware.

Tabela 102. Exceções do Cyber hygiene na configuração de segurança preferencial

Vulnerabilidade	Servidor	Ocorrência	Explicação
GEN000360: GID configurado como o valor no intervalo do sistema para Linux (0-499).	servidor de dados	dasadm1	O ID do Grupo (GID) dasadm1 está configurado como 102. Esse é o grupo de administração para os IDs da instância de tempo de execução do DB2. Esse grupo é automaticamente criado quando o DB2 é instalado.

Permissões de Arquivo que Requerem Avaliação do Administrador do Sistema

O Cyber hygiene não faz mudanças para exposições em todas as permissões de arquivo e propriedade. Algumas delas devem ser avaliadas e corrigidas por administradores de sistema, pois as mudanças automatizadas podem tornar algumas funções do sistema inoperantes.

Os scripts do cyber hygiene registram informações sobre recursos possivelmente afetados. Os administradores de sistema podem revisar essas descobertas e fazer mudanças apropriadas no sistema.

Os arquivos de descobertas estão localizados no diretório `/var/BA15/CH/results` em cada servidor IBM Intelligent Operations Center. O nome do arquivo é `scanrem-combined-log-date-time.log`. O registro de data e hora indica quando o cyber hygiene foi executado.

A Tabela 103 lista vulnerabilidades e ações recomendadas que requerem revisão.

Tabela 103. Vulnerabilidades que requerem avaliação pelo administrador do sistema

STIGID	Descrição	Severidade	Recomendação
GEN001220	Arquivos, aplicativos e diretórios em diretórios do sistema devem pertencer a uma conta do sistema ou a uma conta do aplicativo.	II	Revise a propriedade do recurso e altere ou documente manualmente conforme necessário.
GEN001240	Arquivos, aplicativos e diretórios em diretórios do sistema devem pertencer a um grupo do sistema ou a um grupo de aplicativos.	II	Revise a propriedade do grupo do recurso e altere ou documente manualmente conforme necessário.
GEN001500	O diretório inicial, listado para um usuário no arquivo <code>/etc/password</code> , deve pertencer a um usuário.	II	Revise a propriedade do diretório inicial e altere manualmente a propriedade, ou documente por que ela não pode ser alterada.
GEN001520	O diretório inicial, listado para um usuário no arquivo <code>/etc/password</code> , deve pertencer ao grupo primário do usuário.	II	Revise a propriedade do grupo do diretório inicial e altere manualmente a propriedade do grupo, ou documente por que ela não pode ser alterada.
GEN001560	Os arquivos no diretório inicial, que não são arquivos de inicialização, devem ter permissões de um máximo de 750.	III	Altere as permissões se as exceções ainda não tiverem sido documentadas.

Tabela 103. Vulnerabilidades que requerem avaliação pelo administrador do sistema (continuação)

STIGID	Descrição	Severidade	Recomendação
GEN002520	Os diretórios públicos devem pertencer à conta raiz ou a um ID do usuário do aplicativo.	II	Revise a propriedade e designe conforme apropriado.
GEN002540	Os diretórios públicos devem pertencer à raiz, sys, bin ou a um grupo de aplicativos.	II	Revise a propriedade do grupo e designe conforme apropriado.

Certificações de Segurança de Produtos e Componentes

Alguns dos produtos e componentes incluídos como parte da solução do IBM Intelligent Operations Center possuem certificações de segurança.

Tabela 104. Certificações de segurança de produtos instalados com o IBM Intelligent Operations Center

Produto	Critérios comuns		FIPS 140-2		IPV6
	Liberação	Nível	Liberação	Certificado?	
IBM WebSphere Business Monitor	Nenhuma	Nenhuma	7.5	Sim	Sim
IBM Cognos Business Intelligence	10.1.1	Nenhuma	Nenhuma	Nenhuma	Sim
DB2 Enterprise Server Edition com DB2 Spatial Extender	9.7	EAL4+ALC_FLR.1	9.1 FP2	Sim	Sim
IBM HTTP Server	7.0.0.19		7.0	Sim	Sim
Lotus Domino	Nenhuma	Nenhuma	8.0.1	Sim	Sim
Lotus Sametime Standard	Nenhuma	Nenhuma	8.5	Sim	Sim
Tivoli Access Manager for e-Business	6.0 FP3	EAL3+ALC_FLR.1	6.0	Sim	Sim
Tivoli Composite Application Manager	Nenhuma	Nenhuma	Nenhuma	Nenhuma	Sim
Tivoli Directory Integrator	Nenhuma	Nenhuma	7.0	Sim	Sim
Tivoli Directory Server	6.2	EAL4+ALC_FLR.1	6.1	Sim	Sim
Tivoli Identity Manager	5.0	EAL3+ALC_FLR.1	Nenhuma	Nenhuma	Sim
Tivoli Monitoring	Nenhuma	Nenhuma	6.2.0.1	Sim	Sim
Tivoli Netcool/Impact	Nenhuma	Nenhuma	5.1	Sim	Sim
Tivoli Netcool/OMNIBus e análise XML	7.1	EAL2	Todos	Sim	Sim
Tivoli Service Request Manager	Nenhuma	Nenhuma	Todos	Sim	Sim
WebSphere Application Server Network Deployment	6.1.0.2	EAL4+ALC_FLR.1	Todos	Sim	Sim
WebSphere Application Server for Tivoli Service Request Manager	6.1.0.2	EAL4+ALC_FLR.1	Todos	Sim	Sim
WebSphere Message Broker	6.0.0.3	EAL4+ALC_FLR.2 (de)	6.1	Sim	Sim
WebSphere MQ	6.0.1.1.	EAL4+ALC_FLR.2	Todos	Sim	Sim
WebSphere Operational Decision Management (Mecanismo de Regras)	Nenhuma	Nenhuma	Nenhuma	Nenhuma	Sim
WebSphere Portal Enable	5.0	EAL2	Todos	Sim	Sim

