IBM Cognos Analytics
Versão 11.0

Instalação e Configuração

©

Informações sobre o Produto

Este documento se aplica ao IBM Cognos Analytics versão 11.0.0 e pode também se aplicar a liberações subsequentes.

Direitos autorais

Índice

Capítulo 1. Preparando para Instalar 1

Revisar as Notas sobre a Liberação 1
Ações de configuração críticas a serem executadas primeiro! 1
Revise os ambientes suportados 2
Verificar Requisitos do Sistema 2
Definições de memória 4
Requisitos Java 6
Revisar as configurações de porta padrão. 7
Diretrizes para Criar o Armazenamento de Conteúdo. 8
Configurações sugeridas para criar o armazenamento de conteúdo em sistemas operacionais IBM Db2 no Linux, Windows e UNIX. 9
Configurações sugeridas para criar o armazenamento de conteúdo no IBM Db2 on z/OS 11
Configurações Sugeridas para Criar o Armazenamento de Conteúdo no Oracle. 12
Configurações Sugeridas para Criar o Armazenamento de Conteúdo no Microsoft SQL Server. 13
Configurações sugeridas para criar o armazenamento de conteúdo no servidor de banco de dados IBM Informix 14
Configurar uma conta do usuário ou uma conta do serviço de rede para o IBM Cognos Analytics 14
Configurar navegadores da web 15

Capítulo 2. Opções de Distribuição 19

Componentes do Cognos Analytics 19
Componentes do servidor 19
Componentes de modelagem 22
Componentes Necessários do Banco de Dados. 24
componentes do Cognos Mobile 24
Distribuição de Componentes 25
Componentes da Camada de Aplicativos e Content Managers em Computadores Separados 26
Consolidando Servidores para Linux no System z 28
Instalação para os componentes de modelagem opcionais 28
Considerações sobre Firewall 29
Distribuição dos Componentes do Framework Manager 30
Distribuindo Componentes do Transformer. 30
Opções de Distribuição para o Cognos Mobile. 32
Componentes do Cognos Mobile Instalados em Um Computador 33
Componentes do Cognos Mobile Instalados em Computadores Separados 33
IBM Cognos Analytics com outros produtos IBM Cognos 34
Produtos IBM Cognos que interoperam com o IBM Cognos Analytics 34

Capítulo 3. Upgrade do IBM Cognos Analytics. 37

Processo de Upgrade 37
Revisando a Documentação 39
Aplicativos de Avaliação em seu Ambiente antes do Upgrade 39
Pastas e arquivos preservados ao fazer upgrade do Cognos Analytics 40
Tarefas de Atualização. 42

Capítulo 4. Instalar e configurar os componentes do servidor 55

Sequência de Instalação para os Componentes do Servidor 57
Recomendação - instale e configure a instalação básica para instalações distribuídas 58
Modos de instalação 59
Instalando Componentes do Servidor nos Sistemas Operacionais UNIX ou Linux 59
Instalando Componentes do Servidor em Sistemas Operacionais Windows 61
Instalando e configurando o Content Manager para o repositório de conteúdo 62
Componentes ativo e em espera do Content Manager 63
Instalando o Content Manager nos Sistemas Operacionais UNIX ou Linux 64
Instalando o Content Manager nos Sistemas Operacionais Windows 65

Configure a conectividade do banco de dados para o banco de dados de armazenamento de conteúdo. . . . 66
Ações de configuração críticas a serem executadas primeiro! 72
Início do IBM Cognos Configuration 73
Definição de propriedades de conexão com o banco de dados para o armazenamento de conteúdo 74
Configuração de propriedades do ambiente para computadores com Content Manager 78
Especifique uma conexão com um servidor de e-mail 79
Ativação da segurança. 81
Início do Content Manager 82
Testar a instalação do Content Manager 82
Instalando e configurando os serviços de aplicativo 83
Instalar os componentes de serviço de aplicativo 83
Configurar a Conectividade de Banco de Dados para Bancos de Dados de Relatório 85
Início do IBM Cognos Configuration 88
Configurar propriedades do ambiente para computadores de componentes de serviço de aplicativo 89
Ativando a versão de 64 bits de um servidor de relatório 90
Iniciar os componentes de serviço de aplicativo 91
Testar os componentes de serviço de aplicativo 92

Capítulo 5. Instalar e configurar o gateway 95
Instalando o gateway do Cognos Analytics 96
Configure o Cognos Analytics com o seu servidor da web. 96
Ativando o gateway da web de 32 bits 98
Configurando URIs do dispatcher 98
Configurar o Servidor HTTP Apache ou o Servidor HTTP IBM. 100
Configurando o IBM HTTP Server V9 no Cognos Analytics 11.0.10+ 100
Configurando o WebDAV no Servidor HTTP IBM ou no Servidor HTTP Apache 104
Configurando o Servidor HTTP IBM com SSL 105
Configurando o Servidor HTTP Apache ou o Servidor HTTP IBM no Cognos Analytics 11.0.5+ 107
Configurando o Servidor HTTP Apache ou o Servidor HTTP IBM no Cognos Analytics 11.0.4 108
Configurando o Servidor HTTP Apache ou o IBM HTTP Server no Cognos Analytics 11.0.3 111
Configurar o Microsoft Internet Information Services 114
Configurando o WebDAV no IIS 114
Configurando o IIS com SSL 115
Configurando o IIS no Cognos Analytics 11.0.4 e versões mais recentes 116
Configurando o IIS no Cognos Analytics 11.0.3 121
Configurando o gateway de CGI no IIS versão 7 ou 8 124
Testando o gateway 127

Capítulo 6. Instalar e configurar componentes de modelagem opcionais 129
IBM Cognos Framework Manager 129
Requisitos do sistema para o IBM Cognos Framework Manager 130
Instalando o IBM Cognos Framework Manager 130
Configurando o IBM Cognos Framework Manager 131
Configurando variáveis para conexões de origem de dados para o Framework Manager 133
Testando a instalação do Framework Manager 135
IBM Cognos Transformer 135
Requisitos do sistema para o IBM Cognos Transformer 136
Instalando o IBM Cognos Transformer 136
Configurando o IBM Cognos Transformer 138
Comunicação entre o Transformer e o Cognos Analytics 139
Origens de dados e o Transformer 140
Testando a instalação do Transformer 142
Tarefas de Configuração Adicionais para IBM Cognos Transformer 142

Capítulo 7. Opções de Configuração 147
Alterando a versão do Java usada pelos comonentes do IBM Cognos Analytics 147
Alteração de definições de configuração padrão 149
Configurações de porta e de URI 149
Gerenciando o grupo de configurações 152
Gerenciando o servidor de configuração 154

Configuração de definições criptográficas 155
IBM Cognos Application Firewall 160
Criptografia de propriedades de arquivo temporário 162
Configuração do gateway para usar um namespace 162
Ativação e desativação de serviços 163
Configurando Fontes 163
Alterar a Fonte Padrão de Relatórios em PDF 166
Configuração de fontes integradas a relatórios em PDF 167
Saída de relatório salvo 168
Mudando o local da saída de relatório temporária 170
Mudando o local dos mapas anteriores do Gerenciador de mapas para o Relatórios 170
Ajustando o WebSphere Liberty Profile 171
Ativando replicação de sessão para serviços do Content Manager em espera 171
Usar um armazenamento de objeto externo para a saída de relatório e conjuntos de dados 172
Verifique o Acesso ao Objeto de Armazenamento Externo 173
Customizando a Impressão no Lado do Servidor para Plataformas UNIX e Linux 173
Alterar o Banco de Dados de Notificação 174
Configurações sugeridas para criar um banco de dados de notificação no IBM Db2 on z/OS 175
Criando espaços de tabela para um banco de dados de notificação no IBM Db2 for z/OS 176
Alterar as propriedades de conexão para o banco de dados de notificação 176
Mude a Conformidade Padrão de Segurança para os Armazenamentos Confiáveis do IBM Cognos. 177
Restaure Certificados Padrão Não NIST SP800-131a para Armazenamentos Confiáveis do IBM Cognos . . . 177
Remova Certificados Padrão Não NIST SP800-131a dos Armazenamentos Confiáveis do IBM Cognos 178
Configurando Componentes do IBM Cognos para Usar Outra Autoridade de Certificação 179
Comandos e exemplos de ThirdPartyCertificateTool 179
Criar Arquivos Certificate Signing Request (CSR) 181
Importar os Certificados CA nos Componentes do IBM Cognos 182
Configurar componentes do IBM Cognos para usar certificados gerados por sua CA 183
Configurando o Protocolo SSL para Componentes do IBM Cognos 184
Configurando SSL para componentes do IBM Cognos 184
Configure a Confiança Compartilhada entre Servidores IBM Cognos e Outros Servidores 186
Selecionar e Classificar Conjuntos de Cifras para Secure Socket Layer 187
Usar o protocolo secure sockets layer (SSL) para conexões com o banco de dados no IBM Cognos Configuration 188
Usando SSL para conexões com o banco de dados no IBM Cognos Configuration para o Microsoft SQL Server 189
Usando SSL para conexões com o banco de dados no IBM Cognos Configuration para um banco de dados do IBM Db2, Informix 191
Usando SSL para conexões com o banco de dados no IBM Cognos Configuration para um banco de dados Oracle 193
Protegendo origens de dados JDBC com SSL 194
Configure conexões da origem de dados JDBC para conexão única usando Kerberos 195
Criando arquivos de inicialização do Kerberos 196
Criando um SPN para o serviço de consulta 197
Criando um arquivo keytab 197
Configurando o módulo de login do Kerberos 197
Verificando a configuração do Kerberos 198
Verificando os recursos do driver JDBC. 198
Configurando conexões de origem de dados usando o Kerberos 199
Configurando um Repositório para Mensagens de Log 200
Diretrizes para Criar um Banco de Dados de Criação de Log 201
Conectividade do Banco de Dados para o Banco de Dados de Criação de Log. 202
Repositório de Mensagens de Log 204
Ativação de conexão específica do usuário 210
Alteração de definições globais 211
Personalização do suporte ao idioma na interface com o usuário 212
Personalização do suporte de moeda 212
Customizar Suporte do Código de Idioma do Conteúdo 213
Códigos do idioma do conteúdo 214
Mapeamento de códigos do idioma do produto 216
Personalização do fuso horário do servidor 217
Codificação para E-mails 217
Customizando configurações de cookies 218

Mudança da versão do endereço IP 219
Configurando a Versão IP 220
Configurando Manualmente o IBM Cognos Configuration para Iniciar com a Opção IPv6 220
Configurando o IBM Cognos Configuration para Sempre Começar com a Opção IPv6 no Windows 221
Configuração do URI de descoberta de colaboração 221
Configurando o IBM Cognos Workspace 222
Configurando Acesso ao IBM Cognos Workspace ou às suas Funções 222
Configurando Tipos MIME Suportados no Microsoft Internet Information Services 223
Criando espaços de tabela para a tarefa manual e para o banco de dados de anotação no IBM Db2 on z/OS 224
Configurando um Banco de Dados para Tarefas Manuais e Anotações 225
Configurando o IBM Cognos Workspace para Usar Dados do IBM Cognos TM1 226
Configurando o IBM Cognos Workspace para Acessar IBM Cognos TM1 Applications 229
Alterando o estilo de Objetos de Relatório no IBM Cognos Workspace 230
Acessando as Amostras do IBM Cognos Workspace 230
Configuração do roteador para testar a disponibilidade do dispatcher 230
Configurando o IBM Cognos Analytics para trabalhar com outros produtos IBM Cognos 231
Ativando Agentes e Relatórios Programados para Origens de Dados do IBM Cognos Planning Contributor 231

Capítulo 8. Configurando provedores de autenticação 233
Desativando o acesso anônimo 234
Restringindo o acesso de usuário ao namespace Cognos 235
Configurando o Lightweight Third-Party Authentication 235
Configurando o LTPA usando um namespace LDAP 236
Configurando o LTPA usando um namespace do Active Directory 238
Provedor de autenticação OpenID Connect 239
Configurando um namespace do OpenID Connect 241
Configurando Componentes do IBM Cognos para Usar o Active Directory Server 242
Configurando um namespace do Active Directory 243
Disponibilizando Propriedades de Usuário Customizadas para o Active Directory para Componentes do IBM Cognos 244
Ativação da comunicação segura para o Servidor do Active Directory 245
Inclusão ou exclusão de domínios utilizando Propriedades avançadas 245
Ativar a Conexão Única entre o Active Directory Server e os Componentes do IBM Cognos 246
Configurando o IBM Cognos para Usar Namespace IBM Cognos Series 7 250
Configurando um namespace do IBM Cognos Series 7 251
Ativando Comunicação Segura para o Servidor de Diretório Usado pelo Namespace IBM Cognos Series 7 . . 252
Ativando Conexão Única entre o IBM Cognos Series 7 e o IBM Cognos 252
Namespaces IBM Cognos Series 7 e o Plug-in de Conexão Confiável do IBM Cognos Series 7 252
Configurando o IBM Cognos para Usar um Provedor de Autenticação Customizada 255
Configuração de namespaces de autenticação customizada 255
Ocultação do namespace dos usuários durante o login 256
Configurando componentes do IBM Cognos para uso com LDAP 256
Mapeamento de LDAP 257
Configurando um Namespace LDAP 258
Configurando um namespace do LDAP para o Active Directory Server 259
Configurando um namespace LDAP para o IBM Directory Server 260
Configurando um namespace LDAP para o Novell Directory Server 261
Configurando um namespace LDAP para o Oracle Directory Server 263
Tornar propriedades de usuário customizadas para LDAP disponíveis para componentes do IBM Cognos . . 264
Ativando a comunicação segura para o servidor LDAP 264
Ative a conexão única entre o LDAP e componentes IBM Cognos 266
Operação de Substituição 267
Provedor de autenticação CA SiteMinder 267
Configurando um namespace SiteMinder 269
Configurando o IBM Cognos para Usar SAP 271
Configuração de namespaces SAP 272
Ativar Conexão Única entre SAP e IBM Cognos 273
Exclusão de provedores de autenticação 273

Capítulo 9. Manutenção do desempenho . . . 275
Métricas de desempenho do sistema . . . 275
Monitoramento das métricas do sistema externamente . . . 275
Ativação apenas de serviços obrigatórios . . . 276
Ajustando um IBM Db2 Content Store . . . 279
Ajustando os recursos de memória para o serviço do IBM Cognos . . . 280
Desempenho do Cognos Mobile . . . 280
Redução do tempo de entrega para relatórios em uma rede . . . 281
Aumento do limite de tempo assíncrono em ambiente de carregamento de uso intenso . . . 281

Capítulo 10. Configurando manualmente o IBM Cognos Analytics em sistemas operacionais UNIX e Linux . . . 283
Alterar Manualmente Definições de Configuração Padrão . . . 283
Incluindo um Componente em Sua Configuração . . . 284
Alterando as Configurações Criptografadas Manualmente . . . 285
Configurações Globais em Sistemas Operacionais UNIX e Linux . . . 286
Alterando Manualmente as Configurações Globais nos Sistemas Operacionais UNIX e Linux . . . 287
Iniciando e parando o Cognos Analytics no modo silencioso em sistemas operacionais UNIX e Linux . . . 288
Iniciando o Cognos Analytics no modo silencioso em sistemas operacionais UNIX e Linux . . . 288
Parando o Cognos Analytics no modo silencioso em sistemas operacionais UNIX e Linux . . . 289

Capítulo 11. Instalação, desinstalação e configuração não assistidas . . . 291
Use uma instalação não assistida . . . 291
Usar um arquivo de modelo de resposta para criar uma instalação Customizada ou Fácil . . . 293
Usar uma Configuração Não Assistida . . . 295
Use uma Desinstalação Não Assistida . . . 296

Capítulo 12. Desinstalando o IBM Cognos Analytics . . . 299
Desinstalar o IBM Cognos Analytics em sistemas operacionais UNIX ou Linux . . . 299
Desinstalar o IBM Cognos Analytics nos sistemas operacionais Microsoft Windows . . . 300
Recuperando-se de uma desinstalação malsucedida . . . 301

Capítulo 13. IBM Cognos Content Archival . . . 303
Configurar Arquivamento de Conteúdo . . . 305
Criando um Local do Arquivo para o Repositório do Sistema de Arquivos . . . 305
Importando as Definições de Classes Customizadas e Propriedades no IBM FileNet Content Manager . . . 306
Importando Definições e Propriedades de Classes Customizadas para o IBM Content Manager 8 . . . 306
Especificando um Tempo Disponível para Executar o Processo de Arquivamento . . . 308
Especificando o Tempo de Execução de Encadeamento . . . 308
Arquivando Formatos Selecionados de Saídas de Relatório . . . 309
Especificando quais Especificações de Relatórios Não Estão Arquivadas . . . 310

Apêndice A. Opções da Linha de Comandos do IBM Cognos Configuration . . . 311

Apêndice B. Resolução de problemas . . . 313
Resolvendo um Problema . . . 313
Procurando em Bases de Conhecimento . . . 315
Obtendo Correções . . . 316
Entrando em Contato com o Suporte IBM . . . 316
Trocando Informações com a IBM . . . 317
Assinando Atualizações de Suporte . . . 318
Arquivos de log . . . 320

Apêndice C. Avisos de descontinuação . . . 323

Apêndice D. Sobre este Manual . . . 325

Índice Remissivo . . . 327

Capítulo 1. Preparando para Instalar

Antes de instalar o IBM® Cognos Analytics, você deve configurar recursos no ambiente para que os componentes possam operar. Por exemplo, deve-se criar um banco de dados para uso como um armazenamento de conteúdo do Cognos Analytics e criar uma conta do usuário para o Cognos Analytics.

Se você usa a opção **Instalação fácil** (anteriormente **Pronto para execução!**) para instalar o Cognos Analytics (somente no Windows), não é necessário criar e configurar um banco de dados de armazenamento de conteúdo. Um banco de dados Informix já está configurado como seu armazenamento de conteúdo e o Cognos Analytics pode usá-lo agora mesmo.

Após concluir essas tarefas, continue com Capítulo 4, "Instalar e configurar os componentes do servidor", na página 55.

Revisar as Notas sobre a Liberação

Revise as Notas sobre a Liberação antes de instalar o produto. As Notas sobre a Liberação contêm as informações mais recentes sobre problemas conhecidos, atualizações de documentação e avisos de descontinuação.

As Notas sobre a Liberação estão disponíveis no IBM Cognos Analytics Knowledge Center (www.ibm.com/support/knowledgecenter/SSEP7J_11.0.0/com.ibm.swg.ba.cognos.cbi.doc/welcome.html).

Ações de configuração críticas a serem executadas primeiro!

Essas ações de configuração são críticas ao sucesso da instalação. Execute estas ações depois de instalar os componentes.

Certifique-se de que os drivers JDBC estejam no local correto

Para a liberação do IBM Cognos Analytics 11.0.x, os drivers JDBC devem ser copiados para o diretório *install_location*\drivers.

O uso de *install_location*\webapps\p2pd\WEB-INF\lib para drivers JDBC não é suportado.

Substitua o driver JSQL para Microsoft SQL Server pelo driver JDBC Microsoft

A partir do IBM Cognos Analytics versão 11.0.5, o driver JSQL para Microsoft SQL Server foi substituído pelo driver JDBC Microsoft. Você deve fazer download e colocar o arquivo JAR necessário no diretório *install_location*\drivers. Para obter informações adicionais, consulte Configuração para um armazenamento de conteúdo do Microsoft SQL Server.

Especificar a propriedade Grupo de configurações

Se você usou a instalação **Customizada** para instalar o IBM Cognos Analytics, abra o IBM Cognos Configuration e configure a propriedade **Grupo de configurações**. Para obter mais informações, consulte Gerenciando o Grupo de Configurações.

Ativar ou desativar a modelagem baseada na web

Por padrão, as conexões de origem de dados JDBC que foram criadas no IBM Cognos Administration não são expostas na interface de administração **Gerenciar** > **Servidores de dados** para uso em módulos de dados. Se desejar usar suas conexões de origem de dados existentes (atualizadas) para criar módulos de dados, você deve ativar a modelagem baseada na web nessas conexões.

Algumas origens de dados são inapropriadas para uso como origens para criar módulos de dados. Nesse caso, é possível proibir o uso de modelagem baseada na web nas conexões de origem de dados.

Para ativar ou desativar a modelagem baseada na web para suas conexões de origem de dados, execute as seguintes etapas:

1. No IBM Cognos Analytics, acesse **Gerenciar** > **Console de administração**.
2. No IBM Cognos Administration, na guia **Configuração**, selecione **Conexões de origem de dados**.
3. Localize a origem de dados e clique em sua ação **Configurar propriedades**.
4. Na guia **Conexão**, selecione ou desmarque a caixa de seleção **Permitir modelagem baseada na web**.

Revise os ambientes suportados

Para assegurar que seu produto funcione corretamente, aplique todas as correções de sistema operacional mínimas necessárias e use somente as versões suportadas de software de terceiros.

Para revisar uma lista atualizada de ambientes suportados pelos produtos do IBM Cognos Analytics, incluindo informações sobre sistemas operacionais, correções, navegadores, servidores da web, servidores de diretório, servidores de banco de dados e servidores de aplicativos, consulte a página IBM Software Product Compatibility Reports (www.ibm.com/support/docview.wss?uid=swg27047186).