Produtos com a certificação FIP 104-2 normalmente devido ao uso de módulos IBM Crypto for C e Java. Os números de certificados desses produtos são mostrados na Tabela 105.

Tabela 105. Certificados FIPS 140-2

Módulo	Número do Certificado
IBM Crypto for C (V8.0.0)	1433
IBM CryptoLite for Java (V4.2)	910

Tabela 105. Certificados FIPS 140-2 (continuação)

Módulo	Número do Certificado
IBM CryptoLite for C (V4.5)	899
Módulo Criptográfico IBM Java JCE 140-2	497
Módulo Criptográfico IBM Java JSSE FIPS 140-2	409
IBM SSL Lite for Java	406

Informações relacionadas:

 Critérios Comuns: <http://www.commoncriteriaportal.org/>

 Avaliações de Segurança para Produtos IBM

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:

- IBM Intelligent Operations Center Centro de Informações

Glossário

Este glossário inclui termos e definições para IBM Intelligent Operations Center.

As referências cruzadas a seguir são usadas neste glossário:

- Consulte o encaminha de um termo para um sinônimo preferencial ou de um acrônimo ou abreviação para a forma integral definida.
- Consulte também o encaminha a um termo relacionado ou contrastante.

Para visualizar glossários de outros produtos IBM, acesse www.ibm.com/software/globalization/terminology (abrir em uma nova janela).

"A" "B" na página 347 "C" na página 347 "D" na página 348 "E" na página 348 "F" na página 349 "G" na página 349 "H" na página 349 "I" na página 350 "J" na página 350 "K" na página 351 "L" na página 351 "M" na página 352 "N" na página 352 "O" na página 352 "P" na página 352 "R" na página 353 "S" na página 353 "T" na página 354 "U" na página 354 "V" na página 355 "W" na página 355 "X" na página 356

A

Abstract Syntax Notation One (ASN.1)

O padrão internacional para definir a sintaxe de dados de informações. Define diversos tipos de dados simples e especifica uma notação para referência a esses tipos e para especificação de valores desses tipos. As notações ASN.1 podem ser aplicadas sempre que necessário para definir a sintaxe abstrata das informações sem restringir de nenhuma maneira como as informações são codificadas para transmissão.

lista de controle de acesso (ACL)

Na segurança do computador, uma lista associada com um objeto que identifica todos os assuntos que podem acessar o objeto e seus direitos de acesso.

ACL Consulte lista de controle de acesso.

permissão do administrador

A autoridade concedida a um administrador para dar acesso a eles para criar, configurar e excluir recursos do portal ou usuários. Esta autoridade é concedida pela associação de um grupo de função de usuário.

KPI de agregação

Um valor de KPI que é calculado a partir de uma métrica usando uma função de agregação.

alerta Uma mensagem que sinaliza uma mudança de status de evento ou principal indicador de desempenho (KPI).

acionar de alerta

Uma mudança do valor do principal indicador de desempenho (KPI) predefinido que faz com que uma notificação de alerta seja enviada ao portlet Coordenador - Alertas.

APAR Consulte Authorized Program Analysis Report.

ASN.1 Consulte Abstract Syntax Notation One.

assíncrono

Pertencente a ocorrências que não estão sincronizadas a tempo ou não ocorrem em intervalos de tempo regulares ou previsíveis.

atributo

Uma característica ou traço de uma entidade que descreve a entidade; por exemplo, o número de telefone de um funcionário é um dos atributos do funcionário.

usuário do portal autenticado

Um usuário que é membro de um grupo dentro do WebSphere Portal autenticado com um perfil contendo uma senha e um ID do usuário.

autenticação

Um serviço de segurança que fornece prova de que um usuário de um sistema de computador é genuinamente quem essa pessoa afirma ser. Mecanismos comuns para a implementação desse serviço são senhas e assinaturas digitais.

autorização

O processo de conceder a um usuário, sistema ou processo acesso restrito ou completo a um objeto, recurso ou função.

permissão de autorização

Acesso a um portal, recurso ou dados associados com a associação de um grupo.

Authorized Program Analysis Report (APAR)

Uma solicitação de correção de um defeito em uma liberação suportada de um programa fornecido pela IBM.

B**mapa de base**

Um mapa que representa informações de referência básicas, como acidentes geográficos, estradas, marcos e limites políticos, sobre as quais outras informações temáticas são colocadas. Um mapa de base é usado para referência de localização e geralmente inclui uma rede de controle geodésico como parte de sua estrutura.

C

cache Memória usada para melhorar tempos de acesso a instruções, dados ou ambos. Dados que residem na cache de memória normalmente são uma cópia dos dados que residem em qualquer outro lugar em um armazenamento mais lento e mais barato, como um disco ou outro nó de rede.

CAP Consulte Common Alerting Protocol.

aplicativo em nuvem

Um aplicativo que é estendido para se tornar acessível por meio da Internet. Aplicativos em nuvem usam grandes datacenters e servidores poderosos que hospedam aplicativos da web e serviços da web.

Common Alerting Protocol (CAP)

Um formato geral, mas simples, para trocar alertas emergenciais e avisos públicos de todos os riscos em todos os tipos de redes.

widget comum

Um widget fornecido pela IBM que não está associado a um determinado produto. Consulte também widget.

configuração

1. A maneira em que o hardware e o software de um sistema, subsistema ou rede são organizados e interconectados.
2. O processo de descrever para um sistema os dispositivos, recursos opcionais e produtos do programa que foram instalados para que esses recursos possam ser usados. Consulte também customização.

arquivo CSV

Um arquivo de texto contendo valores separados por vírgula. Um arquivo CSV é normalmente usado para troca de arquivos entre sistemas de banco de dados e aplicativos que usam formatos diferentes.

customização

1. A modificação de uma página de portal ou portlet por um usuário. O WebSphere Portal permite que um usuário customize uma página de portal modificando o layout da página e selecionando quais portlets exibir por dispositivo. Consulte também personalização.
2. O processo de descrever mudanças opcionais em padrões de um programa de software já instalado no sistema e configurado para poder ser usado. Consulte também configuração.

D**painel**

1. Uma página da web que pode conter um ou mais widgets que representam dados de negócios graficamente.
2. Uma interface que integra dados de uma variedade de origens e fornece uma exibição unificada de informações relevantes e no contexto.

permissão de acesso a dados

Acesso a dados em uma categoria específica, por exemplo, dados médicos e de saúde pública ou dados ambientais. Esse acesso é associado com um grupo de categorias de dados.

grupo de categorias de dados

Um grupo cujos membros possuem acesso a uma categoria específica de dados, por exemplo, dados médicos e de saúde pública ou dados ambientais. A associação de um grupo de categorias de dados é designada para dar a um usuário o nível apropriado de acesso a dados. Cada usuário é incluído como um membro do grupo ou grupos apropriados.

domínio

Uma divisão individual de uma operação principal, que em geral corresponde à estrutura da organização e ao conhecimento das pessoas envolvidas. Por exemplo, a autoridade de uma cidade é dividida em departamentos que lidam com transporte, água e segurança pública.

E

EAR Consulte archive corporativo.

EJB Consulte Enterprise JavaBeans.

archive corporativo (EAR)

Um tipo especializado de arquivo JAR, definido pelo padrão Java EE, usado para implementar aplicativos Java EE em servidores de aplicativo Java EE. Um arquivo EAR contém componentes EJB, um descritor de implementação e arquivos archive web (WAR) para aplicativos da web individuais. Consulte também Java archive.

Enterprise JavaBeans (EJB)

Uma arquitetura de componente definida pela Sun Microsystems para o desenvolvimento e a implementação de aplicativos em nível corporativo orientados a objetos e distribuídos (Java EE).

ocorrência

Uma ocorrência significativa que ocorre em um determinado local e hora. Consulte também incidente.

correlação de ocorrência

O processo de analisar dados do evento para identificar padrões, causas comuns e causas raiz. A correlação de evento analisa os eventos recebidos para estados predefinidos, usando regras predefinidas e com relação a relacionamentos predefinidos.

KPI de expressão

Um KPI que possui seu valor calculado a partir dos valores de outros KPIs.

Linguagem de Marcação Extensível (XML)

Uma metalinguagem padrão para definir linguagens de marcação que é baseada em Standard Generalized Markup Language (SGML).

F

formulário de filtro

Um formulário que pode ser usado para selecionar conteúdo para ser exibido no mapa e na lista.

G

GDDM

Consulte Graphical Date Display Manager.

sistema de informações geográficas (GIS)

Um complexo de objetos, dados e aplicativos que é usado para criar e analisar informações espaciais sobre recursos geográficos.

geoespacial

Pertencente às características geográficas da Terra.

GIS Consulte sistema de informações geográficas.