Verificar Requisitos do Sistema

Use as tabelas a seguir para verificar os requisitos mínimos de hardware e software para instalar e executar componentes do IBM Cognos Analytics em um computador. Podem ser solicitados recursos adicionais para ambientes de distribuição ou de produção.

A tabela a seguir lista os requisitos de hardware e as especificações para uma única instalação do computador.

Requisitos de Hardware

Tabela 1. Requisitos de Hardware para uma Instalação em Computador Único

Exigência	Especificação
Sistema operacional	Microsoft Windows UNIX Linux
RAM	Mínimo de 10 GB. Para obter mais informações, consulte “Definições de memória” na página 4.

Tabela 1. Requisitos de Hardware para uma Instalação em Computador Único (continuação)

Exigência	Especificação
Especificações do sistema operacional	Limite do descritor de arquivos configurado para 8192 no UNIX e Linux
Espaço em disco	Um mínimo de 3,5 GB de espaço livre é necessário para instalar o software, e 5 GB de espaço livre na unidade que contém o diretório temporário usado pelos componentes IBM Cognos. Uma variável de ambiente aponta para o diretório temporário. No Windows essa variável é TMP. No UNIX e Linux, essa variável é IATEMPDIR Para todos os bancos de dados, o tamanho aumentará com o tempo. Certifique-se de ter espaço em disco suficiente para exigências futuras.
Impressora	Para garantir que os relatórios sejam impressos corretamente no Windows, o Adobe Reader requer que pelo menos uma impressora seja configurada no computador em que os Componentes da Camada de Aplicativos estão instalados. Todos os relatórios, independente do formato de impressão escolhido, são enviados como arquivos PDF temporários para o Adobe Reader para impressão.
Servidor de e-mail	Para enviar relatórios por e-mail, o sistema requer a habilidade de usar e acessar um servidor de e-mail.

Requisitos de Software

A tabela a seguir lista os requisitos e as especificações de software para uma instalação em computador único.

Tabela 2. Requisitos de Software para uma Instalação em Computador Único

Exigência	Especificação
Java™ Runtime Environment (JRE)	Um IBM JRE é fornecido como parte da instalação com o IBM Cognos Analytics em todos os sistemas operacionais.
Banco de Dados	Deve-se ter um dos bancos de dados disponíveis a seguir para armazenar os dados do IBM Cognos: • Oracle • IBM Db2 • Microsoft SQL Server • Informix A instalação Fácil (anteriormente Pronto para executar!) instala e configura um banco de dados Informix como um armazenamento de conteúdo. A conectividade TCP/IP é necessária para todos os tipos de bancos de dados.

Tabela 2. Requisitos de Software para uma Instalação em Computador Único (continuação)

Exigência	Especificação
Navegador web	Para todos os navegadores web, o seguinte deverá ser ativado: • Cookies • JavaScript Apenas para o Microsoft Internet Explorer, o seguinte deve ser ativado: • Executar os controles e plug-ins ActiveX. • Controles de script ActiveX marcados como seguros para criação de scripts. • Criação ativa de scripts. • Permissão de META REFRESH

Requisitos para visualizações de mapa

Os mapas que você cria em painéis e em relatórios usam um mapa de ladrilho baseado em nuvem e o serviço de polígono. Deve-se ter acesso à Internet de sua estação de trabalho de forma que seu navegador da web possa acessar o serviço por meio de uma conexão HTTPS.

O acesso à Internet para serviço não é necessário no servidor Cognos Analytics. O serviço fornece somente os mapas base e os polígonos. Nenhum dado do usuário é enviado para o serviço de nuvem.

Definições de memória

As configurações de memória dependem de inúmeros fatores, como nível de atividade esperado no servidor, complexidade dos aplicativos IBM Cognos, número de usuários e solicitações e tempos de resposta aceitáveis.

Se o seu ambiente suporta mais de 100 usuários nomeados, é complexa, experimenta altos períodos de picos de uso, ou inclui qualquer combinação desses fatores, considere concluir um plano de capacidade. Para obter informações adicionais, consulte IBM Cognos Analytics Services (www.ibm.com/software/analytics/cognos/services/).

Para determinar as configurações que melhor se adaptam ao seu ambiente, é aconselhado o teste de desempenho.

Use as seguintes configurações de memória como ponto de início e ajuste-as baseado no uso da memória de seu sistema.

- 2 GB para o sistema operacional de base e para um software acompanhante, como um software antivírus, de backup e de gerenciamento corporativo
- 4 GB para a JVM despachante (Content Manager ou Application Tier)
- 2 GB para o Cognos Graphics Service JVM
- 8 GB para a JVM de Serviço de Consulta/Serviço de Conjunto de Dados
- 2 GB por núcleo para os processos do servidor de relatório (BIBus)

Configurar valores de ulimit em sistemas operacionais UNIX e Linux

A configuração dos valores de ulimit adequados no sistema operacional UNIX ou Linux pode afetar o desempenho do IBM Cognos Analytics.

Por exemplo, em sistemas operacionais Linux, os problemas que são causados por configurações de ulimit de pilha incluem erros de alto uso incomum de memória de BIBusTKServerMain ou BIBusTKServerMain quando grandes relatórios são processados.

Se você estiver usando o serviço de relatórios em sistemas operacionais Linux, relatórios em execução ou processos BIBusTKServerMain inativos poderão usar toda a sua RAM disponível.

Considerando que, em sistemas operacionais UNIX, podem surgir problemas se as configurações de ulimit de pilha forem muito baixas.

Assegurar as configurações de ulimit de pilha corretas pode evitar esses problemas.

As configurações de ulimit recomendadas para uma nova instalação são como a seguir:

IBM AIX

- Tempo de CPU (segundos): ulimit -t unlimited
- Tamanho de arquivo (blocos): ulimit -f unlimited
- Tamanho máximo de memória (kbytes): ulimit -m unlimited
- Máximo de processos do usuário: ulimit -u unlimited
- Arquivos abertos: ulimit -n 8192 (valor mínimo)
- Tamanho de pilha (kbytes): ulimit -s 8192 (valor mínimo)
- Memória virtual (kbytes): ulimit -v unlimited

Oracle Solaris

- Tempo de CPU (segundos): ulimit -t unlimited
- Tamanho de arquivo (blocos): ulimit -f unlimited
- Máximo de processos do usuário: ulimit -u unlimited
- Memória (kbytes): ulimit -m unlimited
- Arquivos abertos: ulimit -n 8192 (valor mínimo)
- Tamanho de pilha (kbytes): ulimit -s 8192 (valor mínimo)
- Memória virtual (kbytes): ulimit -v unlimited

Linux (x, z e p)

- Tempo de CPU (segundos): ulimit -t unlimited
- Tamanho de arquivo (blocos): ulimit -f unlimited
- Tamanho máximo de memória (kbytes): ulimit -m unlimited
- Máximo de processos do usuário: ulimit -u unlimited
- Arquivos abertos: ulimit -n 8192 (valor mínimo)
- Tamanho de pilha (kbytes): ulimit -s unlimited
- Memória virtual (kbytes): ulimit -v unlimited

Nota: Estas configurações podem precisar ser ajustadas para seu ambiente durante o ciclo de vida do aplicativo.

Requisitos Java

Para suportar os serviços criptográficos no IBM Cognos Analytics, pode ser necessário atualizar a versão do Java ou configurar uma variável de ambiente JAVA_HOME. Dependendo dos requisitos da sua política de segurança, também poderá ser necessário instalar o arquivo de políticas Java Cryptography Extension (JCE) não restrito.

É possível usar um Java Runtime Environment (JRE) existente ou o JRE fornecido com o IBM Cognos Analytics.

Padrões Criptográficos

Os serviços criptográficos do IBM Cognos® usam um arquivo jar (Java Archive) específico, denominado `bcprov-jdknn-nnn.jar`, que deve estar no Java Runtime Environment. Esse arquivo fornece rotinas adicionais de criptografia e decriptografia que não são fornecidas como parte de uma instalação JVM (Java Virtual Machine) padrão. Para garantir a segurança, o arquivo de criptografia deve ser carregado pela JVM usando o diretório de extensões Java.

1. Acesse o diretório `install_location/jre/lib/ext`.
2. Copie o arquivo `bcprov-jdk14-145.jar` para o diretório `$JAVA_HOME/lib/ext`.

Por padrão, o IBM Cognos Analytics é configurado para suportar o padrão de segurança NIST SP800-131a. Para ser compatível com este padrão de segurança, você deve utilizar um JRE que também suporta esse padrão.

Para obter mais informações sobre as versões Java suportadas para o IBM Cognos Analytics, consulte o IBM Software Product Compatibility Reports (www.ibm.com/support/docview.wss?uid=swg27047186).

Para obter informações adicionais sobre esse padrão de segurança, consulte o IBM SDK, Java Technology Edition Knowledge Center (www.ibm.com/support/knowledgecenter/SSYKE2/welcome_javasdk_family.html).

JAVA_HOME

Configure uma variável de ambiente JAVA_HOME se desejar usar o seu próprio Java.

Certifique-se de que a versão do JRE é suportada pelos produtos IBM Cognos.

Em sistemas operacionais Microsoft Windows, se não tiver uma variável JAVA_HOME, os arquivos JRE que são fornecidos com a instalação são usados.

Para verificar se o JRE é suportado, consulte IBM Software Product Compatibility Reports (www.ibm.com/support/docview.wss?uid=swg27047186).

Arquivo de política irrestrita do JCE

Os JREs incluem um arquivo de políticas restrito que limita a determinados algoritmos criptográficos e conjuntos de cifras. Se você precisar de uma gama maior de algoritmos criptográficos e conjuntos de cifras do que a mostrada no IBM Cognos Configuration, é possível fazer o download e instalar o arquivo de políticas irrestritas JCE.

Para o Java que é fornecido pela IBM, o arquivo de políticas JCE irrestrito está disponível no Website da IBM (www14.software.ibm.com/webapp/iwm/web/preLogin.do?source = jcesdk).

Revisar as configurações de porta padrão

Após a instalação, é possível usar a ferramenta de configuração para mudar as configurações padrão do IBM Cognos Analytics. O tipo de instalação **Fácil** seleciona as configurações de porta para você.

Importante: Essas portas devem ser abertas para tráfego de entrada e saída.

Configurações de porta padrão para componentes do Cognos Analytics

A tabela a seguir lista as configurações de porta e URI padrão para o IBM Cognos Analytics.

Tabela 3. Configurações de porta padrão para componentes do Cognos Analytics

Configuração	Valor padrão	Descrição
URI do Content Manager	`http://localhost:9300/p2pd/servlet`	O URI do Content Manager.
URI do gateway	`http://computer_name:port/bi/v1/disp`	O URI para o gateway.
URI do dispatcher (Interno, Externo)	`http://localhost:9300/p2pd/servlet/dispatch`	O URI para o dispatcher.
URI do Dispatcher para Aplicativos Externos	`http://localhost:9300/bi/v1/disp`	O URI para o dispatcher.
Porta do servidor de log	9362	A porta utilizada pelo servidor de log local.
Porta de sincronização de membros	4300	A porta local usada para comunicação de rede que transfere e sincroniza informações de configuração de um servidor para outro.
Porta de coordenação de membro	5701	A porta local usada para comunicação de rede para coordenação de grupo. Esta porta é usada para descobrir e associar um grupo e para manter uma lista atualizada de membros do grupo de configurações.
Porta de serviço do conjunto de dados	9301	A porta local que é usada para comunicação entre processos. Essa porta é designada quando o Cognos Analytics é iniciado pela primeira vez. O número da porta é baseado na porta do dispatcher do Cognos Analytics mais 1. Por exemplo, 9300 + 1 = 9301.

Para obter mais informações, consulte “Configurações de porta e de URI” na página 149.

Diretrizes para Criar o Armazenamento de Conteúdo

O armazenamento de conteúdo é um banco e dados que o Content Manager usa para armazenar dados de configuração globais, definições globais (como os formatos de idioma e moeda exibidos na interface com o usuário), conexões a origens de dados e conteúdo específico de produtos. É necessário usar um dos bancos de dados de nível empresarial suportados como o armazenamento de conteúdo em um ambiente de produção.

Modelos de projeto e arquivos de log não são guardados no armazenamento de conteúdo.

Crie o armazenamento de conteúdo para que seja possível usar seu produto do IBM Cognos Analytics. Se você usar a instalação Fácil (anteriormente Pronto para executar!) , de que o Informix esteja instalado e configurado para ser usado como seu armazenamento de conteúdo.

Se você estiver usando o IBM Db2 para o seu armazenamento de conteúdo, será possível gerar um DDL para permitir que seu administrador de banco de dados crie um banco de dados do Db2 adequado para o armazenamento de conteúdo. Para obter mais informações, consulte “Gerando um arquivo de script para criar um banco de dados para um armazenamento de conteúdo do IBM Db2” na página 67.

Propriedades do Banco de Dados

Você deve criar o banco de dados de armazenamento de conteúdo usando um dos bancos de dados listados na seguinte tabela.

A tabela a seguir mostra a codificação de caracteres e o protocolo que são usados por diferentes tipos de bancos de dados.

Tabela 4. Codificação de Caracteres e Protocolos para o Banco de Dados de Armazenamento de Conteúdo

Banco de Dados	Codificação de caracteres	Protocolo
Db2	UTF-8	TCP/IP
Oracle	AL32UTF8 ou AL32UTF16	TCP/IP
Microsoft SQL Server	UTF-8 ou UTF-16	TCP/IP
Informix	UTF-8	TCP/IP

Sequência de Ordenação

O Cognos Analytics usa uma única ordem de classificação, que especifica as regras usadas pelo banco de dados para interpretar, coletar, comparar e apresentar os dados de caracteres. Por exemplo, uma ordem de classificação define se a letra A é menor, igual ou maior que a letra B; se a ordenação diferencia maiúsculas de minúsculas e acentos. Para obter mais informações sobre ordenação e sequências de ordenação, consulte o website ICU - International Components for Unicode (http://site.icu-project.org/), selecione o Guia do Usuário e procure por Ordenação.

Configurações sugeridas para criar o armazenamento de conteúdo em sistemas operacionais IBM Db2 no Linux, Windows e UNIX

O banco de dados criado nos sistemas operacionais Microsoft Windows, Linux ou UNIX para o armazenamento de conteúdo deve conter as definições de configuração especificadas.

Para garantir uma instalação com sucesso, siga as seguintes diretrizes ao criar o armazenamento de conteúdo. Use as mesmas diretrizes para criar um banco de dados para registrar mensagens.

Diretrizes para Criar o Armazenamento de Conteúdo

Use a lista de verificação a seguir para ajudá-lo a configurar o armazenamento de conteúdo no Db2.

- Configure as variáveis de ambiente apropriadas para o Db2, que são mostradas na tabela a seguir.

Tabela 5. Variáveis de ambiente para o Db2

Variável do ambiente	Descrição
DB2PATH	O diretório de nível superior que contém o software do cliente de banco de dados ou a instalação do banco de dados inteiro.
LD_LIBRARY_PATH	O caminho da biblioteca de carregamento. Inclua o local do driver no caminho e substitua o símbolo de hash duplo por `64-bit`. Para Windows: `LD_LIBRARY_PATH= $DB2_location/sqllib/lib##: $LD_LIBRARY_PATH` Para Solaris e Linux:`LD_LIBRARY_PATH= $DB2DIR/lib##: $LD_LIBRARY_PATH` Para AIX: `LIBPATH=$DB2DIR/lib##:$LIBPATH`
DB2INSTANCE	A conexão padrão do servidor de banco de dados.
DB2CODEPAGE	A definição dessa variável de ambiente opcional a um valor de 1208 oferece suporte para bancos de dados multilíngues. Para obter informações sobre se essa variável de ambiente deve ser usada, consulte a documentação do Db2.

Tabela 5. Variáveis de ambiente para o Db2 (continuação)

Variável do ambiente	Descrição
COGUDA_EXTENDEDCHAR_SUPPORT	Alguns bancos de dados fornecem funções de sequência de caracteres utilizando um esquema baseado em bytes por padrão. Isso pode causar problemas com o processamento de sequências. Por exemplo, o banco de dados do Db2 com o conjunto de caracteres UTF-8 retorna um número indesejado de bytes, em vez do número de caracteres para a função LENGTH. Para evitar esse tipo de problema, configure essa variável para `T` ou `t`. Como resultado, o software IBM Cognos especifica a unidade de sequência CODEUNIT32 para as expressões de subsequência, character_length e posição no Db2 SQL para que essas expressões funcionem no esquema baseado em caracteres. Não use essa variável no modo de consulta dinâmica.

- Utilize o **UTF-8** como o valor de conjunto de códigos ao criar o banco de dados.

  Para verificar se o banco de dados possui o conjunto de códigos correto, use a interface da linha de comandos e digite o seguinte no prompt de comandos:

  `configuração do banco de dados db2 get para` *`database_name`*

  O valor do conjunto de códigos é UTF-8 e o valor da página de códigos é 1208.
- Certifique-se de definir os parâmetros de configuração conforme mostrado na tabela a seguir.

Tabela 6. Parâmetros de configuração para o Db2

Propriedade	Configuração
Tamanho da memória temporária do aplicativo (applheapsz)	AUTOMATIC ou pelo menos 1024 KB Se o valor do tamanho de intervalo do aplicativo for muito pequeno, erros de falta de memória podem ocorrer quando houver muitos usuários.
Tempo limite de bloqueio (locktimeout)	240 segundos Não defina esta opção com um valor de limite de tempo infinito.
Variável de registro do Db2 (DB2_INLIST_TO_NLJN)	SIM Definir essa variável como SIM melhora o desempenho.

- Crie um buffer pool com um tamanho de página de 32 KB e um segundo com um tamanho de página de 8 KB.
- Crie um espaço de tabela temporário de sistema utilizando o pool de buffer de 32 KB criado na etapa anterior.
- Crie um espaço de tabela temporário de usuário utilizando o buffer pool de 8 KB criado.

  Serão criadas tabelas temporárias globais no espaço de tabela temporário do usuário.

- Crie um espaço de tabela comum de usuário utilizando o buffer pool de 8 KB criado.

  Se estiver criando um banco de dados de criação de log, crie um espaço de tabela de usuário comum adicional com um tamanho de página de 8 KB.
- Conceda os seguintes privilégios do banco de dados para a conta do usuário que o IBM Cognos Analytics utilizará para acessar o banco de dados:
  - Conectar-se ao banco de dados
  - Criar tabelas
  - Criar esquemas implicitamente

  Dica: Se você deseja hospedar mais de um armazenamento de conteúdo em sua instância do Db2 e usar os dois ao mesmo tempo, utilize uma conta de usuário diferente para cada armazenamento de conteúdo para garantir que cada instância do IBM Cognos Analytics esteja totalmente isolada da outra.
- Certifique-se que a conta do usuário tenha privilégios de uso para o espaço de tabela de usuário temporário e outros espaços de tabela adequados associados com o banco de dados.
- Crie um esquema para a conta de usuário que o IBM Cognos Analytics utilizará para acessar o banco de dados e certifique-se de que o usuário tenha permissões para criar, eliminar e alterar o esquema.
- Crie um perfil que origine o `sqllib/db2profile` a partir do diretório inicial do usuário do Db2. Por exemplo, o conteúdo do seu perfil será semelhante ao seguinte:

```
   se
[ -f /home/db2user/sqllib/db2profile ]; then
./home/db2user/sqllib/db2profile
fi
```

- O administrador do banco de dados deve fazer backup regularmente dos bancos de dados do IBM Cognos Analytics regularmente, porque eles contêm os dados do IBM Cognos. Para garantir a segurança e integridade dos bancos de dados, proteja-os de acesso não autorizado ou inadequado.

Configurações sugeridas para criar o armazenamento de conteúdo no IBM Db2 on z/OS

O banco de dados criado para o armazenamento de conteúdo deve conter as definições de configuração especificadas.

Para garantir uma instalação com sucesso, siga as seguintes diretrizes ao criar o armazenamento de conteúdo.

Use a lista de verificação a seguir para ajudá-lo a configurar o armazenamento de conteúdo no Db2 on z/OS.

- Efetue logon no sistema z/OS como um usuário com os privilégios Administrador do Sistema (SYSADM) ou Controle do Sistema (SYSCTRL) no Db2 para criar o banco de dados.
- Crie uma instância do banco de dados, um grupo de armazenamento e uma conta de usuário para o armazenamento de conteúdo.

  O IBM Cognos Analytics usa as credenciais da conta do usuário para se comunicar com o servidor de banco de dados.
- Assegure-se de reservar um buffer pool com um tamanho de página de 32 KB, e um segundo com um tamanho de página de 4 KB para a instância de banco de dados.

- Os administradores devem executar um script para criar espaços de tabela para manter Objetos Grandes e outros dados para o armazenamento de conteúdo e conceder ao usuário os direitos aos espaços de tabela. Para obter mais informações sobre como executar o script, consulte “Criando espaços de tabela para um armazenamento de conteúdo no IBM Db2 for z/OS” na página 68.
- Seu administrador de banco de dados deve fazer backup do armazenamento de conteúdo regularmente porque ele contém as informações de aplicativo de dados e de segurança do IBM Cognos. Para garantir a segurança e integridade do banco de dados de armazenamento de conteúdo, proteja-o de acesso não autorizado ou inapropriado.

Configurações Sugeridas para Criar o Armazenamento de Conteúdo no Oracle

O banco de dados criado para o armazenamento de conteúdo deve conter as definições de configuração especificadas.