Graphical Date Display Manager (GDDM)

Um sistema de computação gráfica da IBM que define e exibe texto e gráficos para saída em um monitor ou impressora.

grupo Um conjunto de usuários que pode compartilhar permissões de acesso de recursos protegidos.

H

heap Em programação Java, um bloco de memória que a Java virtual machine (JVM) usa no tempo de execução para armazenar objetos Java. A memória de heap Java é gerenciada por um coletor de lixo, que desaloca automaticamente objetos Java que não estão mais em uso.

ajuda instantânea

Texto explicativo que pode ser visualizado movendo o cursor sobre um item da interface gráfica com o usuário (GUI), tal como um ícone, campo ou sequência de texto. A ajuda instantânea pode conter rich text e links.

I**incidente**

Um evento que não faz parte da operação padrão de um serviço e causa, ou pode causar, interrupção ou redução da qualidade de serviços e produtividade do cliente. Consulte também evento.

integração

a atividade de desenvolvimento de software em que componentes de software separados são combinados em um executável inteiro.

modelo ISO

Um conjunto de regras para comunicação de dados, sancionado pela organização internacional para normatização (International Standardization Organization). Os protocolos ISO permitem que sistemas fornecidos por provedores diferentes se conectem e se comuniquem. Eles formam a base das normas de interconexão de sistemas abertos (OSI).

J

J2EE Consulte Java Platform, Enterprise Edition.

JAR Consulte Java archive.

Java archive (JAR)

Um formato de arquivo compactado para armazenar todos os recursos necessários para a instalação e a execução de um programa Java em um único arquivo. Consulte também archive corporativo.

Java EE

Consulte Java Platform, Enterprise Edition.

Java Naming and Directory Interface (JNDI)

Uma extensão para a plataforma Java que fornece uma interface padrão para nomenclatura e serviços de diretório heterogêneos.

Java Platform, Enterprise Edition (J2EE, Java EE)

Um ambiente para desenvolver e implementar aplicativos corporativos definidos pela Oracle. A plataforma Java EE consiste em um conjunto de serviços, interfaces de programação de aplicativos (APIs) e protocolos que fornecem a funcionalidade de desenvolvimento de aplicativos com multicamadas baseados na web. (Sun)

JavaScript Object Notation (JSON)

Um formato de intercâmbio de dados leve baseado em notação literal de objetos de JavaScript. JSON é uma linguagem de programação neutra, mas usa convenções de linguagens que incluem C, C++, C#, Java, JavaScript, Perl, Python.

Java virtual machine (JVM)

Uma implementação de software de um processador que executa código Java compilado (applets e aplicativos).

JNDI Consulte Java Naming and Directory Interface.

JSON Consulte JavaScript Object Notation.

JVM Consulte Java virtual machine.

K

keyhole markup language (KML)

Um formato de arquivo e gramática XML para modelagem e armazenamento de recursos geográficos como pontos, linhas, imagens e polígonos.

indicador chave de desempenho (KPI)

Uma medida quantificável projetada para controlar um dos fatores críticos de sucesso de um processo de negócios.

KML Consulte keyhole markup language.

KPI Consulte principal indicador de desempenho.

Modelo de KPI

A parte do modelo de monitor que contém os contextos KPI, que por sua vez contém os principais indicadores de desempenho e seus acionares e ocorrências associados.

política de KPI

Uma política que determina se uma ocorrência recebida é uma atualização de ocorrência do KPI, que, então, a envia para processamento para gerar uma atualização do KPI ou um alerta dependendo dos parâmetros.

L

latitude

A distância angular de um local ao norte ou ao sul da linha do equador da terra, normalmente expressa em graus e minutos.

camada

Uma sobreposição que pode ser colocada no mapa para fornecer informações geoespaciais adicionais.

LDAP Consulte Lightweight Directory Access Protocol.

Formato de Troca de Diretórios LDAP (LDIF)

Um formato de arquivo que é utilizado para descrever informações de diretório, bem como alterações que precisam ser aplicadas a um diretório, de modo que as informações de diretório possam ser trocadas entre os servidores de diretórios que utilizam o LDAP.

LDIF Consulte Formato de Troca de Diretório LDAP.

nível de serviço (LOS)

Uma medida qualitativa usada no segmento de mercado de transporte por engenheiros de tráfego para determinar a eficácia de elementos de uma infraestrutura de transporte. Essa medida descreve as condições operacionais de tráfego conforme definido no Highway Capacity Manual.

Lightweight Directory Access Protocol (LDAP)

Um protocolo aberto que usa TCP/IP para fornecer acesso a diretórios que suportam um modelo X.500 e não envolve os requisitos de recurso do Directory Access Protocol (DAP) X.500 mais complexo. Por exemplo, LDAP pode ser usado para localizar pessoas, organizações e outros recursos em um diretório da Internet ou intranet.

referência linear

Um marcador de referência de localização ao longo de uma estrada, geralmente em um acostamento, indicando sua localização ao longo de uma rota. Um exemplo de marcador é o marcador de milhagem.

mapa de localização

Um mapa ou plano contendo áreas interativas que foram definidas no IBM Intelligent Operations Center. Eventos podem ser associados a uma ou mais dessas áreas. Por exemplo, um diagrama das áreas de assento em um grande estádio esportivo pode ser definido para que os eventos que ocorrerem possam ser associados à área apropriada.

zona lógica

Um agrupamento lógico de ativos ou eventos em uma área geográfica.

longitude

A distância angular de um local ao leste ou ao oeste do meridiano em Greenwich, na Inglaterra, normalmente expressa em graus e minutos.

LOS Consulte nível de serviço.

M**instância do contexto de monitoramento**

Informações no IBM WebSphere Business Monitor que são coletadas em um momento específico dentro de um contexto de monitoramento.

modelo de monitor

Um modelo que descreve os aspectos do gerenciamento de desempenho de negócios de um modelo de negócio, incluindo eventos, métricas de negócios e principais indicadores de desempenho (KPIs) necessários para monitoramento de negócios em tempo real.

N**KPI aninhado**

Um KPI que é definido como um filho de um KPI pai.

O**ontologia**

Uma especificação formal explícita da representação de objetos, conceitos e outras entidades que podem existir em algumas áreas de interesse e os relacionamentos entre elas.

visualização das operações

Uma página da Web contendo portlets que podem cooperar para facilitar o fornecimento e a interação de informações abrangentes no nível das operações para monitorar ocorrências atuais e planejar ocorrências futuras.

OWL Consulte Web Ontology Language.

P**página**

No ambiente de portal, o elemento de interface que contém um ou mais portlets.

personalização

O processo de ativar informações alvo para usuários específicos com base em regras de negócios e informações de perfil do usuário. Consulte também customização.

plug-in

Um módulo de software instalável separadamente que inclui função a um programa, aplicativo ou interface existente.

PMR Consulte Problem Management Record.

polígono

Na função GDDM, uma sequência de linhas retas adjuntas que abrangem uma área.

portal Um ponto de acesso único e seguro a informações, aplicativos e pessoas diferentes que pode ser customizado e personalizado.

portlet

Um componente reutilizável que faz parte de um aplicativo da Web que fornece informações específicas ou serviços a serem apresentados no contexto de um portal.

Problem Management Record (PMR)

O número no mecanismo de suporte IBM que representa um incidente de serviço com um cliente.

R

RDF Consulte Resource Description Framework.

Really Simple Syndication (RSS)

Um formato de arquivo XML para webcontent sindicado que é baseado na especificação Really Simple Syndication (RSS 2.0). Os formatos de arquivo XML RSS são usados por usuários da Internet para subscrever a Web sites que forneceram feeds RSS.

Representational State Transfer (REST)

Um estilo de arquitetura de software para sistemas de hipermídia distribuídos, como World Wide Web. O termo também costuma ser usado para descrever qualquer interface simples que usa XML (ou YAML, JSON, texto simples) sobre HTTP sem uma camada de mensagem adicional como SOAP.

pacote configurável de recursos

1. Uma classe contendo texto para páginas de armazenamento. Arquivos de pacote configurável são criados e acessados de acordo com a API Java PropertyResourceBundle.
2. Uma coleção estruturada de dados que fornece um mapeamento chave-valor para dados (recursos) usada na localização de um programa. Os valores são geralmente sequências, mas podem eles mesmos ser dados estruturados.

Resource Description Framework (RDF)

Uma estrutura para representar informações na web.

REST Consulte Representational State Transfer.

RSS Consulte Really Simple Syndication.

S

Secure Sockets Layer (SSL)

Um protocolo de segurança que fornece privacidade de comunicação. Com SSL, aplicativos de cliente/servidor podem se comunicar de uma maneira projetada para evitar escuta, violação e falsificação de mensagem.

SGML

Consulte Linguagem de Marcação Generalizada Padrão.

arquivo de forma

Um formato de arquivo digital para software de sistema de informações geográficas.

conexão única (SSO)

Um processo de autenticação no qual um usuário pode acessar mais de um sistema ou aplicativo inserindo um único ID do usuário e senha.

aparência

Um elemento de uma interface gráfica com o usuário que pode ser alterado para alterar a aparência da interface sem afetar sua funcionalidade.

SOAP Um protocolo leve baseado em XML para troca de informações em um ambiente distribuído descentralizado. SOAP pode ser usado para consultar e retornar informações e chamar serviços por meio da Internet. Consulte também serviço da web.

solução

Uma combinação de produtos que aborda um problema ou projeto de cliente específico.

SPARQL

Uma linguagem de consulta para RDF usada para expressar consultas em diferentes origens de dados. A especificação W3 define a sintaxe e a semântica da linguagem de consulta SPARQL.

SSL Consulte Secure Sockets Layer.