Para garantir uma instalação com sucesso, siga as seguintes diretrizes ao criar o armazenamento de conteúdo. Use as mesmas diretrizes para criar um banco de dados para registrar mensagens.

Use a lista a seguir para ajudá-lo a configurar o armazenamento de conteúdo no Oracle.

- Certifique-se de que o parâmetro para o nível de compatibilidade da instância de banco de dados esteja configurado para 9.0.1 ou mais alto.

  Por exemplo, é possível marcar a configuração do parâmetro de inicialização COMPATIBLE emitindo a seguinte instrução SQL: `SELECT name, value, description FROM v$parameter WHERE name='compatible';`

  Para obter informações sobre como alterar um parâmetro de configuração de instância, consulte a documentação do Oracle.
- Determine se o banco de dados é Unicode.

  Dica: Um método é digitar a seguinte instrução select:

  ```
  select * from NLS_DATABASE_PARAMETERS
  ```

  Se o conjunto de resultados gerar um NLS_CHARACTERSET que não seja Unicode, crie um novo banco de dados e especifique AL32UTF8 nos parâmetros de conjunto de caracteres do banco de dados.

  Se estiver usando o modo de consulta compatível, você talvez queira especificar a variável de ambiente COGUDA_EXTENDEDCHAR_SUPPORT com o valor `T` ou `t`. Essa variável substitui expressões de subsequência por SUBSTRC para o Oracle para retornar resultados corretos quando a sequência contém caracteres complementares Unicode.
- Determine qual conta do usuário será usada para acessar o banco de dados.

  Dica: Se quiser hospedar mais de um armazenamento de conteúdo na instância do Oracle e quiser utilizá-los ao mesmo tempo, use uma conta de usuário diferente para cada armazenamento de conteúdo, para garantir que cada instância do IBM Cognos Analytics fique totalmente isolada das outras.
- Certifique-se de que a conta de usuário que acessa o banco de dados tenha permissão para executar o seguinte:
  - Conectar-se ao banco de dados
  - Criar, alterar e descartar acionadores, visualizações, procedimentos e sequências

- Criar e alterar tabelas
- Inserir, atualizar e excluir dados nas tabelas de banco de dados

- O administrador do banco de dados deve fazer backup regularmente dos bancos de dados do IBM Cognos Analytics, pois eles contêm os dados do Cognos. Para garantir a segurança e integridade dos bancos de dados, proteja-os de acesso não autorizado ou inadequado.

Configurações Sugeridas para Criar o Armazenamento de Conteúdo no Microsoft SQL Server

O banco de dados criado para o armazenamento de conteúdo deve conter as definições de configuração especificadas.

Para garantir uma instalação com sucesso, siga as seguintes diretrizes ao criar o armazenamento de conteúdo. Use as mesmas diretrizes para criar um banco de dados para registrar mensagens.

Use a seguinte lista de verificação para ajudá-lo a configurar o armazenamento de conteúdo no Microsoft SQL Server.

- Verifique se a sequência de ordenação faz distinção entre maiúsculas e minúsculas.

  Em uma instalação Customizada, você escolhe uma ordenação, que inclui os conjuntos de caracteres e a ordem de classificação, durante a configuração do Microsoft SQL Server. Na instalação típica, o código do idioma identificado pelo programa de instalação é usada para a ordenação. Esta definição não pode ser alterada mais tarde.
- Ao se conectar ao Microsoft SQL Server Management Studio para criar o banco de dados, use a autenticação do Microsoft SQL Server.

  Se você se conectar usando a autenticação do sistema operacional Microsoft Windows, o banco de dados criado também usará a autenticação do Windows. Nesse caso, será necessário configurar a conexão do banco de dados usando um tipo de banco de dados do **SQL Server (Autenticação do Windows)** no IBM Cognos Configuration.
- Para a conta de usuário que será utilizada para acessar o banco de dados, crie um novo login em **Segurança** e utilize as seguintes configurações:
  - Selecione **Autenticação do SQL Server**.
  - Desmarque a caixa de seleção **Enforce password policy**.

  Dica: Se quiser hospedar mais de um armazenamento de conteúdo na instância do Microsoft SQL Server e quiser utilizá-los ao mesmo tempo, use uma conta de usuário diferente para cada armazenamento de conteúdo, para garantir que cada instância do IBM Cognos Analytics fique totalmente isolada das outras.
- Para o Microsoft SQL Server 2008, conceda permissão de EXECUÇÃO para a conta do usuário que acessa o banco de dados.
- Para o banco de dados de armazenamento de conteúdo, crie um novo banco de dados em **Bancos de dados**.
- Em **Segurança** para o novo banco de dados, crie um novo esquema e atribua um nome a ele.
- Em **Segurança** para o novo banco de dados, crie um novo usuário com as seguintes configurações:
  - Para **Nome de login**, especifique o novo login criado para a conta de usuário.
  - Para **Esquema padrão**, especifique o novo esquema.

- Para **Owned Schemas**, selecione o novo esquema.
- Para **Role Members**, selecione **db_datareader**, **db_datawriter** e **db_ddladmin**.

Configurações sugeridas para criar o armazenamento de conteúdo no servidor de banco de dados IBM Informix

O banco de dados criado para o armazenamento de conteúdo do IBM Cognos Analytics deve conter definições de configuração específicas.

Use as diretrizes a seguir ao criar o armazenamento de conteúdo. Use as mesmas diretrizes para criar um banco de dados para registrar mensagens.

Use a lista de verificação a seguir para ajudar a configurar o armazenamento de conteúdo no banco de dados do servidor de banco de dados do IBM Informix.

- Defina as seguintes variáveis de ambiente:
  - Configure **GL_USEGLU** para 1 para ativar o International Components for Unicode (ICU) no servidor de banco de dados Informix.
  - Configure **DB_LOCALE** para `en_us.utf8` para configurar o código do idioma do banco de dados para Unicode.
- Crie um banco de dados no modo ANSI e com o login ativado.
- Para a conta de usuário utilizada para acessar o banco de dados, conceda o privilégio de banco de dados DBA.

  Importante: Se você hospedar mais que um banco de dados na sua instância do Informix e usá-los ao mesmo tempo, use uma conta do usuário diferente para cada banco de dados. Você também deve definir a conta do usuário em cada instância do aplicativo IBM Cognos Configuration, criando um parâmetro de propriedade avançada e especificando a conta do usuário como o valor. Para diversos bancos de dados de armazenamento de conteúdo, nomeie a propriedade **CMSCRIPT_CS_ID**. Para diversos bancos de dados de criação de logs, nomeie a propriedade **IPFSCRIPTIDX**.

Configurar uma conta do usuário ou uma conta do serviço de rede para o IBM Cognos Analytics

É possível configurar uma conta do usuário ou uma conta do serviço de rede para o IBM Cognos Analytics.

A conta do usuário ou do serviço de rede na qual o IBM Cognos Analytics é executado deve:

- Ter acesso a todos os recursos necessários, como impressoras.
- Ter direitos de fazer logon como um serviço e atuar como parte do sistema operacional.

Além disso, a conta de usuário deve ser membro do grupo administrador local.

Por exemplo, para imprimir relatórios usando uma impressora da rede, a conta deve possuir acesso à impressora da rede ou você deve designar uma conta de logon para o serviço do IBM Cognos.

Configuração de contas de usuário

Para o sistema operacional Microsoft Windows, designe uma conta de logon para o serviço do IBM Cognos. É possível configurar o serviço do IBM Cognos para usar

uma conta do usuário especial ao selecionar o serviço do IBM Cognos na lista de serviços mostrada na janela Serviços no Windows. Em seguida, pode-se definir as propriedades da conta de usuário.

Nos sistemas operacionais UNIX ou Linux crie um novo grupo chamado UNIX ou Linux cognos, por exemplo. Esse grupo deve conter o usuário que possui os arquivos do IBM Cognos. Altere a propriedade do grupo dos arquivos IBM Cognos para o grupo cognos e altere as permissões de arquivo para todos os arquivos IBM Cognos para GROUP READABLE/WRITABLE/EXECUTABLE.

Configure o servidor web para utilizar aliases. Para obter mais informações, consulte o tópico sobre configuração do servidor web.

Configuração de contas de serviço de rede

A conta de serviço de rede é a conta integrada NT AUTHORITY\NetworkService no sistema operacional. Os administradores não precisam gerenciar uma senha ou manter a conta.

Use uma conta com privilégios de administrador se estiver instalando no Windows Server 2008.

Configure o servidor web para utilizar pool de aplicativos. Para obter mais informações, consulte o tópico sobre configuração do servidor web. Também é necessário ter permissões de gravação para fazer instalações no diretório.

Configurar navegadores da web

Os componentes do IBM Cognos Analytics usam configurações padrão do navegador. As configurações adicionais solicitadas são específicas para o navegador.

Configurações do navegador necessárias para o Cognos Analytics

A seguinte tabela mostra as configurações que devem ser habilitadas.

Tabela 7. Configurações do navegador ativadas

Navegador	Configuração
Internet Explorer	Permitir cookies Criação ativa de scripts Permissão de META REFRESH Executar os controles e plug-ins ActiveX. Controles de script ActiveX marcados como seguros para criação de scripts. Comportamentos Binários e de Script Permitir acesso programático à área de transferência Persistência de dados do usuário

Tabela 7. Configurações do navegador ativadas (continuação)

Navegador	Configuração
Firefox	Permitir cookies Ativar Java Ativar JavaScript Carregar Imagens
Safari 5	Ativar Java Ativar JavaScript Bloquear Cookies: Nunca
Google Chrome	Cookies: Permitir que dados locais sejam configurados Imagens: Mostrar todas as imagens JavaScript: Permitir que todos os sites executem JavaScript

O Relatórios e o Query Studio usam o suporte a XML nativo do Microsoft Internet Explorer, que é um componente do navegador. O suporte a ActiveX deve ser ativado porque os aplicativos Microsoft implementam XML usando ActiveX. O Cognos Analytics não fornece ou faz o download de controles do ActiveX. Somente os controles ActiveX instalados como parte do Internet Explorer são ativados nesta configuração.

Se você usar o Microsoft Internet Explorer, será possível incluir a URL para seus gateways na lista de Sites confiáveis. Por exemplo, `http://<server_name>:<port_number>/ibmcognos`. Isso permite o prompt automático com relação a downloads de arquivos.

Permita pop-ups para todas as páginas do Cognos Analytics, para todos os navegadores.

Cookies usados pelos componentes do Cognos Analytics

O Cognos Analytics usa os seguintes cookies para armazenar informações de usuários.

Tabela 8. Cookies usados pelos componentes do Cognos Analytics

Cookie	Tipo	Finalidade
AS_TICKET	Sessão temporária	Criado se o Cognos Analytics estiver configurado para usar um namespace do IBM Cognos Series 7
caf	Sessão temporária	Contém informações de segurança de estado

Tabela 8. Cookies usados pelos componentes do Cognos Analytics (continuação)

Cookie	Tipo	Finalidade
Cam_passport	Sessão temporária	Armazena uma referência para uma sessão do usuário armazenada no servidor do Content Manager. Os administradores podem configurar o atributo HTTPOnly para bloquear scripts de leitura ou manipulação do cookie de passaporte do CAM durante uma sessão do usuário com seu navegador da Web. Para obter mais informações, consulte o *IBM Cognos AnalyticsGuia de administração e segurança*.
cc_session	Sessão temporária	Contém informações de sessão
cc_state	Sessão temporária	Mantém as informações durante as operações de edição, tais como recortar, copiar e colar.
CRN	Sessão temporária	Contém informações de código de idioma do produto e conteúdo e está configurado para todos os usuários do IBM Cognos
CRN_RS	Persistente	Armazena a opção feita pelo usuário para a pasta de membros de visualização no Relatórios
PAT_CURRENT_ FOLDER	Persistente	Armazena o caminho da pasta atual se for usado o acesso de arquivo local, e é atualizado após as caixas de diálogo Abrir ou Salvar forem usadas
qs	Persistente	Armazena as configurações feitas pelo usuário para elementos de interface como menus e barras de ferramentas
userCapabilities	Sessão temporária	Contém todos os recursos e a assinatura do usuário atual
usersessionid	Sessão temporária	Contém um identificador de sessão de usuário exclusivo, válido para a duração da sessão do navegador.

Tabela 8. Cookies usados pelos componentes do Cognos Analytics (continuação)

Cookie	Tipo	Finalidade
XSRF (falsificação de solicitação entre sites)	Sessão temporária	A XSRF engana um navegador da web para executar uma ação maliciosa em um site confiável no qual o usuário está atualmente autenticado. A XSRF explora a confiança que um site tem no navegador de um usuário. Evita que uma página da web carregada a partir do domínio X faça solicitações para o domínio Y, supondo que o usuário já esteja autenticado no domínio Y. Quando autenticado pela primeira vez no Cognos Analytics, o cookie XSRF é configurado. Daquele ponto em diante, todas as solicitações requererão o cookie XSRF-TOKEN, assim como um cabeçalho HTTP chamado X-XSRF-TOKEN.

Após atualizar ou instalar um novo software, reinicie o navegador web e avise aos usuários para limparem o cache de seus navegadores.

Capítulo 2. Opções de Distribuição

Antes de implementar o IBM Cognos Analytics, decida como instalá-lo em seu ambiente. É possível instalar todos os componentes do servidor em um computador ou distribuí-los em uma rede. A melhor opção de distribuição depende de requisitos de relatórios, recursos e preferências. Os requisitos de configuração são diferentes quando você instala todos os componentes em um computador e quando você distribui os componentes entre múltiplos computadores.

O Cognos Analytics é compatível com outros produtos Cognos. Se seu ambiente incluir outros produtos Cognos, deve-se considerar como o Cognos Analytics se ajustará nesse ambiente.

O Cognos Analytics não pode ser instalado no mesmo local que outros produtos Cognos, como o Cognos Framework Manager, o Cognos Transformer, o Cognos PowerPlay e assim por diante.

Componentes do Cognos Analytics

O IBM Cognos Analytics é uma solução de inteligência de negócios baseada na web com relatórios integrados, painéis, análise, gerenciamento de eventos e outros recursos. O Cognos Analytics inclui componentes do servidor e de modelagem.

O Cognos Analytics integra-se facilmente à infraestrutura existente, usando recursos que estão no ambiente. Alguns desses recursos existentes são necessários, como um banco de dados para o armazenamento de conteúdo. Outros recursos são opcionais, tal como um provedor de segurança para autenticação.

Dica: Quando o Cognos Analytics é instalado usando a opção **Instalação fácil**, não é necessário configurar um banco de dados de armazenamento de conteúdo ou um provedor de segurança. O produto está pré-configurado e pronto para uso.

O IBM Cognos Analytics executa o WebSphere Application Server Liberty Profile como o servidor de aplicativos.

Componentes do servidor

Os componentes do servidor para o IBM Cognos Analytics estão separados em três camadas: dados, aplicativo e um gateway opcional.

Os componentes do servidor fornecem as interfaces com o usuário para relatórios, painéis, análise, gerenciamento de evento e assim por diante, bem como a funcionalidade para roteamento e processamento de solicitações de usuários.

No programa de instalação, selecione os seguintes componentes do servidor:

- “Camada de dados: Content Manager” na página 20
- “Camada do aplicativo: componentes” na página 20
- “Camada de gateway opcional: comunicação da web” na página 22

  Dica: O gateway opcional é necessário somente para o Kerberos.

Como um componente do servidor opcional, também é possível instalar as amostras do Cognos Analytics. Usando dados de uma empresa fictícia, a Companhia de Aventuras de Amostra, as amostras ilustram os recursos do produto e melhores práticas técnicas e de negócios. É possível usar as amostras para experimentar e compartilhar técnicas de relatório e para resolução de problemas. Para obter mais informações, consulte o *Guia de amostras para o IBM Cognos Analytics*.

Camada de dados: Content Manager

O Content Manager é o serviço do IBM Cognos Analytics que gerencia o armazenamento de dados do aplicativo, incluindo especificações de segurança, de dados de configuração, de modelos, de relatórios, de saídas de relatório, etc.

O Content Manager é necessário para publicar pacotes, recuperar e armazenar especificações de relatório, gerenciar informações de planejamento e gerenciar o namespace do Cognos.

O Content Manager armazena informações em um banco de dados de armazenamento de conteúdo.

Camada do aplicativo: componentes

A camada do aplicativo IBM Cognos Analytics contém um ou mais servidores Cognos Analytics. Os servidores executam solicitações, como relatórios, análises e consultas que são encaminhados pelo gateway, e renderizam as interfaces.

Configurando e Gerenciando o Produto - IBM Cognos Configuration

O IBM Cognos Configuration é usado para configurar o Cognos Analytics e para iniciar e parar seus serviços.

Publicando, gerenciando e visualizando o conteúdo - portal doCognos Analytics

O portal do Cognos Analytics fornece um ponto de acesso único aos dados corporativos disponíveis para seus produtos. Ele fornece um ponto único de entrada para consultas, análises e organização de dados, e para a criação de relatórios, scorecards e eventos. Os usuários podem executar todos os seus aplicativos do Cognos Analytics baseados na web por meio do portal. Os outros aplicativos e os endereços da web para outros aplicativos podem ser integrados ao portal.

Relatórios profissional

Ao usar a ferramenta Relatórios, os autores de relatório criam, editam e distribuem uma ampla gama de relatórios profissionais.

Criação de painéis

O Cognos Analytics fornece painéis para comunicar seus insights e análises. É possível montar uma visualização que contém visualizações, como um gráfico, diagrama, tabela, mapa ou qualquer outra representação visual de dados.

Um painel é um tipo de visualização que o ajuda a monitorar eventos ou atividades em uma visão rápida. Ele fornece insights e análises chaves sobre os seus dados em uma ou mais páginas ou telas.

Administração central - Console de Gerenciamento e de Administração

O Cognos Analytics possui uma função **Gerenciar** que pode ser usada para executar tarefas de administração comuns diárias. Uma opção do menu **Gerenciar** abre o **Console de administração**, uma interface de gerenciamento central que contém as tarefas administrativas do IBM Cognos Analytics. Ela fornece acesso fácil ao gerenciamento geral do ambiente do IBM Cognos. O acesso às funções de administração depende das permissões do usuário.

IBM Cognos Mobile

O IBM Cognos Mobile estende o Cognos Analytics e o gerenciamento de desempenho para dispositivos móveis. Com este rich client, o Cognos Mobile permite que os usuários visualizem em seus dispositivos os relatórios, áreas de trabalho e análises do Cognos Analytics produzidos por ferramentas como Relatórios, Query Studio, Analysis Studio e Cognos Workspace. O Cognos Mobile entrega informações adequadas, informativas e interativas para suportar usuários móveis em seus processos de tomada de decisões, independentemente do local em que os usuários estejam localizados.

O Cognos Mobile processa cada relatório doCognos Analytics que ele recebe e o renderiza em uma versão adequada para dispositivos móveis.

O Cognos Mobile usa a funcionalidade de prompts do Cognos Analytics e mecanismos de planejamento para fornecer relatórios customizados de uma maneira adequada. Para obter mais informações sobre prompts, veja o *IBM Cognos Analytics - Reporting User Guide*. Para obter mais informações sobre planejamentos, veja o *IBM Cognos Analytics Administration and Security Guide*.

O Cognos Mobile usa a segurança do Cognos Analytics, implementa medidas de segurança adicionais específicas para um aplicativo móvel, utiliza diversas arquiteturas de segurança específicas do fornecedor e aproveita a vantagem das medidas de segurança baseadas em dispositivo e em servidor.

Diversos servidores de gerenciamento específicos do dispositivo e ferramentas de administração usadas pelo Cognos Mobile oferecem a capacidade de remover conteúdo remotamente de um dispositivo ou de desativar completamente o dispositivo. Dessa forma, por exemplo, se um dispositivo for perdido ou roubado, o administrador do Cognos Analytics pode usar esta funcionalidade para proteger conteúdo sensível no dispositivo. Ou, um administrador do Cognos Analytics poderia configurar uma data de expiração para um relatório após a qual o relatório fica inacessível até que o usuário se reautentique. Para obter mais informações sobre a segurança do Cognos Analytics, veja o *IBM Cognos Analytics Administration and Security Guide*. Para obter mais informações sobre o gerenciamento de dispositivo e segurança, consulte a documentação do dispositivo.

O Cognos Mobile também suporta solicitações entre o dispositivo móvel e o ambiente do servidor para as funções de procura, navegação e execução do produto:

Deve-se instalar e executar a mesma versão do Cognos Mobile e do servidor Cognos Analytics.

Consultas ad hoc e relatórios para uso próprio - Query Studio

Usando o Query Studio, os usuários com pouco ou nenhum treinamento podem rapidamente projetar, criar e salvar relatórios para atender necessidades de relatórios não abrangidas pelos relatórios profissionais padrão criados no Relatórios.

Monitoração de dados para condições excepcionais - Event Studio

No Event Studio, define-se agentes para monitorar seus dados e realizar tarefas quando ocorrerem eventos de negócios ou condições excepcionais com os quais se deve lidar. Quando um evento ocorre, as pessoas são alertadas para agir. Os agentes podem publicar detalhes no portal, mandar alertas por e-mail, executar e distribuir relatórios baseados em eventos, e monitorar o status de eventos. Por exemplo, uma chamada de suporte de um cliente principal ou o cancelamento de um grande pedido pode acionar um evento, enviando um email às pessoas apropriadas.

Facilitando a Tomada de Decisão - IBM Cognos Workspace

É possível criar áreas de trabalho interativas sofisticadas usando o conteúdo do IBM Cognos, bem como origens de dados externas como TM1 Websheets e CubeViews, de acordo com suas necessidades de informações específicas. É possível visualizar e abrir áreas de trabalho e relatórios favoritos, manipular o conteúdo e enviar provas por email. Também é possível usar os comentários e atividades para tomar decisões de maneira colaborativa.

Também é possível usar um software social, como o IBM Connections para tomar decisões de maneira colaborativa.

Compatibilidade com o Microsoft Office - IBM Cognos para Microsoft Office

Usando o IBM Cognos for Microsoft Office, os usuários do Microsoft Office podem acessar dados e visualizações nos relatórios do IBM Cognos dentro dos aplicativos do Microsoft Office, como Excel, PowerPoint e Word.

Os componentes do Cognos for Microsoft Office estão incluídos com o Cognos Analytics e devem ser instalados separadamente.

Camada de gateway opcional: comunicação da web

Os gateways em geral são programas CGI, mas podem seguir outros padrões, como o Internet Server Application Program Interface (ISAPI) ou os Módulos Apache (apache_mod). O IBM Cognos Analytics usa somente o CGI, o ISAPI ou o Módulo Apache para o Kerberos. Caso contrário, não será necessário configurar um gateway.

No IBM Cognos Analytics, a camada do aplicativo fornece as funções de um gateway.

Componentes de modelagem

Os componentes de modelagem modelam dados em origens de dados para estruturar e apresentar dados de uma forma que faça sentido para o usuário. Os componentes de modelagem incluem as seguintes ferramentas:

Modelagem da web do IBM Cognos Analytics

O IBM® Cognos® Analytics possui uma ferramenta de modelagem sem presença e simples de usar que pode ser usada para criar rapidamente módulos de dados a partir de várias origens de dados. É possível usar origens de dados, como servidores de dados, arquivos transferidos por upload e módulos de dados salvos anteriormente para criar módulos de dados. A modelagem de dados do Cognos Analytics usa modelagem orientada à intenção para gerar um módulo usando termos que você define. Para obter detalhes sobre todos os recursos disponíveis, consulte o *Guia de Modelagem do IBM Cognos Analytics Data*.

A modelagem de dados do Cognos Analytics não substitui os recursos de modelagem mais complexos do IBM Cognos Framework Manager ou do IBM Cognos Cube Designer. Essas ferramentas ainda estão disponíveis no Cognos Analytics.

Criação de uma visualização de negócios dos dados - Framework Manager

O IBM Cognos Framework Manager é a ferramenta de modelagem para criar e gerenciar metadados relacionados a negócios para uso no IBM Cognos Analytics. Os metadados são publicados para uso com ferramentas de relatórios como o pacote, fornecendo uma visualização de negócios única e integrada de qualquer quantidade de origens de dados heterogêneas.

O Framework Manager deve ser instalado em um local diferente do Cognos Analytics.

Modelagem do ROLAP - Cube Designer

O IBM® Cognos® Cube Designer é a ferramenta de modelagem fornecida pelo IBM Cognos Dynamic Cubes. Use-a para construir cubos dinâmicos e publicá-los para uso no IBM Cognos Analytics.

Para a introdução, importe dados de um banco de dados relacional. Usando os metadados, você modela cubos dinâmicos e salva as definições de cubo em um projeto. Após publicar os cubos, eles serão listados como origens de dados no Content Manager e seus pacotes relacionados estarão disponíveis para autores de relatório.

O Cube Designer deve ser instalado em um local diferente do Cognos Analytics.

Modelagem Multidimensional - IBM Cognos Transformer

O IBM Cognos Transformer é a ferramenta de modelagem do IBM Cognos Analytics usada para criar PowerCubes para uso no IBM Cognos Analytics. Os IBM Cognos Analytics PowerCubes protegidos não são compatíveis com o IBM Cognos Series 7.

O Transformer deve ser instalado em um local diferente do Cognos Analytics.

Dica: Para obter informações sobre como instalar e configurar versões do Transformer anteriores à 8.4, consulte a documentação fornecida com a sua edição do Transformer.

Importar e gerenciar mapas (somente mapas anteriores do Gerenciador de mapas)

O IBM Cognos Map Manager é um utilitário baseado em Windows que os administradores e modeladores usam para importar mapas e atualizar rótulos para mapas no Relatórios. Para recursos de mapas, como nomes de país ou região e de cidade, os administradores e os modeladores podem definir nomes alternativos para fornecer versões multilíngues do texto que aparece no mapa.

O Map Manager deve ser instalado em um local diferente do Cognos Analytics.

Para obter mais informações, consulte o Guia de Instalação e Usuário do *IBM Cognos Map Manager*.

Componentes Necessários do Banco de Dados

Além das ferramentas que são fornecidas, o IBM Cognos Analytics requer que os componentes a seguir sejam criados usando outros recursos.

Armazenamento de conteúdo

O armazenamento de conteúdo é um banco de dados relacional que contém dados que o Cognos Analytics precisa para operar, tais como especificações de relatório, modelos e pacotes publicados que os contêm, informações de conexão para origens de dados, informações sobre namespaces externos e o próprio namespace do Cognos, informações sobre planejamento e bursting de relatórios e assim por diante.

Ao configurar seu ambiente do Cognos Analytics, configure o armazenamento de conteúdo para usar um banco de dados suportado que possa ser protegido e ajustado para desempenho e estabilidade. Para obter mais informações, veja o tópico sobre implementação do armazenamento de conteúdo inteiro no *IBM Cognos Analytics Administration and Security Guide*.

Modelos de projeto e arquivos de log não são guardados no armazenamento de conteúdo.

O serviço do IBM Cognos que usa o armazenamento de conteúdo é chamado Content Manager.

Origens de dados

Origens de dados, também conhecidas como banco de dados de consulta, são bancos de dados relacionais, cubos dimensionais ou OLAP, arquivos ou outros armazenamentos de dados físicos que podem ser acessados por meio do Cognos Analytics. Os Componentes de camada de aplicativos usam conexões de origens de dados para acessar origens de dados.

componentes do Cognos Mobile

O IBM Cognos Mobile inclui o serviço Cognos Mobile e o aplicativo Cognos Mobile. Esses componentes são instalados com o IBM Cognos Analytics.

Depois de configurar o serviço Cognos Mobile, os usuários podem instalar o aplicativo Cognos Mobile em seus dispositivos móveis para acessar conteúdo do

Cognos Analytics, como relatórios ou painéis. Para usar o aplicativo, os usuários fazem o download da versão iOS na Loja de aplicativos da Apple, ou da versão Android na Loja Google Play.

O serviço Cognos Mobile manipula as seguintes operações:

- Realiza o push do conteúdo de relatório e de análise para os dispositivos móveis.
- Facilita solicitações relacionadas a relatórios e a análises de entrada e saída entre o dispositivo móvel e o ambiente para procurar, navegar e executar relatórios.
- Sincroniza o armazenamento de conteúdo remoto no servidor com o banco de dados remoto no dispositivo móvel.
- Comunica-se com o dispositivo móvel.

O dispositivo móvel contém o aplicativo Cognos Mobile e o armazenamento de conteúdo móvel compactado e criptografado. Esses componentes fornecem a funcionalidade que o usuário do dispositivo móvel precisa para trabalhar com relatórios, painéis e análises do Cognos Analytics.

O diagrama a seguir mostra como os componentes interagem no ambiente do Cognos Analytics. Os dispositivos móveis se conectam ao servidor IBM Cognos por meio de operadoras de Internet e de serviços wireless usando HTTP.

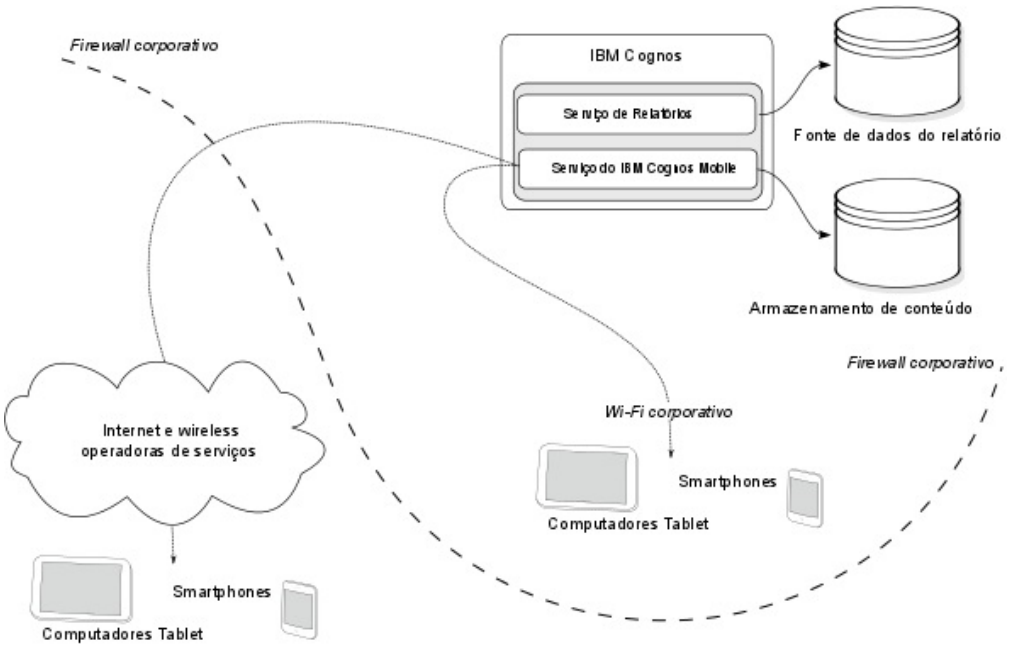


Figura 1. Componentes do Cognos Mobile no ambiente do Cognos Analytics

Distribuição de Componentes

Ao instalar os componentes do servidor do IBM Cognos Analytics, você especifica o local no qual a camada do aplicativo, a camada de dados (Content Manager) e os componentes opcionais da camada do gateway serão colocados.

É possível usar os seguintes cenários de instalação:

- Instale todos os componentes em um computador.

Essa opção é normalmente usada para implementações departamentais, como um sistema de demonstração ou em um ambiente de prova de conceito.

- Instale os Componentes da camada de aplicativos e o Content Manager em computadores separados.

  Escolha essa opção para maximizar o desempenho, a disponibilidade, a capacidade ou a segurança com base nas características de processamento da organização.
- Instale o gateway opcional em um computador separado.

  Nessa opção, o gateway e o servidor da web estão em um computador e os componentes restantes do Cognos estão em outros computadores. Será possível escolher essa opção se você tiver servidores da web existentes que estejam disponíveis para manipular as solicitações de componentes do Cognos Analytics.
- Consolide diversos servidores instalando no System z

  O IBM Cognos Analytics é suportado para o Linux no sistema operacional System z. Esse tipo de instalação é adequada quando se está configurando ou personalizando uma instalação no ambiente para adequar-se aos requisitos de TI e de infraestrutura.

Depois de instalar os componentes do servidor, eles deverão ser configurados para que possam comunicar-se uns com os outros.

Além de instalar a camada de dados (Content Manager), a camada do aplicativo e os componentes opcionais da camada do gateway, também é possível instalar o Cognos Framework Manager, a ferramenta de modelagem de metadados e o Cognos Transformer, a ferramenta de modelagem para criar PowerCubes. Independentemente do cenário de instalação do IBM Cognos que você segue, instale os componentes de modelagem em locais separados.

Componentes da Camada de Aplicativos e Content Managers em Computadores Separados

Os Componentes da Camada de Aplicativos balanceiam cargas, acessam dados, executam consultas, planejam tarefas e renderizam relatórios. O Content Manager armazena todas as especificações de relatórios, resultados, pacotes, pastas e tarefas no armazenamento de conteúdo.

É possível instalar os Application Tier Components e o Content Manager no mesmo computador ou em computadores diferentes. A instalação em computadores diferentes pode aperfeiçoar o desempenho, a disponibilidade e a capacidade.

Mais de um Content Manager

É possível instalar qualquer número de Content Managers, embora apenas um fique ativo num dado momento. As outras instalações agem como uma reserva do Content Manager. Essas reservas ficam ativas apenas se ocorre uma falha que afeta o computador com Content Manager ativo. Para suporte de failover, é aconselhável instalar o Content Manager em dois ou mais computadores.

Instalar Diversos Content Managers

O Content Manager armazena os dados que o IBM Cognos Analytics precisa para operar, como especificações de relatórios, modelos publicados e os pacotes que os utilizam; informações de conexão para origens de dados; informações sobre o namespace externo e o próprio namespace do Cognos; e informações sobre planejamento e relatórios burst. O armazenamento de conteúdo é um sistema de

gerenciamento de banco de dados relacional (RDBMS). Há apenas um armazenamento de conteúdo para cada instalação do IBM Cognos.

É possível instalar o Content Manager separadamente do Application Tier Components. Por exemplo, o Content Manager pode ser necessário na camada de dados em vez da camada de aplicativos.

Se um Content Manager ativo falhar, os dados de sessão que não foram salvos serão perdidos. Quando o novo Content Manager ativo assumir, os usuários poderão ter que refazer logon.

No diagrama a seguir, o gateway passa a solicitação ao dispatcher (não exibido), que a passa para o computador com Content Manager ativo padrão. Como o computador falhou, a solicitação é redirecionada para o computador em espera com Content Manager, que se tornou ativo quando o computador ativo padrão com Content Manager falhou.

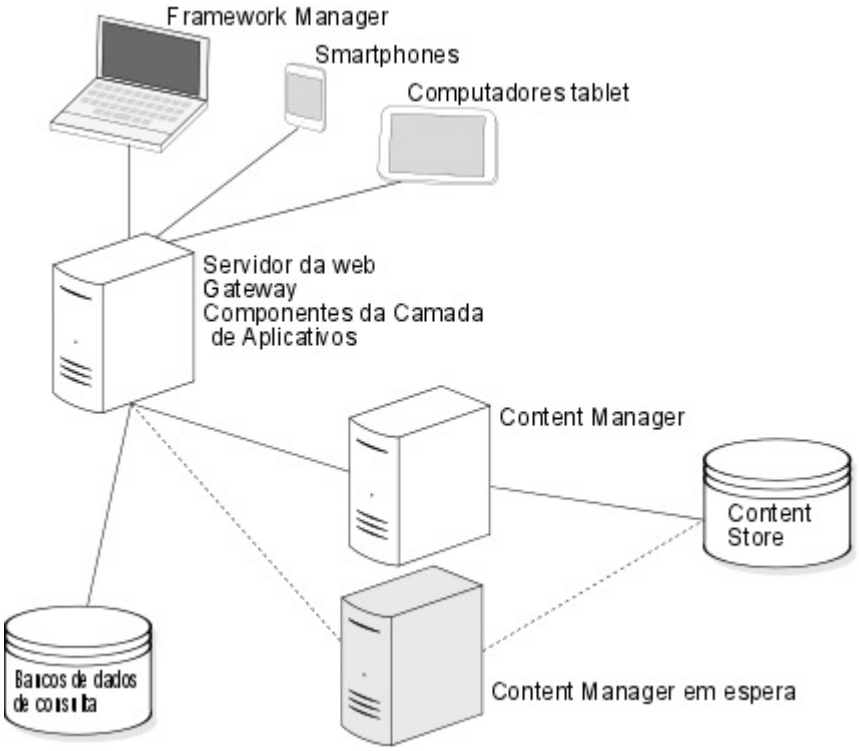


Figura 2. Instalação com um Content Manager Ativo e um em Espera

Requisitos de Configuração

Em cada computador no qual foi instalado o Content Manager, é necessário

- Especificar informações de conexão para o armazenamento de conteúdo.
- Especificar os URIs de dispatchers.
- Especificar todos os URIs do Content Manager.
- Especificar o URI do dispatcher para aplicativos externos.
- configurar uma conexão com um servidor de e-mail (se desejar enviar relatórios ou notificações por e-mail)

Mais de um Computador com Componentes da Camada de Aplicativos

Para melhorar a escalabilidade em um ambiente no qual haja normalmente um grande volume de solicitações para processar, é possível instalar o Application Tier Components em vários computadores dedicados ao processamento de solicitações recebidas. Com a instalação de Application Tier Components em vários computadores, as cargas são distribuídas e balanceadas entre os computadores. A acessibilidade e a taxa de transferência também são melhores que em um único computador, assim como o suporte a failover.

Requisitos de Configuração

Se você instalar um ou mais Componentes da Camada de Aplicativos em um computador separado, para garantir que eles possam se comunicar com outros componentes do IBM Cognos Analytics, faça o seguinte:

- Especificar todos os URIs do Content Manager.
- Especificar os URIs de dispatchers.
- Especificar o URI do dispatcher para aplicativos externos.

Consolidando Servidores para Linux no System z

O sistema operacional Linux no System z é uma implementação nativa do sistema operacional Linux. As opções de hosting incluem a execução do Linux e uma ou mais partições lógicas (LPAR).

Recurso Integrado para Linux (IFL)

IFLs são processadores do System z dedicados à execução de cargas de trabalho do sistema operacional Linux nativamente, ou sob software de virtualização, dependendo de suas necessidades. IFLs permitem consolidar e gerenciar centralmente recursos do Linux no System z.

Modo de Partição Lógica (LPAR)

O sistema operacional Linux pode ser executado em LPARs e se comunicar com outras partições do Linux usando conexões TCP/IP.

A escalabilidade horizontal em um grande ambiente Linux é limitada pelo número de LPARs que podem ser criadas. A execução do Linux em LPARs pode ser melhor se você estiver executando um pequeno número de imagens do Linux e cada uma dessas imagens estiver usando uma grande quantidade de energia de processamento ou exigir uma grande quantidade de memória dedicada. Isso garante que as imagens não terão recursos sub-utilizados alocados a elas.

Instalação para os componentes de modelagem opcionais

Você instala as ferramentas de modelagem, como o Framework Manager e o Transformer em computadores com sistema operacional Microsoft Windows.

Para publicar pacotes para que estejam disponíveis aos usuários, deve-se configurar as ferramentas de modelagem opcionais para usar um dispatcher, diretamente ou por meio de um gateway. Se o portal estiver assegurado, será necessário ter privilégios para criar origens de dados e publicar pacotes no portal

Considerações sobre Firewall

Quando a ferramenta de modelagem estiver fora de um firewall de rede que proteja os Application Tier Components, podem surgir problemas de comunicação com o dispatcher. Por motivos de segurança, a configuração padrão do IBM Cognos Analytics impede que o dispatcher aceite solicitações da ferramenta de modelagem quando ela está fora do firewall de rede.

Uma ferramenta de modelagem que está fora do firewall de rede, por exemplo, o Framework Manager, não pode enviar solicitações pelo firewall de rede para o dispatcher no servidor de aplicativos do IBM Cognos Analytics. Para evitar problemas ao se comunicar por um firewall de rede, instale a ferramenta de modelagem na mesma camada de arquitetura que o Application Tier Components. O diagrama a seguir mostra o computador do Framework Manager dentro do firewall de rede, comunicando-se com êxito com o dispatcher no servidor de aplicativos do IBM Cognos Analytics.

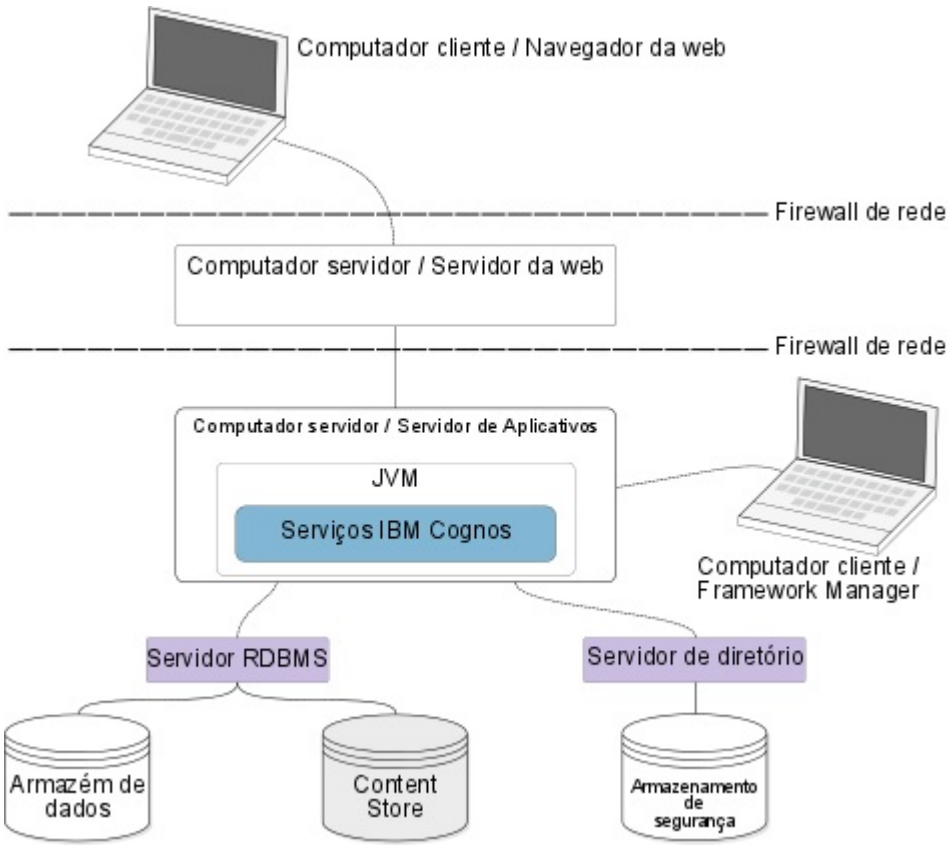


Figura 3. Computador Cliente Fora do Firewall

Como alternativa, é possível instalar um gateway adicional que é dedicado à comunicação com a ferramenta de modelagem conforme mostrado no diagrama a seguir. Em seguida, a ferramenta e o gateway podem ser configurados de forma que o dispatcher aceite solicitações da ferramenta de modelagem.