SSO Consulte conexão única.

Linguagem de Marcação Generalizada Padrão (SGML)

Uma metalinguagem padrão para definir linguagens de marcação que é baseada no padrão ISO 8879 (SGML). SGML focaliza a estrutura das informações em vez da apresentação das informações; ela separa a estrutura e o conteúdo da apresentação. Ela também facilita a troca de documentos por meio de uma mídia eletrônica.

Procedimento Padrão de Operação

Um procedimento definindo uma sequência de atividades que são acionadas em resposta a um evento cujos parâmetros atendem a certas condições predefinidas.

Matriz de Seleção de Procedimento Padrão de Operação

Uma matriz contendo conjuntos exclusivos de parâmetros de evento que determinam se um Procedimento Padrão de Operação é iniciado para um evento específico.

tabela de propriedades de sistema

Uma tabela que armazena dados de configuração de todo o sistema para o IBM Intelligent Operations Center.

T

TAI Consulte Trust Association Interceptor.

TCP/IP

Consulte Protocolo de Controle de Transmissões/Protocolo da Internet.

tema O elemento de estilo que dá a um local uma aparência específica. O portal fornece vários temas, semelhantes a um papel de parede virtual, que podem ser escolhidos durante a criação de um local.

Protocolo de Controle de Transmissões/Protocolo da Internet (TCP/IP)

Um conjunto de protocolos de comunicação padrão de mercado não proprietário que fornece conexões de ponta a ponta confiáveis entre aplicativos em redes interconectadas de diferentes tipos.

acionador

Um mecanismo que detecta uma ocorrência e pode causar processamento adicional em resposta.

Trust Association Interceptor (TAI)

O mecanismo pelo qual a confiança é validada no ambiente do produto para cada pedido recebido pelo servidor proxy. O método de validação é concordado pelo servidor proxy e o interceptador.

U

Identificador Uniforme de Recursos (URI)

1. Um endereço exclusivo que é usado para identificar conteúdo na web, como página de texto, vídeo ou clipe musical, imagem estática ou animada ou programa. A forma mais comum de URI é o endereço de página da web, que é uma forma ou subconjunto específico de URI chamado Localizador Uniforme de Recursos (URL). Um URI normalmente descreve como acessar o recurso, o computador que contém o recurso e o nome do recurso (um nome de arquivo) no computador.
2. Uma sequência compacta de caracteres para identificar um recurso físico ou abstrato.

Localizador Uniforme de Recursos (URL)

O endereço exclusivo de um recurso de informações que está acessível em uma rede, como a Internet. A URL inclui o nome abreviado do protocolo usado para acessar o recurso de informações e as informações usadas pelo protocolo para localizar o recurso de informações.

URI Consulte Identificador Uniforme de Recursos.

URL Consulte Localizador Uniforme de Recursos.

administrador de usuários

Uma pessoa que inclui novos usuários e garante a segurança, fornecendo participação do usuário em grupos de autorização baseada em função com permissões apropriadas.

permissão de usuário

A autoridade concedida a um usuário para dar acesso a eles para visualizar e trabalhar com os recursos do portal. Esta autoridade é concedida pela associação de um grupo de funções de usuários.

perfil do usuário

Uma descrição de um usuário que inclui informações como ID do usuário, nome do usuário, senha, autoridade de acesso e outros atributos que são obtidos quando um usuário efetua login.

grupo de funções de usuários

Um grupo que designa associação para dar a um novo usuário o nível de acesso apropriado à solução. Cada novo usuário é incluído como um membro do grupo de funções apropriado. Há diferentes níveis de permissão associados a cada grupo de funções.

V**Virtual Network Computing (VNC)**

Um sistema de compartilhamento de desktop gráfico que usa protocolo Remote Frame Buffer (RFB) para controlar remotamente outro computador. Ele transmite eventos do mouse e do teclado de um computador para outro, retransmitindo as atualizações na tela gráfica de volta para a outra direção em uma rede.

VNC Consulte Virtual Network Computing.

W**Web Map Service (WMS)**

Um protocolo padrão para fornecer imagens de mapa geograficamente referenciado na Internet que são geradas por um servidor de mapa usando dados de um banco de dados do sistema de informações geográficas. A especificação foi desenvolvida e publicada pela primeira vez pelo Open Geospatial Consortium em 1999.

Web Ontology Language (OWL)

Uma linguagem que é usada para representar explicitamente o significado de termos em vocabulários e os relacionamentos entre esses termos. A OWL é destinada a ser usada quando as informações contidas em documentos precisam ser processadas por aplicativos, em oposição a situações em que o conteúdo precisa ser apresentado apenas a humanos.

serviço da Web

Um aplicativo modular autoexplicativo e autocontido que pode ser publicado, descoberto e chamado em uma rede usando protocolos de rede padrão. Tipicamente, XML é usado para identificar os dados, SOAP é usado para transferir os dados, WSDL é usado para descrever os serviços disponíveis, e UDDI é usado para listar quais serviços estão disponíveis. Consulte também SOAP, Web Service Definition Language.