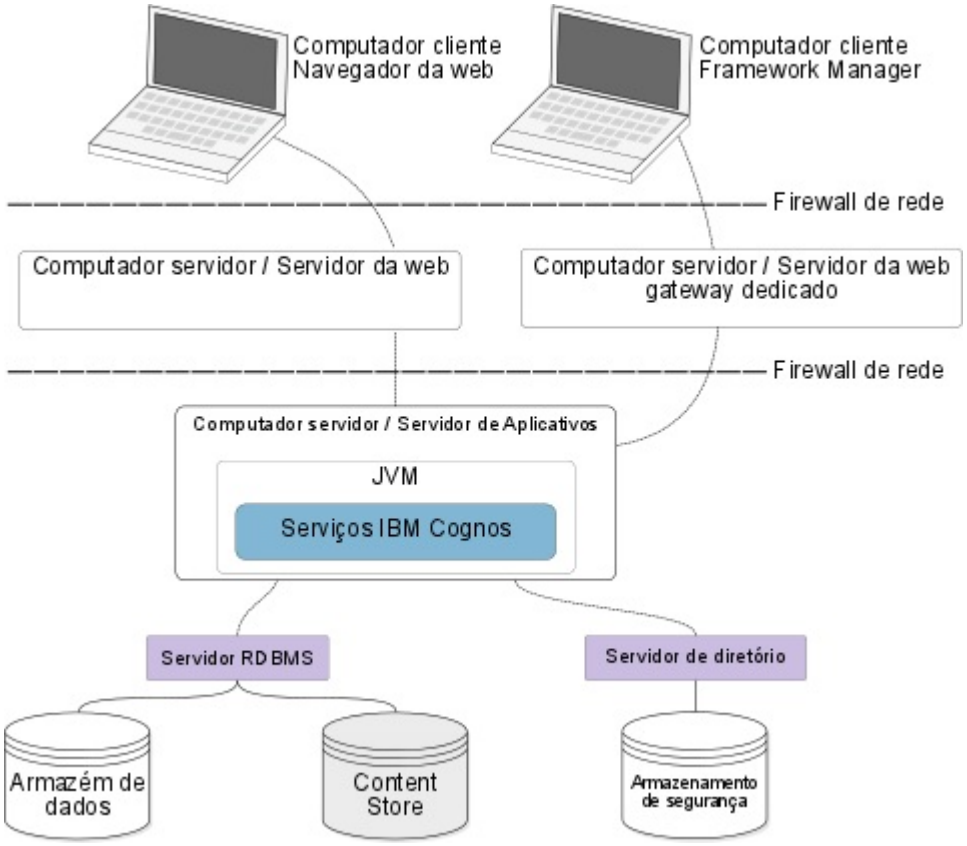


Figura 4. Computador Cliente Fora do Firewall

Distribuição dos Componentes do Framework Manager

O Framework Manager comunica-se com os Componentes da camada de aplicativos, que podem ser instalados em um ou mais aplicativos. Para publicar pacotes, configure o Framework Manager para se comunicar com o dispatcher, tanto diretamente como através de um gateway dedicado.

Requisitos de Configuração

No computador em que o Framework Manager está instalado, configure as seguintes propriedades de ambiente:

- **URI do Gateway**
- **URI do dispatcher para aplicativos externos**

Se a ferramenta de modelagem estiver utilizando um gateway dedicado em vez de se comunicar diretamente com o dispatcher, é necessário configurar também a propriedade **URIs de dispatchers do gateway** no computador de gateway dedicado.

Distribuindo Componentes do Transformer

O Transformer pode ser instalado em um computador que contém outros componentes do IBM Cognos Analytics ou em um computador que esteja separado de outros componentes do IBM Cognos Analytics. Quando instalado

separadamente, o Transformer pode ser usado como um produto independente ou pode ser configurado para se comunicar com outros componentes do IBM Cognos Analytics.

O Transformer consiste nos seguintes componentes. É possível ter um ou ambos, dependendo do ambiente.

- Transformer no Windows

  Esta é a ferramenta de modelagem do sistema operacional Microsoft Windows para projetar os PowerCubes que são usados no IBM Cognos Analytics. Também pode ser utilizado para criar e publicar PowerCubes.
- Transformer no UNIX ou Linux

  Este é o utilitário de linha de comandos para a construção de PowerCubes nos sistemas operacionais UNIX e Linux. Primeiro você projeta os modelos usando o Transformer Windows ou scripts MDL e depois usa os modelos para a construção de PowerCubes.

  Instale os componentes de construção do Transformer PowerCube para Linux on System z.

Recursos Suportados

Ao utilizar o Transformer como um produto independente, é possível usar origens de dados que são externas para o IBM Cognos Analytics e não é possível criar visualizações protegidas com filtragem dimensional. Ao usar o Transformer com outros componentes do IBM Cognos Analytics, é possível usar os seguintes recursos fornecidos pelo IBM Cognos Analytics:

- Provedores de autenticação do IBM Cognos Analytics
- Origens de dados do IBM Cognos Analytics, como pacotes publicados, relatórios do Query Studio e relatórios do Relatórios

  Não é possível utilizar arquivos simples como origens de dados.
- O portal para publicação da origem de dados e do pacote do PowerCube
- construção de PowerCubes

Considerações do Servidor Baseado em Função

Você pode querer configurar os servidores dedicados do Transformer para obter o desempenho de construção do cubo ideal e acessibilidade para usuários do IBM Cognos Analytics. Nesse cenário, considere os seguintes requisitos:

- O software cliente de banco de dados é instalado em qualquer computador em que o Transformer será utilizado para criar PowerCubes ou testar origens de dados.
- Para conectividade de origem de dados, configure variáveis de ambiente apropriadas para servidores UNIX and Linux.
- Os servidores IBM Cognos Analytics têm acesso ao local no qual os PowerCubes são armazenados, para que o servidor de relatório possa acessar os PowerCubes.

A construção e atualização de PowerCubes de produção podem ter scripts e ser executados remotamente quando houver acesso e privilégios de usuário suficientes. Para obter mais informações sobre como criar e atualizar PowerCubes de produção, consulte o Transformer *User Guide*.

Analistas ou Especialistas de Negócios

Pode-se ter negócios especializados ou usuários com poder que podem criar PowerCubes modelados em uma combinação de origens de dados pessoais e corporativas. Esses usuários podem fazer sua própria análise dos dados para sua linha de negócio ou pequeno grupo de usuários. É possível permitir que tais usuários sejam auto-suficientes dentro da infra-estrutura de TI e de segurança da organização atendendo aos seguintes requisitos:

- O software do cliente de banco de dados está instalado, ou disponível para ser instalado pelos modeladores, nos computadores que têm o Transformer e que são usados para acessar origens de dados do IBM Cognos Analytics ou origens de dados IQD do IBM Cognos Series 7.
- Modeladores devem ter privilégios para criar uma origem de dados no IBM Cognos Administration.

  Modeladores não precisam de acesso direto ao IBM Cognos Administration. Eles podem criar e atualizar origens de dados utilizando o ferramentas do Transformer ou de linhas de comandos. É possível fornecer modeladores com uma pasta assegurada no portal no qual publicar pacotes do PowerCube.
- Os modeladores devem ter acesso a uma localização na qual armazenar PowerCubes depois de criá-los.

  Esse local também deve estar acessível para o serviço do IBM Cognos e pode ser um compartilhamento protegido em uma LAN.
- Para criar PowerCubes em um servidor Transformer específico, os modeladores devem ter privilégios de FTP para transferir modelos e executar privilégios para criar cubos nesse servidor.

  Os modeladores podem transferir modelos e executar criações de cubo utilizando scripts. Os modeladores podem também utilizar métodos automatizados para criar PowerCubes. Para obter mais informações, consulte o *Guia de administração e segurança*.

Requisitos de Configuração

Para publicar pacotes PowerCubes, configure o Transformer para se comunicar com o dispatcher, tanto diretamente como através de um gateway dedicado. Se o IBM Cognos Connection estiver assegurado, será necessário ter privilégios para criar origens de dados e publicar pacotes no portal.

No computador em que o Transformer está instalado, configure as seguintes propriedades de ambiente:

- **URI do Gateway**
- **URI do dispatcher para aplicativos externos**

Se a ferramenta de modelagem estiver utilizando um gateway dedicado em vez de se comunicar diretamente com o dispatcher, é necessário configurar também a propriedade **URIs de dispatchers do gateway** no computador de gateway dedicado.

Opções de Distribuição para o Cognos Mobile

O IBM Cognos Mobile é um componente integrado da arquitetura do IBM Cognos Analytics. É possível instalar todos os componentes do IBM Cognos Mobile em um computador, ou distribuí-los em uma rede.

O Cognos Mobile consiste nos componentes a seguir:

- Componentes da camada de aplicativos
- O aplicativo Cognos Mobile.

Os Componentes da camada de aplicativos do Cognos Mobile devem ser instalados com os Componentes da camada de aplicativos do Cognos Analytics.

Todos os componentes necessários são instalados e ativados por padrão.

Componentes do Cognos Mobile Instalados em Um Computador

É possível instalar e configurar o IBM Cognos Mobile em um único computador.

O diagrama a seguir mostra um exemplo em que todos os componentes do servidor estão instalados em um computador.

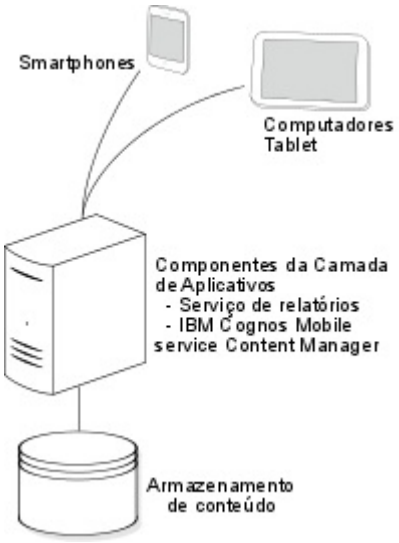


Figura 5. Componentes do Servidor do Cognos Mobile Instalados em Um Computador

Componentes do Cognos Mobile Instalados em Computadores Separados

Distribua os componentes do IBM Cognos Mobile usando o mesmo método de instalação e configuração usado para distribuir os componentes do IBM Cognos Analytics.

Execute a instalação em cada computador e, em seguida, conclua a configuração, especificando a localização dos componentes distribuídos do IBM Cognos Analytics.

Em uma instalação distribuída, você instala os componentes da camada de aplicativos do Cognos Mobile nos sistemas em que deseja executar o serviço do Cognos Mobile.

Todas as instâncias do serviço do IBM Cognos Mobile devem ser capazes de acessar o banco de dados onde as tabelas do IBM Cognos Mobile são armazenadas. Se não houver uma instância de servidor do IBM Cognos Analytics configurada com os detalhes do banco de dados para o armazenamento de conteúdo do IBM Cognos ou se você quiser que o IBM Cognos Mobile use uma instância de banco

de dados diferente do armazenamento de conteúdo do IBM Cognos, use o IBM Cognos Configuration para incluir um banco de dados.

IBM Cognos Analytics com outros produtos IBM Cognos

É possível instalar o IBM Cognos Analytics em um ambiente que inclui outros produtos IBM Cognos.

O assistente de instalação do IBM Cognos Analytics pode reconhecer diretórios compatíveis e mostrar um aviso quando houver conflitos. Após a instalação do IBM Cognos Analytics, é possível acessar objetos que foram criados em outro produto IBM Cognos no IBM Cognos Analytics. As exigências de acesso dependem de como se escolhe executar os dois produtos.

Serviços Duplicados se Usando Diversos Produtos

Muitos produtos IBM Cognos usam serviços semelhantes, tais como o serviço de relatório e o serviço de apresentação. Se estiver usando vários produtos, como o IBM Cognos Analytics com o IBM Cognos PowerPlay, deve-se desativar alguns dos serviços duplicados para assegurar que seus produtos funcionarão corretamente.

Por exemplo, o IBM Cognos Analytics e o IBM Cognos PowerPlay estão instalados. Ambos os produtos têm um serviço de relatórios e um serviço de apresentação. Se ambos os produtos forem acessados por meio do mesmo gateway, os relatórios que devem ser executados nos serviços do IBM Cognos Analytics podem ser roteados para os serviços do IBM Cognos PowerPlay. O resultado pode ser que seus relatórios exibam um erro.

Produtos IBM Cognos que interoperam com o IBM Cognos Analytics

Alguns produtos IBM Cognos fornecem funcionalidades que não estão disponíveis no IBM Cognos Analytics. É possível usar esses produtos no mesmo ambiente que o IBM Cognos Analytics. Com alguns produtos, é possível acessar os diferentes tipos de cubos ou relatórios no portal do IBM Cognos Analytics. Com outros produtos, é possível acessar recursos exclusivos no portal do IBM Cognos Analytics.

Cognos Planning - Analyst

É possível acessar dados de plano publicados no IBM Cognos Analytics utilizando o assistente Gerar Modelo do Framework Manager, que requer o IBM Cognos Planning - Analyst 7.3 MR1 ou posterior.

Se desejar usar esse produto com o servidor IBM Cognos Analytics, assegure-se de que ambos os produtos sejam da mesma versão.

Para obter mais informações, consulte o Guia do Usuário do Analista do *IBM Cognos.*

Cognos Planning - Contributor

É possível acessar cubos não publicados (tempo real) do Contributor no IBM Cognos Analytics, instalando de forma customizada o componente do IBM Cognos Analytics - Contributor Data Server, que é incluído na liberação do IBM Cognos Planning - Contributor 7.3 MR1 ou posterior. É possível acessar dados de plano

publicados no IBM Cognos Analytics utilizando a extensão de administração Gerar Modelo do Framework Manager no Contributor, que requer o IBM Cognos Planning - Contributor 7.3 MR1 ou posterior.

Se desejar usar esse produto com o servidor IBM Cognos Analytics, assegure-se de que ambos os produtos sejam da mesma versão. Não é possível instalar o IBM Cognos Planning no mesmo caminho que o IBM Cognos Analytics de 64 bits.

Para obter mais informações, consulte *IBM Cognos Contributor: Guia de Administração*.

Cognos Controller

É possível acessar o IBM Cognos Analytics para criar Relatórios Padrão do IBM Cognos Controller utilizando um modelo de Framework Manager predefinido, que é criado quando o IBM Cognos Controller é instalado. Acesse também dados do Controller publicados e estruturas no Framework Manager para criação de relatórios padrão e análises.

Cognos Transformer

É possível usar o IBM Cognos PowerCubes e modelos do Transformer que foram gerados pelo Transformer 7.3 ou posterior diretamente no IBM Cognos Analytics. Os cubos e modelos são compatíveis com versões mais recentes e não necessitam de ferramentas de migração ou de atualização. É possível executar relatórios e análises no IBM Cognos Analytics com relação aos IBM Cognos PowerCubes.

Se quiser usar os novos recursos de integração do Transformer com o IBM Cognos Analytics, é possível fazer upgrade dos modelos do IBM Cognos Series 7.x Transformer para o IBM Cognos Analytics Transformer 8.4 ou posterior. Isso permite usar as origens de dados do IBM Cognos Analytics (como pacotes publicados), listar relatórios criados no Query Studio ou no Relatórios, autenticar usando a segurança do IBM Cognos Analytics e publicar diretamente no portal.

Antes do carregamento do modelo, o namespace do IBM Cognos Series 7 deve ser configurado no IBM Cognos Analytics e o ID do nome usado para configurá-lo no IBM Cognos Analytics deve corresponder ao nome usado no IBM Cognos Series 7.

Para obter mais informações sobre como fazer upgrade de PowerCubes protegidos do IBM Cognos Series 7, consulte o *Guia do usuário do IBM Cognos Analytics Transformer*.

Para que seja possível utilizar PowerCubes do IBM Cognos Series 7 no IBM Cognos Analytics, otimize os cubos para uso no IBM Cognos Analytics, usando o utilitário pcoptimizer, que é fornecido com o IBM Cognos Analytics. Caso contrário, os PowerCubes que foram criados com versões anteriores do Transformer podem demorar muito para serem abertos nos studios da web do IBM Cognos Analytics. Esse utilitário de otimização é adequado para PowerCuber antigos criados antes do Transformer 8.4 e não necessita de acesso ao modelo ou à origem de dados. Não é necessário executar este utilitário de linha de comandos para cubos criados no Transformer 8.4 ou posterior. Para obter mais informações sobre como otimizar PowerCubes, consulte o Transformer *User Guide*.

É possível publicar PowerCubes usando o Transformer 8.4, o Framework Manager ou diretamente no portal do IBM Cognos Analytics. É possível publicar origens de dados e pacotes únicos do PowerCube no portal de forma interativa no

Transformer ou na linha de comandos. Publique também no modo silencioso usando scripts em lote após criar um PowerCube. Um usuário que tem privilégios para criar origens de dados e pacotes no portal também podem publicar PowerCubes no portal. O arquivo MDC deve estar em um local seguro que possa ser acessado pelo dispatcher do IBM Cognos Analytics e pelo processo do servidor de relatório. Os pacotes que usam diversos PowerCubes de definições diferentes de PowerCube ou PowerCubes misturados a outras origens de dados devem ser publicados usando o Framework Manager.

Se você usar um PowerCube do IBM Cognos Series 7 como origem de dados, o IBM Cognos Analytics converterá os dados do cubo da codificação que foi usada no sistema no qual o PowerCube foi criado. Para uma conversão bem-sucedida, os IBM Cognos Series 7 PowerCubes devem ser criados com um código de idioma do sistema configurado para corresponder aos dados no PowerCube.

Cognos Lifecycle Manager

O Lifecycle Manager é um aplicativo baseado em Windows que faz auditoria de upgrades do Cognos 8 e superior para versões mais recentes do IBM Cognos Analytics. Ele fornece um recurso de verificação que valida, executa e compara os resultados do relatório de duas liberações diferentes do IBM Cognos Analytics. Isso ajuda a identificar problemas de atualizações e compatibilidade entre versões. O design da interface com o usuário e o recurso de informações do estado fornecem um processo de prática comprovada e suporte ao planejamento de projetos de atualização e a informações de status.

Para obter mais informações, consulte o *IBM Cognos Lifecycle Manager User Guide*.

Planning Analytics

O IBM Planning Analytics integra o planejamento de negócios, a medida de desempenho e os dados operacionais para permitir que as empresas otimizem a efetividade de negócios e a interação do cliente, independentemente da geografia ou estrutura. O Planning Analytics fornece visibilidade imediata nos dados, prestação de contas em um processo colaborativo e uma visualização consistente de informações, permitindo que os gerenciadores estabilizem rapidamente as flutuações operacionais e aproveitem as novas oportunidades.

Para obter mais informações, consulte a documentação do *IBM Planning Analytics*.

Capítulo 3. Upgrade do IBM Cognos Analytics

Os aprimoramentos nas novas versões do IBM Cognos Analytics podem afetar muitas partes de seu ambiente de inteligência de negócios. Portanto, é melhor executar o upgrade em estágios. Para assegurar o sucesso, trate o upgrade como um projeto de TI que requer planejamento cuidadoso, tempo adequado e recursos adequados.

Website do Cognos Upgrade Central

O website Cognos Upgrade Central (www-01.ibm.com/support/docview.wss?uid=swg22011664) fornece informações adicionais para ajudá-lo a fazer upgrade. Por exemplo, as perguntas mais frequentes, os vídeos de demonstração e os links para recursos adicionais estão disponíveis no website.

Processo de Upgrade

Cada upgrade requer um plano e cada plano segue o mesmo processo de upgrade básico.

Você deve planejar seu upgrade para que saiba o que esperar em cada estágio do processo. No estágio de planejamento, reveja a documentação de atualização para informações sobre comportamento esperado, novos recursos, recursos descontinuados, compatibilidade entre versões e exigências para preparar seu ambiente de produção. Quando terminar a revisão, conduza uma pesquisa local para identificar a infra-estrutura do BI, aplicativos, relatórios e definições de configuração customizadas. Finalmente, é possível testar o upgrade em um subconjunto de dados, para que seja possível otimizar os relatórios e os dados antes de assumir compromisso com o upgrade integral.

Ao planejar seu upgrade, assegure-se de executar as tarefas a seguir:

- Reúna as informações necessárias, como entradas necessárias e saídas esperadas para cada fase.
- Avalie os aplicativos em seu ambiente de relatório e agrupe os relatórios semelhantes.
- Instale o novo software em um ambiente de teste e implemente o conteúdo para o ambiente de teste.
- Teste os aplicativos atualizados para assegurar que seus relatórios são executados conforme o esperado.

  É possível usar o Lifecycle Manager para comparar relatórios de uma versão diferente do IBM Cognos Analytics. Para obter mais informações, consulte a documentação do Lifecycle Manager.

A implantação e o teste são em geral um processo repetitivo. Avalie as diferenças entre os ambientes de origem e de destino. Vá até seu ambiente de produção quando estiver certo de que os aplicativos implantados tenham correspondido às suas exigências de negócios.

O diagrama a seguir mostra um fluxo de trabalho de upgrade geral e os estágios no processo de upgrade. O processo inclui os estágios a seguir:

- Criar um plano de upgrade, que inclua as atividades a seguir:

- Revisão de recursos, como a documentação, o Upgrade do website central (www.ibm.com/support/docview.wss?uid=swg22011664) e as seguintes etapas de upgrade: http://www-01.ibm.com/support/docview.wss?uid=swg21994915
- Verificar os ambientes suportados para garantir a compatibilidade com outros software acessando os IBM Software Product Compatibility Reports (www.ibm.com/support/docview.wss?uid=swg27047186). Você também pode querer verificar esta página se estiver pensando em atualizar o sistema operacional.
- Avaliar seu sistema existente para determinar se deseja mover sua nova versão do produto.
- Criar um plano detalhado para implementar sua estratégia de upgrade.

• Criar um desenvolvimento ou sistema de teste com a nova versão do produto.
• Usar as informações aprendidas do desenvolvimento ou sistema de teste e aplicá-las conforme cria seu QA ou sistemas de produção.

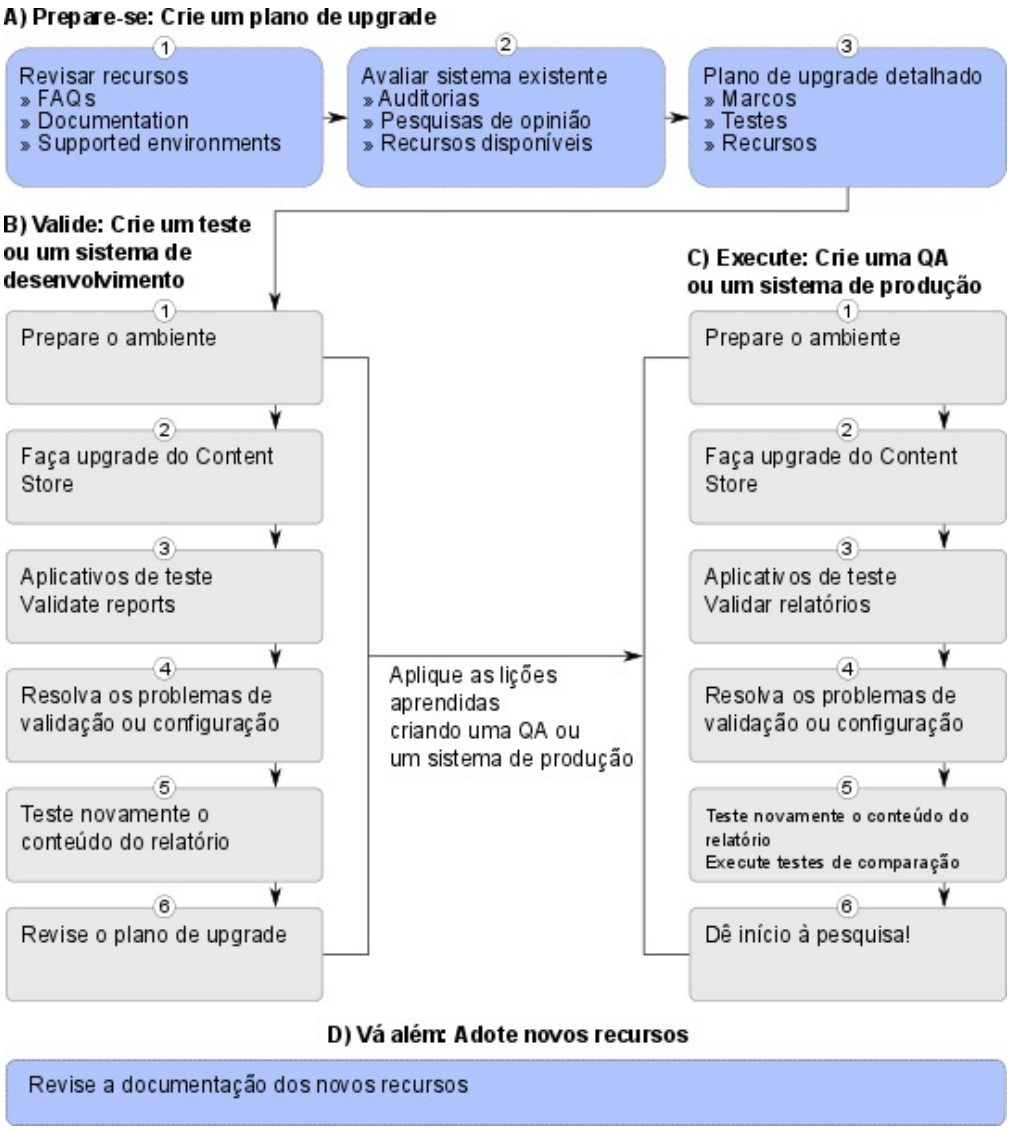


Figura 6. Processo de Upgrade

Revisando a Documentação

A documentação é fornecida de várias fontes para ajudá-lo a executar um upgrade com êxito.

Toda a documentação está disponível on-line no IBM Cognos Knowledge Center (http://www.ibm.com/support/knowledgecenter/SSEP7J_11.0.0/com.ibm.swg.ba.cognos.cbi.doc/welcome.html).

Aplicativos de Avaliação em seu Ambiente antes do Upgrade

A preparação para o upgrade fornece uma oportunidade de revisar seus aplicativos existentes e limpar o ambiente de origem.

Por exemplo, você pode ter vários aplicativos em seu ambiente. No entanto, não é raro localizar diversos aplicativos não usados ou que não atendem mais aos requisitos.

Avaliar os seus aplicativos é um exercício útil porque pode reduzir o número de aplicativos a serem considerados durante um upgrade.

Uma auditoria de seus aplicativos existentes pode incluir as tarefas a seguir:

- Execute uma pesquisa de opinião do site para avaliar o ambiente de produção atual e identificar as áreas que requerem atenção durante o upgrade. A pesquisa do site inclui informações sobre a infraestrutura, os aplicativos, os usuários e as definições de configuração.
- Avalie o software que você usa em seu ambiente e crie uma lista do software, como sistemas operacionais, servidores da web, provedores de segurança e bancos de dados.

  Para revisar uma lista atualizada de ambientes suportados pelos produtos do IBM Cognos Analytics, incluindo informações sobre sistemas operacionais, correções, navegadores, servidores da web, servidores de diretório, servidores de banco de dados e servidores de aplicativos, consulte a página IBM Software Product Compatibility Reports (www.ibm.com/support/docview.wss?uid=swg27047186).
- Complete uma avaliação detalhada de seus aplicativos. A utilização, idade, o tamanho e a complexidade de seus aplicativos são fatores importantes de se considerar ao planejar a atualização. O tamanho total dos aplicativos pode ter um impacto no tempo necessário para concluir o upgrade.
- Liste as seguintes informações sobre suas configurações:
  - As definições de configuração que você ativou no IBM Cognos Configuration

    Instalar a nova versão do produto em um local diferente da versão existente permite comparar as definições entre as duas versões. Para executar as duas versões, você deve assegurar-se de usar os números de porta exclusivos, os alias do servidor da web e os bancos de dados de armazenamento de conteúdo.
  - Mudanças em outros arquivos de configuração

    Você deve alterar manualmente os outros arquivos de configuração durante o upgrade. Se alterou outros arquivos de configuração. avalie as mudanças que deseja preservar no ambiente atualizado. Isso pode incluir os arquivos `.xml`, `.txt` e `.css` nos diretórios `configuration`, `templates`, `webapps` e `webcontent`.

    Nota: Se você modificou os arquivos `.ini`, entre em contato com o Suporte ao Cliente para determinar se as mudanças são suportadas na versão do software.

- Faça backup do seu banco de dados de armazenamento de conteúdo.

Depois que a sua auditoria for concluída, será possível criar um plano de upgrade.

Diretrizes ao Atualizar o Sistema Operacional

Você pode querer considerar as diretrizes a seguir antes de fazer upgrade para uma versão posterior do sistema operacional nos computadores nos quais o IBM Cognos Analytics está instalado:

- Verifique o IBM Software Product Compatibility Reports (www.ibm.com/support/docview.wss?uid=swg27047186) para certificar-se de que a versão do IBM Cognos Analytics suporte a versão do sistema operacional para a qual você está pensando em mudar.
- Certifique-se de que o software de terceiros utilizado pelo IBM Cognos Analytics seja suportado na versão do sistema operacional proposto. O software de terceiros incluiria componentes como banco de dados e driver de banco de dados, servidores de aplicativos, servidores da web e navegadores.
- Determine se você deve recompilar os aplicativos SDK do IBM Cognos Analytics.
- Determine se você deve recriar as implementações da web, que incluem os arquivos do archive web (.war) e os arquivos do archive corporativo (.ear).

Pastas e arquivos preservados ao fazer upgrade do Cognos Analytics

É possível instalar uma nova versão do IBM Cognos Analytics sobre sua versão do produto atual em execução sem sobrescrever as definições de configuração da versão anterior.

Os arquivos a serem preservados durante um upgrade estão listados no arquivo *install_location*\configuration\preserve\.ca_base_preserve.txt. Não edite este arquivo. Em vez disso, edite o arquivo *install_location*\configuration\preserve\preserve.txt, se você deseja remover ou preservar determinados arquivos ou diretórios durante o upgrade. Instruções sobre como usar o preserve.txt são incluídas no próprio arquivo.

Dica: Hard ou soft links que são criados por clientes dentro da estrutura de arquivo Cognos Analytics não são suportados.

Por padrão, as seguintes pastas e arquivos são preservados ao fazer upgrade do Cognos Analytics:

Pastas *install_location*\data

install_location\deployment

install_location\drivers

install_location\ldapschema

install_location\informix

install_location\configuration\certs

install_location\configuration\csk

install_location\configuration\data

install_location\webcontent\bi\alp\images

install_location\webapps\p2pd\WEB-INF\AAA\lib

arquivos de configuração

install_location\configuration\cogconfig.prefs

install_location\configuration\cogconfig_reg.txt

install_location\configuration\coglocale.xml

install_location\configuration\cogstartup.xml

install_location\configuration\dispatcher.properties

install_location\configuration\install_gatewayurl.xml

install_location\configuration\installData.properties

install_location\configuration\ipfclientconfig.xml

install_location\configuration\configuration\caSerial

install_location\configuration\xqe.diagnosticlogging.xml

Arquivos diversos

install_location\webapps\p2pd\WEB-INF\web.xml

install_location\wlp\usr\servers\cognosserver\bootstrap.properties

install_location\wlp\usr\servers\cognosserver\jvm.options

install_location\wlp\usr\servers\cognosserver\server.xml

install_location\cgi-bin\web.config

install_location\webcontent\web.config

install_location\webcontent\default.htm

install_location\webcontent\index.html

install_location\webcontent\bi\web.config

Arquivos TM1

install_location\templates\ps\portal\variables_TM1.xml

install_location\templates\ps\portal\variables_plan.xml

install_location\templates\ps\portal\icon_active_application.gif

install_location\webcontent\planning.html

install_location\webcontent\tm1\web\tm1web.html

install_location\templates\ps\system.xml

install_location\templates\ps\portal\system.xml

Arquivos PowerPlay

install_location\webcontent\skins\series7\ppwb

install_location\webcontent\skins\presentation\ppwb

install_location\webcontent\skins\modern\ppwb

install_location\webcontent\skins\corporate\ppwb

install_location\webcontent\skins\contemporary\ppwb

install_location\webcontent\skins\classic\ppwb

install_location\webcontent\skins\business\ppwb

install_location\webcontent\bi\skins\series7\ppwb

install_location\webcontent\bi\skins\presentation\ppwb

install_location\webcontent\bi\skins\modern\ppwb

install_location\webcontent\bi\skins\corporate\ppwb

install_location\webcontent\bi\skins\contemporary\ppwb

install_location\webcontent\bi\skins\classic\ppwb

install_location\webcontent\bi\skins\business\ppwb

install_location\webcontent\bi\ppwb

install_location\webcontent\ps\powerplaystudio

install_location\webcontent\fragments\ppesAdmin

install_location\webcontent\ppwb

install_location\webapps\p2pd\WEB-INF\fragments\applications\
cogadmin\pages\ppesAdminPage.xml

install_location\webapps\p2pd\WEB-INF\fragments\applications\
cogadmin\fragments\ppesAdmin.xml

install_location\msgsdk\ppesAdminStrings_en.xml

install_location\msgsdk\ppesAdminStrings_ldkspec.xml

install_location\eclipse\plugins\
org.eclipse.equinox.cm_1.0.400.v20120522-1841.jar

install_location\eclipse\plugins\
org.eclipse.equinox.ds_1.4.1.v20120926-201320.jar

install_location\eclipse\plugins\
org.eclipse.equinox.event_1.2.200.v20120522-2049.jar

install_location\eclipse\plugins\
org.eclipse.equinox.util_1.0.400.v20120917-192807.jar

install_location\eclipse\plugins\
org.eclipse.osgi.services_3.3.100.v20120522-1822.jar

install_location\eclipse\plugins\
org.eclipse.osgi.util_3.2.300.v20120913-144807.jar

Arquivos LCM

install_location\wlp\usr\servers\lcm\server.xml

install_location\project

install_location\benchmarks

install_location\configuration

É necessário migrar manualmente esses arquivos e pastas somente sob as seguintes circunstâncias:

- Você está instalando a nova versão em um novo diretório.
- Você está desinstalando a versão atual e, em seguida, instalando a nova versão. A desinstalação da versão atual exclui completamente o diretório *install_location*.

Tarefas de Atualização

Ao atualizar, execute as tarefas a seguir:

1. Instale e configure a nova versão do produto.

2. Mova seu conteúdo para a nova versão do produto.
3. Atualize suas especificações de relatório.
4. Compare o seu conteúdo atualizado para o conteúdo existente para assegurar a consistência.

Instalar e Configurar uma Nova Versão do Produto

Instale a nova versão do produto em um novo local. O local pode ser no mesmo computador que sua versão existente do produto ou em outro computador.

Instalar em um novo local permite manter sua versão existente do produto e executá-la além da nova versão do produto. Isso pode ajudar você a testar sua nova versão sem afetar sua versão existente. É possível comparar as definições de configuração entre a versão e comparar a aparência e a funcionalidade dos relatórios em ambos os ambientes para assegurar a equivalência.

Executando várias versões ou instâncias do IBM Cognos Analytics no mesmo computador:

Para ter diversas verões ou instâncias do IBM Cognos Analytics no mesmo computador, você deve alterar a configuração para assegurar que as versões não compartilhem números de porta ou outros recursos.

Mudanças Necessárias na Configuração para Executar Diversas Versões no Mesmo Computador

Para executar várias versões do IBM Cognos Analytics no mesmo computador, certifique-se de que cada instalação seja distinta. As versões ou instâncias devem se instaladas em diretórios diferentes. As definições de configuração para cada versão deve usar diferentes configurações para as seguintes propriedades de configuração.

Configurações de Portas e de URI

Se estiver usando o servidor de aplicativos padrão, será necessário usar números de porta diferentes de 9300 para evitar conflitos de porta. O IBM Cognos Analytics reserva um intervalo de números de porta, portanto, deve-se assegurar o uso de um deslocamento de pelo menos 100 para o número da porta. Por exemplo, se você estiver usando o número de porta padrão, 9300, para uma instância do IBM Cognos Analytics. Para uma segunda instalação no mesmo computador, deve-se alterar o número da porta para pelo menos 9400. Não use os mesmos números de porta para ambas as instalações.

Altere as portas a seguir.

- URIs de dispatchers do gateway
- URI do dispatcher externo
- URI do dispatcher interno
- URI do Dispatcher para Aplicativos Externos
- URIs do Content Manager
- Número da porta do servidor de log local

Se estiver instalando o produto em um servidor de aplicativos diferente do fornecido com o IBM Cognos Analytics, assegure-se de instalar a nova versão em um novo perfil de servidor de aplicativos ou em uma instância separada da versão existente.

Armazenamento de conteúdo

Use um armazenamento de conteúdo ou esquema diferentes para cada

instalação. Não é possível reverter o conteúdo após ele ser atualizado. É possível usar uma cópia restaurada do armazenamento de conteúdo existente como o armazenamento de conteúdo para a versão mais recente do IBM Cognos Analytics. A versão mais recente do produto atualiza o armazenamento de conteúdo quando você inicia os serviços.

Diretórios virtuais do servidor da web opcional

Para visualizar o conteúdo estático do IBM Cognos Analytics, os diretórios virtuais para o servidor da web devem ser diferentes para cada versão. Assegure-se de atualiza o URI do Gateway no Cognos Configuration para refletir os nomes dos diretórios virtuais.

Por exemplo, o diretório virtual padrão é `http://servername/ibmcognos`. Se tiver dois gateways instalados no mesmo computador, você deve alterar o diretório virtual `ibmcognos` para um dos gateways.

Conjuntos de Aplicativos (Servidor da Web do Microsoft IIS)
Se você usar `cognosisap.dll`, cada gateway deve usar um conjunto de aplicativos separado.

Conta do Usuário que Inicia o Serviço (Opcional)
Alterar a conta do usuário pode ser útil quando você estiver solucionando os problemas. Por exemplo, é possível solucionar problemas de processos Java pelo proprietário.

Definições de Configuração que São Iguais para Diversas Versões do Mesmo Servidor

Diversas instâncias ou versões do IBM Cognos Analytics executadas no mesmo computador usam os mesmos recursos, como memória, rede e espaço em disco.

Diversas versões do IBM Cognos podem usar a fonte de autenticação para ambas as versões. É possível configurar propriedades idênticas para o namespace.

Arquivos de Configuração Customizados

Se você editou manualmente alguns arquivos de configuração, deve reaplicar as mudanças. Mantenha um registro de quaisquer customizações para assegurar que possam ser reaplicadas após seu upgrade. Além disso, faça backup desses arquivos para que a versão original possa ser restaurada, se necessário.

O serviço de apresentação do IBM Cognos Analytics suporta o upgrade automático de alguns arquivos `system.xml`. Se tiverem sido feitas muitas customizações nos arquivos `system.xml`, é possível usar este recurso de upgrade automático em vez de reaplicar as mudanças manualmente após o upgrade. Ao substituir os arquivos `system.xml` pelos arquivos da sua versão anterior do produto, os arquivos poderão ser atualizados pela nova versão do produto. O upgrade automático é aplicado ao iniciar o serviço do IBM Cognos.

Os arquivos `system.xml`, para os quais o upgrade automático é suportado, estão nos diretórios a seguir:

- *install_location*`/templates/ps`
- *install_location*`/templates/ps/portal`
- *install_location*`/templates/ps/qs`

Configurando uma segunda instância do IBM Cognos Analytics em um computador:

Para ter mais de uma instância do IBM Cognos Analytics em um computador, você deve configurar cada instância com valores exclusivos para as portas, o diretório virtual do servidor da web e o banco de dados de armazenamento de conteúdo.

Antes de Iniciar

Para a nova versão do produto, é necessário um novo armazenamento de conteúdo. Se você estiver atualizando seu armazenamento de conteúdo inteiro, crie um armazenamento de conteúdo a partir de um backup do seu armazenamento de conteúdo existente. Se você estiver movendo seu conteúdo com arquivos de implementação, é possível criar um banco de dados de armazenamento de conteúdo em branco.

Assegure-se de ter seu novo banco de dados de armazenamento de conteúdo antes de configurar a nova versão do produto.

Importante: Se você estiver se conectando a um backup do seu armazenamento de conteúdo, na primeira vez que iniciar os seus serviços IBM Cognos, será solicitado que atualize seus relatórios. Atualizar seus relatórios pode demorar e é melhor atualizá-los depois que tiver a nova versão em execução. É possível atualizar seus relatórios depois usando o IBM Cognos Administration.

Procedimento

1. Para a nova instância do IBM Cognos Analytics, inicie o IBM Cognos Configuration.
2. Na janela **Explorer**, clique em **Ambiente**.
3. Assegure-se de que os números de porta para as configurações a seguir não entrem em conflito com outra instância ou versão do IBM Cognos Analytics:
   - **URIs de dispatchers do gateway**
   - **URI do dispatcher externo**
   - **URI do dispatcher interno**
   - **URI do dispatcher para aplicativos externos**
   - **URIs do Content Manager**
4. Assegure-se de que o **URI do gateway** use um diretório virtual ou alias diferente da outra instância ou versão do IBM Cognos Analytics.
5. Clique em **Criação de Log** e assegure-se de que o **Número de Porta do Servidor de Log Local** seja exclusivo.
6. Se você estiver usando o Portal Services, atualize o local do arquivo `applications.xml`:
   - Na janela **Explorer**, clique em **Ambiente** > **Portal Services**.
   - Na janela **Propriedades**, assegure-se de que o número da porta para a propriedade **Location of applications.xml** corresponda ao número da porta para outras propriedades de URI.
7. Na janela **Explorer**, em **Acesso a dados** > **Content Manager**, assegure-se de não usar o mesmo armazenamento de conteúdo usado para outra instância ou versão do IBM Cognos Analytics.
8. Salve a configuração e inicie o IBM Cognos Analytics.