Web Service Definition Language (WSDL)

Uma especificação baseada em XML para descrever serviços de rede como um conjunto de

terminais que está operando em mensagens que contêm informações orientadas por documentos ou orientadas por procedimentos. Consulte também serviço da web.

widget

Um componente da interface com o usuário reutilizável, como um botão, uma barra de rolagem, uma área de controle ou uma área de edição de texto, que pode receber entrada do teclado ou do mouse e pode se comunicar com um aplicativo ou com outro widget. Consulte também widget comum.

WMS Consulte Web Map Service.

WO Consulte ordem de serviço.

fluxo de trabalho

Um conjunto de específico específico apropriado para um conjunto de circunstâncias específico. A solução pode ser customizada para acionar fluxos de trabalho apropriados, por exemplo, conectar a sistemas de resposta de emergência.

ordem de serviço (WO)

Um registro que contém informações sobre um trabalho que deve ser executado.

WSDL

Consulte Web Service Definition Language.

X

XML Consulte Linguagem de Marcação Extensível.

esquema XML

Um mecanismo para descrever e restringir o conteúdo de arquivos XML indicando quais elementos são permitidos e em quais combinações. Esquemas XML são uma alternativa para definições de tipo de documento (DTDs) e podem ser usados para estender funcionalidade nas áreas de digitação de dados, herança e apresentação.

Informações adicionais do produto

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
- 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 Cognos Business Intelligence: <http://publib.boulder.ibm.com/infocenter/cbi/v10r1m1/index.jsp>
- Centro de informações do DB2: <http://pic.dhe.ibm.com/infocenter/db2luw/v9r7/index.jsp>

- Centro de informações do IBM ILOG CPLEX Optimization Studio: <http://pic.dhe.ibm.com/infocenter/cosinfoc/v12r4/index.jsp>
- Centro de informações do Lotus Domino: <http://publib.boulder.ibm.com/infocenter/domhelp/v8r0/index.jsp>
- Centro de informações do Lotus Notes: <http://publib.boulder.ibm.com/infocenter/domhelp/v8r0/index.jsp>
- Centro de informações do Lotus Sametime Standard: <http://publib.boulder.ibm.com/infocenter/sametime/v8r5/index.jsp>
- 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
- Centro de informações do Tivoli Access Manager: <http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/index.jsp?toc=/com.ibm.IBMDS.doc/toc.xml>
- Centro de informações do Tivoli Composite Application Manager: <http://publib.boulder.ibm.com/infocenter/tivihelp/v24r1/index.jsp>
- Centro de informações do Tivoli Directory Integrator: http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.IBMDS.doc_7.1/welcome.htm
- Centro de informações do Tivoli Directory Server: <http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/index.jsp?toc=/com.ibm.IBMDS.doc/toc.xml>
- Centro de informações do Tivoli Identity Manager : <http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/index.jsp?toc=/com.ibm.IBMDS.doc/toc.xml>
- Centro de informações do Tivoli Netcool/Impact: <http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/index.jsp?topic=/com.ibm.netcoolimpact.doc5.1.1/welcome.html>
- Centro de informações do Tivoli Netcool/OMNIBus: http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/index.jsp?topic=/com.ibm.netcool_OMNIBus.doc_7.3.1/omnibus/wip/welcome.htm
- 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
- Centro de informações do IBM WebSphere 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 WebSphere Message Broker: <http://publib.boulder.ibm.com/infocenter/wmbhelp/v8r0m0/index.jsp>
- Centro de informações do WebSphere MQ: <http://publib.boulder.ibm.com/infocenter/wmqv7/v7r1/index.jsp>
- Centro de informações do WebSphere Operational Decision Management: <http://pic.dhe.ibm.com/infocenter/dmanager/v7r5/index.jsp>

Redbooks

- Domínio Redbooks: <http://www.redbooks.ibm.com/>

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/>

Conceitos relacionados:

“Público-Alvo” na página 1

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.

Aviso de Copyright e Marcas Registradas

Aviso de Copyright

© Copyright IBM Corporation 2011, 2012. Todos os direitos reservados. Deve ser usado somente de acordo com um contrato de licença da IBM. Nenhuma parte desta publicação deve ser reproduzida, transmitida, transcrita, armazenada em sistemas para recuperação posterior ou convertidas em nenhuma linguagem de computador, em qualquer formato ou de qualquer maneira, sejam elas eletrônicas, mecânicas, magnéticas, óticas, químicas, manuais ou de outra maneira sem permissão escrita por parte da IBM Corporation. A IBM Corporation concede ao Cliente permissão limitada para criação de cópias impressas ou outras reproduções de qualquer documentação legível por máquina para uso pessoal do Cliente, contanto que tais reproduções apresentem o aviso de copyright da IBM Corporation. Não é concedido nenhum outro direito sob qualquer copyright sem permissão prévia, por escrito, da IBM Corporation. O documento não foi criado para produção e é fornecido “no estado em que se encontra”, sem nenhuma garantia de qualquer tipo. **Todas as garantias deste documento são excluídas, incluindo a garantia de não infração e as garantias implícitas 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

Cognos, CPLEX, IBM, WebSphere, DB2, Domino, ILOG, Lotus, Notes, Rational, Tivoli, ibm.com, Passport Advantage, Sametime, Service Request Manager, Smarter Cities e Redbooks são marcas registradas da the 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 em outros países

Linux é uma marca registrada de 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 serviços de terceiros.