Mover Seu Conteúdo para a Nova Versão do Produto

Existem dois métodos para mover o seu conteúdo. É possível mover todo o armazenamento de conteúdo ou o conteúdo criando archives de implementação.

Mova o seu Armazenamento de Conteúdo Inteiro

Este método requer que você faça backup do armazenamento de conteúdo existente e, em seguida, restaure o backup para um novo armazenamento de conteúdo. Em seguida, conecte sua nova versão do produto para o armazenamento de conteúdo restaurado e o produto atualiza o armazenamento de conteúdo para a nova versão.

Este método mantém toda a sua segurança e preferências do usuário, mas requer um novo banco de dados de armazenamento de conteúdo.

Ao configurar a segurança, certifique-se de configurar o identificador exclusivo para o mesmo valor que ele tinha na liberação da qual você está fazendo o upgrade, caso contrário, as configurações de segurança serão perdidas.

Execute uma verificação de consistência em seu armazenamento de conteúdo antes de fazer o upgrade para garantir que não há inconsistências. Para obter mais informações, consulte o tópico "Crie uma Tarefa de Manutenção de Armazenamento de Conteúdo" no *Guia de Administração e Segurança do IBM Cognos Business Intelligence*.

Importante: Ao usar este método, na primeira vez que iniciar os serviços IBM Cognos, será solicitado que atualize seus relatórios. Atualizar seus relatórios pode demorar e é melhor atualizá-los depois que tiver a nova versão em execução. Além disso, se você tiver aplicativos do Kit de Desenvolvimento de Software que criem, modifiquem ou salvem as especificações de relatório, não selecione a opção para atualizar suas especificações de relatório. É possível atualizar seus relatórios depois usando o IBM Cognos Administration.

Além disso, você deve assegurar-se de remover o registro de quaisquer dispatchers de sua versão anterior do produto. Isso pode ser feito usando o IBM Cognos Administration depois de você ter iniciado os serviços.

Atenção:

Os arquivos e módulos de dados transferidos por upload no modo de captura instantânea (antes de 11.0.4) são salvos no sistema de arquivos. Esses arquivos de dados **não são armazenados no armazenamento de conteúdo** ou em outro banco de dados. O local padrão para esses arquivos de dados é *install_location*\data\datafiles. Assegure-se de fazer backup desses arquivos antes de desinstalar ou fazer upgrade sobre uma instalação existente e, em seguida, certifique-se de restaurá-los no novo local.

Mova o Conteúdo Criando Arquivos de Implementação

É possível mover o conteúdo criando os arquivos de implementação.

Este método permite mover o conteúdo específico, mas pode demorar para um grande armazenamento de conteúdo.

Se você estiver alterando os fornecedores de banco de dados de armazenamento de conteúdo, deve criar as implementações para mover o seu conteúdo. Por exemplo,

se você estiver mudando seu armazenamento de conteúdo do Microsoft SQL Server para o IBM Db2, isso deverá ser feito com arquivos de implementação.

Considerações para Ambos os Métodos

Não há requisito para trazer as tabelas NC existentes durante um upgrade, pois o sistema os sincronizará novamente. Já que há um requisito para que as tabelas da fila estejam vazias, considere não usar as tabelas NC existentes ao executar o upgrade.

As tabelas NC devem ser completamente esvaziadas antes de executar o upgrade.Execute o `NC_DROP_`*`Database_Type`*`.sql` apropriado antes de fazer upgrade.

Como parte do processo de atualização, verifique se seus aplicativos funcionam como esperado na nova versão. Às vezes, as mudanças podem apresentar resultados inesperados. É importante testar os seus aplicativos com a nova versão do produto antes de movê-los para o ambiente de produção.

Atualizar seu Armazenamento de Conteúdo

O IBM Cognos Analytics faz upgrade do banco de dados de armazenamento de conteúdo para a nova versão do produto quando os serviços são iniciados pela primeira vez.

O processo de atualizar o upgrade para a nova versão do produto inclui as etapas a seguir:

1. Fazer um backup de seu banco de dados de armazenamento de conteúdo existente.
2. Criar um banco de dados do backup.
3. Conecte a nova versão do produto ao armazenamento de conteúdo que você criou a partir do backup no IBM Cognos Configuration.
4. Inicie os seus serviços.

   O armazenamento de conteúdo é atualizado durante o processo de inicialização.

   Dica: Ao reiniciar manualmente os serviços, (se aplicável) o serviço **ApacheDS - cognos** deve ser iniciado antes do serviço **IBM Cognos**.

Este processo permite que você use as versões nova e antiga do produto ao mesmo tempo, onde cada versão possui seu próprio armazenamento de conteúdo.

Ao usar este método, na primeira vez que iniciar os serviços IBM Cognos, será solicitado que atualize seus relatórios. Atualizar seus relatórios pode demorar e é melhor atualizá-los depois que tiver a nova versão em execução. É possível fazer upgrade de seus relatórios com o IBM Cognos Administration. Além disso, se você tiver aplicativos do Kit de Desenvolvimento de Software que criem, modifiquem ou salvem as especificações de relatório, não selecione a opção para atualizar suas especificações de relatório.

Quando você conecta a nova versão do produto ao armazenamento de conteúdo criado a partir do backup, o banco de dados de armazenamento de conteúdo é atualizado e não pode mais ser usado com sua antiga versão do produto.

Cancelar Registro de Dispatchers da Versão Anterior do seu Armazenamento de Conteúdo:

Se você usar um backup do armazenamento de conteúdo existente com uma nova versão do produto, você deve cancelar o registro dos dispatchers da versão anterior.

Procedimento

1. Em **Gerenciar** > **Console de administração**, abra o IBM Cognos Administration.
2. Clique em **Configuração** e, em seguida, clique em **Dispatchers e Serviços**.
3. Clique em **Mais** para os dispatchers pertencentes à versão anterior.
4. Clique em **Cancelar Registro** e, em seguida, clique em **OK**.

   As informações do dispatcher serão removidas do armazenamento de conteúdo.

Movendo o Conteúdo com um Arquivo de Implementação

Para mover o conteúdo específico do armazenamento de conteúdo é possível usar os arquivos de implementação. Os arquivos de implementação são arquivos compactados que é possível importar para a sua nova versão do produto.

Importante: Se você moveu o seu conteúdo restaurando seu armazenamento de conteúdo existente, não precisará mover o conteúdo usando os arquivos de implementação.

Mover o conteúdo com arquivos de implementação envolve as etapas a seguir:

1. Criar um archive.
2. Copiar o archive para a nova versão do produto.
3. Importar o conteúdo.

Criando um Arquivo de Implementação:

Use a tarefa a seguir para criar um arquivo de implementação.

Procedimento

1. Em **IBM Cognos Administration**, na guia **Configuração**, clique em **Administração de Conteúdo**.
2. Na barra de ferramentas, clique no ícone **Nova Exportação**  .
3. Insira **Nome** para o archive.
4. Selecione o conteúdo que você deseja incluir no archive:
   - Para exportar pastas específicas e conteúdo de diretório, clique em **Selecionar Pastas Públicas e Conteúdo de Diretório**.
   - Para exportar o armazenamento de conteúdo inteiro, clique em **Selecionar o Armazenamento de Conteúdo Inteiro**. Se selecionar o armazenamento de conteúdo inteiro, também poderá selecionar **Incluir Informações de Contas dos Usuários**.
5. Clique em **Avançar**.
6. Se você clicou em **Selecionar o Armazenamento de Conteúdo Inteiro**, insira uma senha a ser usada ao importar o conteúdo e, em seguida, clique em **OK**.
7. Se você clicou em **Selecionar Pastas Públicas e Conteúdo do Diretório**:
   a. No painel **Selecionar Conteúdo das Pastas Públicas**, clique em **Incluir**.

b. No painel **Selecionar Entradas**, na caixa **Entradas Disponíveis**, selecione os pacotes ou pastas que deseja exportar.

   É possível procurar na hierarquia de Pastas Públicas e escolher os pacotes e pastas desejados. Clique no ícone **Incluir**  para mover os itens selecionados para a caixa **Entradas Selecionadas** e clique em **OK**.

c. Para cada pacote e pasta que você exportar, faça o seguinte, e, em seguida, clique em **Avançar**:
   - Se você desejar fazer qualquer mudança no pacote ou na pasta no ambiente de destino, clique no ícone **Editar**  , faça as mudanças e clique em **OK**.
   - Para restringir o acesso ao pacote ou pasta e às entradas correspondentes, assinale a caixa de seleção na coluna **Desativar após importação**. Isso é útil quando desejar testar os relatórios antes de disponibilizá-los no ambiente de destino.
   - Em **Opções**, selecione se deseja incluir as versões de saída de relatório, executar o histórico e programações, e o que fazer com as entradas quando há um conflito.

d. No painel **Selecionar o Conteúdo do Diretório**, selecione as opções desejadas e clique em **Avançar**.

e. No painel **Especificar Opções Gerais**, selecione as opções desejadas e clique em **Avançar**.

f. No painel **Especificar um Arquivo de Implementação**, selecione um arquivo de implementação existente a partir da lista ou crie um.

   Se estiver digitando um novo nome para o arquivo de implementação, não use espaços no nome. Se o nome da nova especificação de implementação corresponder ao nome de um arquivo de implementação existente, o arquivo de implementação existente será sobrescrito.

8. Revise as informações de resumo e depois clique em **Avançar**.
9. Em **Ações**, selecione **Salvar e Executar Uma Vez**.
10. No painel **Executar com Opções**, selecione **Agora** e clique em **Executar**.

Resultados

Um arquivo de implementação é criado no diretório `deployment` no qual o IBM Cognos Analytics foi instalado.

Copiando o Arquivo de Implementação para a Nova Versão:

Você deve copiar manualmente os arquivos de implementação a partir da instância na qual eles foram criados em sua nova instância.

Procedimento

Copie os arquivos de implementação que você criou a partir do diretório *old_version_install_location*`/deployment` para o diretório *new_version_install_location*`/deployment`.

Nota: O diretório `de implementação` é configurável no IBM Cognos Configuration. Por padrão, o local é *install_location*`/deployment`. Se você estiver usando um local diferente, assegure-se de copiar os arquivos de implementação para um diretório apropriado.

Incluindo Objetos de Configuração ao Importar um Arquivo de Implementação do Armazenamento de Conteúdo Inteiro:

Inclua objetos de configuração ao importar todo o armazenamento de conteúdo. Por exemplo, talvez você queira importar a configuração porque possui uma série de configurações avançadas para os serviços que deseja do ambiente de origem.

Por padrão, os objetos de configuração são excluídos ao importar todo o armazenamento de conteúdo, mesmo se estiverem incluídos na exportação. Esses objetos incluem dispatchers e pastas de configuração usados para agrupar dispatchers.

Procedimento

1. Em **IBM Cognos Administration**, na guia **Configuração**, clique em **Dispatchers e Serviços**.
2. Clique no dispatcher desejado.
3. Próximo ao **ContentManagerService**, clique no ícone configurar propriedades.
4. Clique na guia **Configurações**.
5. Na coluna **Valor**, clique em **Editar**.
6. Assinale a caixa de seleção **Substituir as configurações obtidas da entrada pai**.
7. Na coluna **Parâmetro**, digite o texto em maiúscula a seguir:
   `CM.DEPLOYMENTINCLUDECONFIGURATION`
8. Na coluna **Valor**, digite `verdadeiro`.
9. Clique em **OK** para finalizar.

Importando um Arquivo de Implementação:

Para importar entradas, cria-se uma especificação da implementação de importações.

Ao importar, selecione entradas que foram exportadas. É possível aceitar as opções padrão definidas durante a exportação ou alterá-las. É possível selecionar as opções que foram incluídas no arquivo de implementação durante a exportação.

Se você executar a implementação parcial do conteúdo do diretório e pastas públicas específicas, o assistente de importação mostrará se os pacotes e as pastas existem no ambiente de destino e a data e a hora da última modificação. Use esta informação para ajudá-lo a decidir como resolver conflitos. Ao implementar novamente, o assistente também mostrará se os pacotes e pastas estavam na implementação original.

Antes de Iniciar

Certifique-se de ter copiado o arquivo de implementação no diretório *install_location*`/deployment` para a nova versão do produto.

Procedimento

1. Para a sua nova versão do produto, no **IBM Cognos Administration**, na guia **Configuração**, clique em **Administração de Conteúdo**.
2. Na barra de ferramentas, clique no novo ícone de importação. 
3. Na caixa **Arquivo de Implementação**, selecione o arquivo de implementação que deseja importar e clique em **Avançar**.

4. Se o seu arquivo de implementação é do armazenamento de conteúdo inteiro, digite a senha inserida durante a exportação e clique em **OK**.
5. Digite o nome da importação e selecione a pasta na qual deseja salvá-la e, em seguida, clique em **Avançar**.
6. Selecione o conteúdo que deseja incluir na importação, selecione as opções e clique em **Avançar**.

   Dica: Clique no ícone de edição  junto ao pacote, se deseja alterar o local de destino para o conteúdo importado.
7. No painel **Especificar Opções Gerais**, selecione as opções desejadas e clique em **Avançar**.
8. Revise as informações de resumo e depois clique em **Avançar**.
9. Em **Ações**selecione **Salvar e Executar Uma Vez** e clique em **Concluir**.
10. No painel **Executar com Opções**, faça o seguinte:
    a. Selecione **Atualizar Todas as Especificações de Relatório para a Versão mais Recente** se desejar atualizar as especificações de relatório durante a importação. Também é possível executar esta tarefa depois de importar o conteúdo.
    b. Clique em **Executar**.

Usar o Lifecycle Manager para Comparar os Relatórios entre suas Versões do Produto

O Lifecycle Manager permite verificar seu conteúdo atualizado comparando os relatórios no seu antigo ambiente com os relatórios em sua nova versão do produto.

Para obter mais informações, consulte a documentação do IBM Cognos Lifecycle Manager.

Atualizar suas Especificações de Relatório:

As especificações de relatório foram alteradas de uma versão do IBM Cognos Analytics para outra. Você deve atualizar qualquer especificação de relatório criada nas versões anteriores do produto.

Se estiver atualizando a partir de um backup de seu armazenamento de conteúdo existente, você deve atualizar as especificações do relatório depois de ter iniciado os serviços.

Se você estiver movendo o conteúdo para uma nova versão usando os arquivos de implementação, será possível optar por atualizar as especificações de importação durante a importação.

Se você moveu o seu conteúdo usando o arquivo de implementação, você pode ter selecionado a opção para atualizar suas especificações de relatório. Se você atualizou as especificações de relatório durante a importação, não é necessário fazer isso novamente.

Antes de Iniciar

Importante: Não atualize suas especificações de relatório se tiver aplicativos Software Development Kit que criam, modificar ou salvam especificações de relatório. Primeiro você deve atualizar seus aplicativos Software Development Kit

para conformidade com o esquema de especificações de relatório do IBM Cognos. Do contrário, os aplicativos do Software Development Kit não poderão acessar as especificações de relatório atualizadas. Para obter informações sobre como fazer upgrade de especificações de relatório, consulte o *IBM Cognos Software Development Kit Developer Guide*.

Procedimento

1. Abra o **IBM Cognos Administration**.
2. Na guia **Configuração**, clique em **Administração de Conteúdo**.
3. Clique na seta no botão nova manutenção de conteúdo  na barra de ferramentas e, em seguida, clique em **Nova Atualização de Relatório**
4. Digite um nome para a tarefa de atualização e, se desejar, uma dica de tela e a descrição. Clique em **Avançar**.
5. Selecione os pacote e os locais para a especificação de relatório que deseja atualizar. Clique em **Avançar**.

   Se atualizar as especificações de relatório por pacote, todos os relatórios do armazenamento de conteúdo baseados no modelo desse pacote serão atualizados. Se atualizar as especificações de relatório por pasta, todos os relatórios da pasta serão atualizados.
6. Escolha uma das seguintes opções:
   - **Salvar e executar uma vez** abre a execução com a página de opções.
   - **Salvar e programar** abre a ferramenta de programação.
   - **Apenas salvar** permite salvar a atualização para que possa ser executada posteriormente.

Configurando o IIS e o Cognos Analytics ao fazer o upgrade da versão 11.0.3 para a 11.0.4 ou superior

11.0.4

Antes de Iniciar

Este tópico supõe que um ambiente da versão 11.0.3 está em funcionamento, que o IIS foi configurado e que a conexão única está em funcionamento.

Sobre Esta Tarefa

Neste tópico, são feitas as seguintes suposições:

- Nome do servidor IIS: **iis-host**
- Nº da porta do IIS: **80**
- Nome do diretório virtual do IIS: **ibmcognos**
- Nome do servidor Cognos Analytics: **ca-host**
- Nº da porta do Cognos Analytics: **9300**

Procedimento

1. Faça backup do armazenamento de conteúdo da versão 11.0.3.
2. Instale a versão 11.0.4 sobre a instalação da versão 11.0.3. Conforme necessário, faça isso nas máquinas da camada de Dados, da camada do Aplicativo e da camada de Gateway.
3. Antes de iniciar os serviços do Cognos Analytics, faça as mudanças a seguir no ambiente.

a. Remova essa entrada do arquivo *install_location*\wlp\usr\servers\cognosserver\server.xml (na camada de Dados e do Aplicativo): <jndiEntry jndiName="glass/sso/login" value="/ibmcognos/cgi-bin/cognosisapi.dll"/>

b. Examine o default.htm e o index.html na pasta *gateway_install_location*/webcontent. Certifique-se de que essa linha <meta http-equiv="refresh" content="0; URL=bi/"> inclua a barra (/) no atributo URL=bi/.

c. Ative o Cognos Configuration na camada de Gateway. Modifique **Ambiente** > **Configurações de Gateway** > **URIs do Despachante para o gateway** para que use o seguinte formato: http://<apptier_host>:<apptier_port>/bi/v1/disp

d. Ative o Cognos Configuration nas camadas de Dados e do Aplicativo. Altere **Ambiente** > **Configurações de gateway** aplicáveis.

- **URI do gateway**: http(s)://iis-host:80/ibmcognos/bi/v1/disp

  Esta é a URL para o conteúdo desconectado, como links em PDFs, Excel e relatórios ativos. Ela também é usada em links enviados por e-mail.

- **URIs do dispatcher para o gateway**: http(s)://ca-host:9300/bi/v1/disp

  Esta é a lista de URIs com os quais o código ISAPI do Cognos se conecta ao encaminhar solicitações. Várias entradas são usadas para failover. Inclua todos os servidores de aplicativos do Cognos Analytics relevantes.

- **URI do dispatcher para aplicativos externos**: http(s)://ca-host:9300/bi/v1/disp

  Aplicativos externos, como o Framework Manager, se conectam nessa URL para executar operações de SDK.

e. Siga os procedimentos em "Configurando o IIS no Cognos Analytics 11.0.3" na página 121 para reconfigurar o IIS.

4. Inicie os serviços nesta ordem: 1) camada de Dados, 2) camada do Aplicativo, 3) camada de Gateway e IIS.

Capítulo 4. Instalar e configurar os componentes do servidor

É possível instalar todos os componentes do IBM Cognos Analytics em um computador, em diversos servidores para uma instalação distribuída ou é possível expandir uma instalação existente de computador único para melhorar o desempenho.

As opções a seguir ficam disponíveis ao instalar o IBM Cognos Analytics a partir do assistente de instalação.

- Use a opção **Instalação fácil** para ajudar no funcionando do IBM Cognos Analytics sem demora, sem qualquer configuração adicional e sem a necessidade de instalar qualquer software de suporte.

  Importante: A **Instalação fácil** está disponível somente para S.O. Windows. Se você estiver fazendo upgrade de uma **Instalação fácil** (ou seja, instalação sobre uma instalação existente), primeiro encerre todos os serviços manualmente, incluindo os serviços Informix e ApacheDS.

  Com essa opção de instalação, tenha tudo a seguir com a configuração toda pronta:

  – Uma versão completa do software IBM Cognos Analytics com todos os novos recursos.
  – Informix 12.10 instalado e configurado para o uso como banco de dados de armazenamento de conteúdo.
  – Apache Directory Server para criar e gerenciar usuários.
- Use a opção **Customizar** para obter flexibilidade total ao selecionar os componentes do IBM Cognos Analytics que deseja instalar. Talvez você deseje customizar ou integrar o IBM Cognos Analytics com o software de terceiros? Essa é a opção que você poderia selecionar.

Caso pretenda instalar dois ou mais componentes no mesmo computador, instale-os no mesmo local de instalação para evitar conflitos entre portas e outras configurações padrão.

Ao executar uma instalação customizada, os componentes do servidor são coletados nas seguintes camadas:

- Repositório de conteúdo (Content Manager)
- Serviços do aplicativo
- Camada opcional do gateway

É possível instalar cada componente em um computador separado ou no mesmo computador. Instale o gateway em um computador que também esteja executando um servidor web.

Parando a Sequência de Serviços

Se for necessário interromper os serviços em um ambiente distribuído, a sequência será importante. Pare o serviço do IBM Cognos para os Componentes da Camada de Aplicativos, seguido pelo Content Manager em espera, e depois ative o Content Manager.