Avisos

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

É possível que a IBM não ofereça os produtos, serviços ou recursos discutidos nesta publicação em outros países. Consulte seu representante IBM local para obter informações sobre os produtos e serviços atualmente disponíveis em sua área. Qualquer referência a produtos, programas ou serviços IBM não significa que apenas produtos, programas ou serviços IBM possam ser utilizados. Qualquer produto, programa ou serviço funcionalmente equivalente, que não infrinja nenhum direito de propriedade intelectual da IBM poderá ser utilizado em substituição a este produto, programa ou serviço. Entretanto, a avaliação e verificação da operação de qualquer produto, programa ou serviço não IBM são de inteira responsabilidade do Cliente.

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

Gerência de Relações Comerciais e Industriais da IBM Brasil
IBM Corporation
Botafogo
Rio de Janeiro, RJ
CEP 22290-240
CEP: 22290-240

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

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106
Japan

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

Estas informações podem conter imprecisões técnicas ou erros tipográficos. As informações contidas nesta publicação estão sujeitas a alterações periódicas. Tais alterações serão incorporadas em novas edições da publicação. A IBM pode, a qualquer momento, aperfeiçoar e/ou alterar os produtos e/ou programas descritos nesta publicação, sem aviso prévio.

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

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

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

IBM Corporation
Department T81B F6/Building 503
4205 S. Miami Boulevard
Durham NC 27709-9990
CEP 22290-240

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

O programa licenciado descrito nesta publicação e todo o material licenciado disponível são fornecidos pela IBM sob os termos do Contrato com o Cliente IBM, do Contrato de Licença de Programa Internacional IBM ou de qualquer outro contrato equivalente.

Qualquer informação sobre desempenho contida neste documento foi determinada em um ambiente controlado. Portanto, os resultados obtidos em outros ambientes operacionais poderão variar significativamente. Algumas medidas podem ter sido tomadas em sistemas de nível de desenvolvimento e não há garantia de que tais medidas sejam iguais em sistemas normalmente disponíveis. Além disso, é possível que algumas medidas tenham sido estimadas por meio de extrapolação. Os resultados reais poderão variar. Os usuários deste documento devem verificar os dados aplicáveis para seu ambiente específico.

As informações relativas a produtos não IBM foram obtidas junto aos fornecedores dos respectivos produtos, de seus anúncios publicados ou de outras fontes disponíveis publicamente. A IBM não testou esses produtos e não pode confirmar a exatidão do desempenho, compatibilidade ou qualquer outra reclamação relacionada a produtos não IBM. Dúvidas sobre os recursos de produtos não IBM devem ser encaminhadas diretamente a seus fornecedores.

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

LICENÇA DE COPYRIGHT:

Estas informações contêm programas de aplicativos de amostra no idioma de origem, ilustrando as técnicas de programação em diversas plataformas operacionais. O Cliente pode copiar, modificar e distribuir estes programas de exemplo sem a necessidade de pagar à IBM, com objetivos de desenvolvimento, utilização, marketing ou distribuição de programas aplicativos em conformidade com a interface de programação de aplicativo para a plataforma operacional para a qual os programas de exemplo são criados. Esses exemplos não foram testados completamente em todas as condições. Portanto, a IBM não pode garantir ou implicar a confiabilidade, manutenção ou função destes programas. Os programas de amostra são fornecidos "NO ESTADO EM QUE SE ENCONTRAM", sem garantia de nenhum tipo. A IBM não deve ser responsabilizada por nenhum dano decorrente do uso dos programas de amostra.

Marcas Registradas

Cognos, CPLEX, IBM, WebSphere, DB2, Domino, ILOG, Lotus, Notes, Rational, Tivoli, ibm.com, Passport Advantage, Sametime, Service Request Manager, Smarter Cities e Redbooks são marcas registradas da the 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 em outros países

Linux é uma marca registrada de 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 serviços de terceiros.

Índice Remissivo

A

avisos 358

G

glossário 346

M

marcas registradas 358

N

novos recursos
visão geral 8

Comentários do Leitor

IBM Intelligent Operations Center
IBM Intelligent Operations Center
Documentação do Produto
Versão 1 Release 5

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
Departamento de Desenvolvimento de Informações DLUA
Caixa Postal 12195
Research Triangle Park, NC
USA



Impresso no Brasil