É importante também interromper os seguintes:

- Aplicativos que estão relacionados ao serviço IBM Cognos, como Framework Manager, Cognos Transformer ou IBM Cognos Administration.
- Quaisquer aplicativos do Kit de Desenvolvimento de Software que estejam em execução.

Atualizando a Instalação

Se você estiver atualizando de uma liberação anterior dos produtos IBM Cognos, consulte Capítulo 3, "Upgrade do IBM Cognos Analytics", na página 37.

Se estiver fazendo upgrade a partir de uma versão anterior do IBM Cognos Analytics, todos os componentes distribuídos devem ter a mesma versão do IBM Cognos Analytics. Se você instalar o IBM Cognos Analytics em hosts adicionais ou alternativos, deverá atualizar as propriedades específicas do local no IBM Cognos Configuration.

Instalações de 64 Bits

O gateway do IBM Cognos Analytics fornece bibliotecas de 32 bits, independentemente de a instalação ser feita em um servidor de 64 bits ou de 32 bits. Em alguns servidores Web, como o Apache Web server, não é possível carregar uma biblioteca compilada de 32 bits em um servidor compilado de 64 bits. Nessa situação, instale a versão de 32 bits do gateway do IBM Cognos em um servidor da Web de 32 bits.

O componente do servidor de relatório, incluído com os Componentes da Camada de Aplicativos, é fornecido nas versões de 32 bits e de 64 bits. A seleção da versão usada é feita com o IBM Cognos Configuration após a instalação. Por padrão, o componente do servidor de relatório está configurado para usar o modo de 32 bits, mesmo em um computador de 64 bits. O modo de 32 bits permite executar todos os relatórios, enquanto o modo de 64 bits permite executar apenas os relatórios criados para o modo de consulta dinâmica.

Se estiver fazendo o upgrade do IBM Cognos Analytics em um ambiente que inclui versões anteriores de outros produtos do IBM Cognos Analytics, como o IBM Cognos Business Intelligence Controller Versão 8.x, o IBM Cognos Analytics Planning Versão 8.x ou o IBM Cognos Business Intelligence Analysis *for Microsoft Excel* Versão 8.x, instale a nova versão do IBM Cognos Analytics em um local separado do outro produto do IBM Cognos Analytics e configure a nova versão do IBM Cognos Analytics para que opere independentemente desse produto. Depois de fazer o upgrade do outro produto para uma versão compatível com o IBM Cognos Analytics, é possível configurar os dois produtos para que operem juntos.

Instalações do Windows

Para instalações do sistema operacional Microsoft Windows, certifique-se de ter os privilégios de administrador para o computador Windows no qual está instalando. Certifique-se também de que o computador possua variável de sistema TEMP que aponte para o diretório onde se deseja armazenar os arquivos temporários. Durante a instalação, os arquivos do disco são copiados temporariamente para esse diretório.

Instalações do UNIX

Para instalações do sistema operacional UNIX, é possível instalar componentes de servidor usando uma interface gráfica com o usuário ou executando uma

instalação silenciosa. Para executar a instalação no modo gráfico, o console conectado ao seu computador UNIX deverá suportar uma interface gráfica de usuário baseada em Java.

Além disso, o IBM Cognos Analytics usa 755 permissões. Isto afeta somente os diretórios de instalação. Não afeta as permissões de arquivo nos diretórios.

Requisitos da Impressora

Para garantir que os relatórios sejam impressos corretamente no Windows, o Adobe Reader requer que você configure pelo menos uma impressora no sistema operacional no qual os Componentes da Camada de Aplicativos estão instalados. Todos os relatórios, independente do formato de impressão escolhido, são enviados como arquivos PDF temporários para o Adobe Reader para impressão.

Desinstalação

Para obter instruções de desinstalação, consulte Capítulo 12, “Desinstalando o IBM Cognos Analytics”, na página 299.

Sequência de Instalação para os Componentes do Servidor

Em uma instalação distribuída, a sequência na qual os componentes são configurados é importante. Configure inicie os serviços em pelo menos um local em que o Content Manager foi instalado antes de configurar outros componentes do servidor.

Você deve configurar o componente de gateway por último para que as chaves criptográficas sejam compartilhadas e a comunicação segura possa ocorrer entre os três componentes. O servidor especificado para a propriedade URI do dispatcher externo no computador de gateway deve ser o último componente do servidor a iniciar.

O diagrama a seguir mostra a sequência do processo de instalação para componentes distribuídos. Após planejar e preparar o ambiente, instale e configure os componentes do Content Manager, em seguida o Application Tier Components e só então os gateways. Depois de instalar os componentes do servidor, instale e configure o Framework Manager.

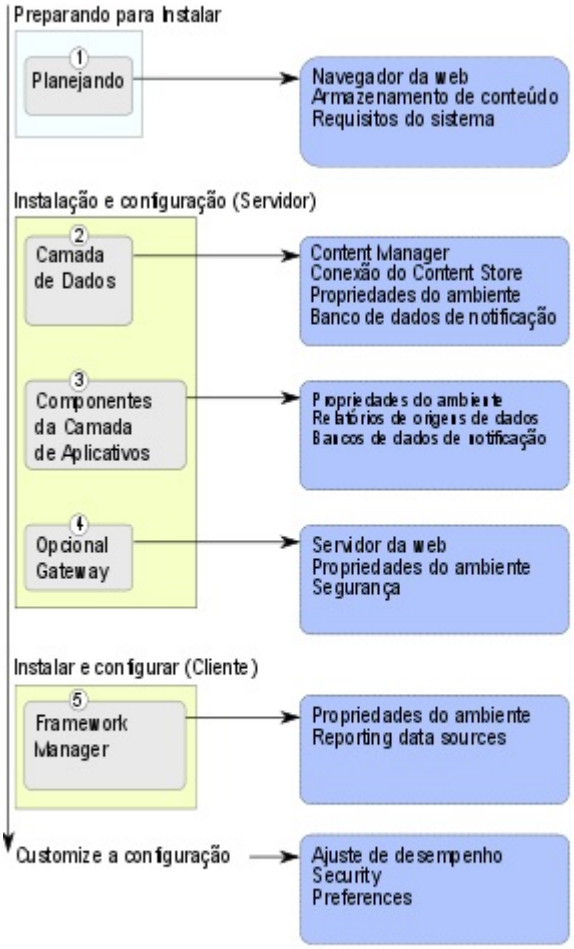


Figura 7. Fluxo de Trabalho do Processo de Instalação Distribuída

Recomendação - instale e configure a instalação básica para instalações distribuídas

Ao fazer uma instalação distribuída, existem várias opções diferentes de instalação e configuração que podem ser usadas para customizar o IBM Cognos Analytics para que ele se adeque à infraestrutura corporativa.

Faça primeiro uma instalação básica, que envolva a instalação de uma ou mais instâncias de cada um dos componentes do servidor necessários: camada de dados (Content Manager), Componentes da camada de aplicativos e camada de gateway. Execute apenas as tarefas de configuração requeridas, como configurar componentes distribuídos para que se comuniquem uns com os outros, para colocar o ambiente distribuído em operação antes de personalizar as configurações.

Mais tarde, é possível adicionar componentes opcionais e personalizar as configurações para que melhor se adaptem às necessidades de inteligência do negócio.

A sequência na qual os computadores são configurados é importante. É preciso configurar e, em seguida, iniciar os serviços em pelo menos um computador onde o Content Manager foi instalado antes de configurar outros componentes de servidor ou o Framework Manager. Para obter mais informações, consulte "Sequência de Instalação para os Componentes do Servidor" na página 57.

A maneira mais simples e rápida de fazer com que o IBM Cognos Analytics seja executado no ambiente é garantindo que uma instalação básica funcione no ambiente.

Modos de instalação

Para uma instalação completa, instale os componentes no servidor e, em seguida, configure-os para trabalharem no ambiente.

Modo Interativo

Normalmente, você executa os programas de instalação e configuração do IBM Cognos no modo interativo. Isso significa que o assistente de instalação solicita que você forneça informações e a ferramenta de configuração permite que mude as configurações padrão. O assistente de instalação é `ca_srv_<platform>_<build>.exe` (Windows) ou `ca_srv_<platform>_<build>.bin` (UNIX, Linux).

Modo Silencioso

É possível automatizar a instalação de componentes utilizando arquivos de resposta e executando o programa de instalação no modo silencioso.

É possível automatizar a configuração de componentes com a exportação das configurações de um computador para outro, desde que os componentes instalados sejam os mesmos. Execute o IBM Cognos Configuration no modo interativo pela primeira vez.

A outra opção é editar o arquivo cogstartup.xml, usando as configurações que se aplicam ao ambiente e, em seguida, executar a ferramenta de configuração no modo silencioso.

Modo interativo nos sistemas UNIX

A menos que pretenda concluir uma instalação no modo silencioso, instale a partir de uma estação de trabalho com sistema X Window, um terminal X, ou um PC ou outro sistema com um software de servidor X instalado.

Para executar a instalação no modo interativo, o console anexado ao computador deve suportar interfaces gráficas de usuário baseadas em Java.

Instalando Componentes do Servidor nos Sistemas Operacionais UNIX ou Linux

Use o assistente de instalação para selecionar os componentes do servidor que deseja instalar e o local em seu computador onde deseja instalá-los.

Antes de Iniciar

Acesse IBM Software Product Compatibility Reports (www.ibm.com/support/docview.wss?uid=swg27047186) para verificar se as correções necessárias estão instaladas em seu computador.

Procedimento

1. Configure a variável de ambiente JAVA_HOME para apontar o local de instalação de seu Java Runtime Environment (JRE), como */directory*/java/*java_version*/jre.

   O IBM Cognos Analytics requer uma JVM, como a fornecida pela IBM, para execução no sistema operacional Linux.
2. No HP-UX, configure a variável de ambiente _M_ARENA_OPTS como a seguir: _M_ARENA_OPTS 1:4.

   Isto aumenta a distribuição de memória no HP-UX para que se encaixe melhor em outras plataformas UNIX.
3. Acesse o local em que os arquivos de instalação foram transferidos por download e extraídos.

   Dica: Use novas versões de software de compactação arquivo para extrair os arquivos. Versões mais antigas desse software não podem extrair os arquivos.
4. Para iniciar o assistente de instalação, acesse o diretório do sistema operacional e digite o seguinte comando:

   ./ca_srv_<*platform*>_<*build*>.bin

   Em que <*build*> é o número da construção e <*platform*> é win (Windows), i386 (Linux i386), ppcle (Linux pl E), ppc (Linux Power PC), s390x (Linux z), sol (Solaris), aix (AIX) e zos (z/OS).

   Dica: Ao usar o comando ./ca_srv_<*platform*>_<*build*>.bin com XWindows, os caracteres japoneses nas mensagens e nos arquivos de log podem ser corrompidos. Ao instalar em japonês no UNIX ou Linux, primeiro configure as variáveis de ambiente LANG=C e LC_ALL=C (em que C é o código de idioma, por exemplo, ja_JP.PCK no Solaris) e inicie o assistente de instalação.

   Se não estiver usando o XWindows, execute uma instalação não assistida. Para obter mais informações, consulte Capítulo 11, “Instalação, desinstalação e configuração não assistidas”, na página 291.
5. Siga as instruções do assistente de instalação e copie os arquivos para seu computador.

   Instale em um diretório que contenha somente caracteres ASCII no nome do caminho. Alguns servidores da web UNIX e Linux não suportam caracteres não ASCII em nomes de diretório.

   Dica: As amostras não estão disponíveis com o kit de instalação do Cognos Analytics AIX, versão 11.0.7 e mais recente. Para obter mais informações, consulte este artigo.
6. Na página **Concluir** do assistente de instalação, é possível clicar em **Visualizar** para acessar os arquivos de log. Não configure o IBM Cognos Analytics imediatamente, porque é necessário executar outras tarefas primeiro, para garantir que o ambiente esteja adequadamente configurado.
7. Anexe o diretório *install_location*/bin na variável de ambiente do caminho de biblioteca apropriado.
   - Para Solaris e Linux, LD_LIBRARY_PATH

- Para AIX, LIBPATH
- Para HP-UX, SHLIB_PATH

O que Fazer Depois

É possível configurar o IBM Cognos Analytics usando o IBM Cognos Configuration. Digite `cogconfig.sh` no diretório *`install_location`*`/bin` para iniciar o Cognos Configuration.

Instalando Componentes do Servidor em Sistemas Operacionais Windows

Use o assistente de instalação para selecionar os componentes do servidor que deseja instalar e o local em seu computador onde deseja instalá-los.

Para computadores Windows, o local de instalação padrão usa o diretório **Arquivos de programa**. Se você instalar nesse local, assegure-se de executar o IBM Cognos Configuration como um administrador. Como alternativa, é possível instalar o produto em um diretório fora de **Arquivos de Programa**, como `C:\IBM\cognos\analytics`.

A instalação requer, no mínimo, 5 GB no diretório temporário. O diretório temporário é configurado com a variável de ambiente TMP.

Procedimento

1. Acesse o local em que os arquivos de instalação foram transferidos por download e extraídos e dê um clique duplo em `ca_srv_<platform>_<build>.exe`.

   Dica: Use novas versões de software de compactação arquivo para extrair os arquivos. Versões mais antigas desse software não podem extrair os arquivos.
2. Selecione o idioma para utilizar na instalação.

   Essa seleção determina o idioma da interface com o usuário. Todos os idiomas suportados são instalados. É possível alterar a interface com o usuário para qualquer um dos idiomas instalados depois de concluída a instalação.
3. Siga as instruções do assistente de instalação e copie os arquivos para seu computador.

   É possível usar uma das opções de instalação a seguir:

   - Use a opção **Instalação fácil** para instalar componentes em um único computador, instalar uma instância do banco de dados Informix para o armazenamento de conteúdo e configurar o sistema.

     Importante: Se você estiver fazendo upgrade (ou seja, instalando sobre uma instalação existente) com uma **Instalação fácil**, primeiramente encerre de modo manual todos os serviços, incluindo os serviços do Informix e do ApacheDS.
   - Use a opção **Customizado** para um dos componentes de instalação installationto distribuídos em múltiplos servidores.

   Instale os componentes do IBM Cognos Analytics em um diretório que contém apenas caracteres ASCII no nome do caminho. Alguns servidores da Web para Windows não suportam caracteres não ASCII em nomes de diretórios.
4. Se esta for a primeira instalação, selecione a opção **Primeira instalação**. Para expandir a capacidade de uma instalação em execução, selecione a opção

Conectar e instalar. Você será solicitado a fornecer os componentes a serem instalados e a URL e as credenciais para o sistema em execução. O namespace e as credenciais devem ser as de um administrador do sistema.

- É possível localizar o valor da URL para a instalação em execução no IBM Cognos Configuration, na categoria **Ambiente** > **Configurações do dispatcher**. O valor da URL necessária é o **URI do dispatcher externo**.
- É possível localizar o namespace para a instalação em execução no IBM Cognos Configuration, na categoria **Segurança** > **Autenticação**.

Instalando e configurando o Content Manager para o repositório de conteúdo

É possível instalar mais de um Content Manager para garantir o failover e é possível instalar o Content Manager em uma localização separada de outros componentes para melhorar o desempenho.

Os computadores com o Content Manager devem conhecer o local do armazenamento de conteúdo, o local de outros componentes do Content Manager e o banco de dados usado para notificação.

Em uma instalação distribuída, pelo menos um dos computadores nos quais você instalou o Content Manager deverá estar configurado, em execução e acessível antes de você configurar outros componentes em seu ambiente do IBM Cognos. Isso garante que o serviço da autoridade de certificação, que está instalado com o Content Manager, está disponível para emitir certificados a outros computadores.

Sua instalação pode incluir mais de um Content Manager, cada um em um computador diferente. Um computador com Content Manager fica ativo e um ou mais computadores com Content Manager ficam em espera.

Permissões

É possível instalar utilizando autoridade raiz ou não raiz.

Além disso, o IBM Cognos Analytics respeita a máscara de criação de modo de arquivo (umask) da conta que executa o programa de instalação. Isto afeta somente os diretórios de instalação. Não afeta as permissões de arquivo nos diretórios. Entretanto, os arquivos gerados pelo tempo de execução, tais como logs, respeitam a máscara. Recomenda-se o umask 022 no diretório de instalação.

Regras para Configuração

Em uma instalação onde exista mais de um componente do Content Manager, ou onde o Content Manager esteja localizado separadamente, pelo menos um dos Content Manager deve estar configurado, em execução e acessível antes de configurar outros componentes do ambiente. Isso garante que o serviço de autoridade de certificação, que está instalado com o Content Manager, fique disponível para emitir certificados para outros computadores IBM Cognos.

Para obter informações sobre a sequência do processo de instalação para componentes distribuídos, consulte “Sequência de Instalação para os Componentes do Servidor” na página 57.

Regras para Content Manager Ativo

Se estiver instalando diversos componentes do Content Manager, o primeiro computador com o Content Manager que iniciar torna-se, por padrão, o Content Manager ativo. É possível designar outro computador com Content Manager como ativo padrão usando IBM Cognos Administration.

Os computadores com Content Manager que ficam em espera servem para proteção de failover. Se o computador com Content Manager ativo não estiver disponível devido a uma falha de software ou hardware, um computador com Content Manager em espera é ativado e as solicitações são direcionadas a ele.

Se o Content Manager ativo falhar, os dados de sessão que não foram salvos serão perdidos. Se outro Content Manager for ativado, os usuários poderão ser alertados para efetuar o logon.

Para obter informações sobre a ativação do serviço do Content Manager, consulte o *Guia de administração e segurança*. Para obter informações sobre os componentes ativos e em espera do Content Manager, consulte "Componentes ativo e em espera do Content Manager".

Em instalações com vários Content Managers, configure o IBM Cognos Analytics para usar gateways compilados, em vez do gateway CGI padrão. Por exemplo, use o Módulo Apache para Servidor Apache ou para IBM HTTP Server ou use ISAPI para IIS. Do contrário, o desempenho pode ser afetado depois do failover.

Atualizando

Se estiver fazendo o upgrade a partir do ReportNet ou de uma versão anterior do IBM Cognos Business Intelligence, será possível usar os dados de configuração existentes. No entanto, alguns recursos no IBM Cognos Analytics são novos e podem exigir configuração.

PowerCubes

Se você pretende instalar o IBM Cognos Transformer e estiver usando PowerCubes protegidos contra um namespace IBM Cognos Series 7, será necessário instalar o Content Manager em um computador que suporte o IBM Cognos Series 7.

Componentes ativo e em espera do Content Manager

É possível instalar qualquer número de Content Managers, embora apenas um fique ativo num dado momento. As outras instalações agem como uma reserva do Content Manager.

Os componentes do Content Manager em espera são para proteção de failover. Se o Content Manager ativo não estiver disponível devido a uma falha de software ou hardware, um Content Manager em espera é ativado e as solicitações são direcionadas a ele.

Se o Content Manager ativo falhar, os dados de sessão que não foram salvos serão perdidos. Se outro Content Manager for ativado, os usuários poderão ser alertados para efetuar o logon.

Por padrão, o primeiro Content Manager instalado com o IBM Cognos Analytics é o ativo. Um administrador do servidor IBM Cognos Analytics pode alterar o

Content Manager padrão e o Content Manager ativo a qualquer momento. Quando o IBM Cognos Analytics é iniciado, o Content Manager padrão bloqueia o armazenamento de conteúdo, impedindo que ele seja acessado por todas as outras instalações do Content Manager. Essas outras instalações do Content Manager entram em espera.

Esse mecanismo de failover funciona porque os dispatchers e o Content Manager comunicam-se rotineiramente um com o outro. Se um dispatcher não pode mais alcançar o Content Manager, o dispatcher sinaliza um Content Manager em espera, que se torna o Content Manager ativo. As outras instalações do Content Manager permanecem em espera para continuar o suporte de failover. Os Content Managers em espera recuperam as configurações criptográficas, como a chave simétrica comum (utilizada para criptografar e descriptografar dados) do Content Manager ativo.

Se estiver instalando diversos Content Managers, **deve-se** assegurar que os relógios do sistema nos computadores do Content Manager estejam sincronizados para o failover bem-sucedido entre os Content Managers.

Instalando o Content Manager nos Sistemas Operacionais UNIX ou Linux

Use o seguinte procedimento para instalar o Content Manager em um sistema operacional UNIX ou Linux.

Antes de Iniciar

Acesse IBM Software Product Compatibility Reports (www.ibm.com/support/docview.wss?uid=swg27047186) para verificar se as correções necessárias estão instaladas em seu computador.

Procedimento

1. Configure a variável de ambiente JAVA_HOME para apontar o local de instalação de seu Java Runtime Environment (JRE), como `/directory/java/java_version/jre`.

   O IBM Cognos Analytics requer uma JVM, como a fornecida pela IBM, para execução no sistema operacional Linux.
2. Acesse o local em que os arquivos de instalação foram transferidos por download e extraídos.

   Dica: Use novas versões de software de compactação arquivo para extrair os arquivos. Versões mais antigas desse software não podem extrair os arquivos.
3. Para iniciar o assistente de instalação, acesse o diretório do sistema operacional e digite `./ca_srv_<platform>_<build>.bin`

   Dica: Ao usar o comando `ca_srv_<platform>_<build>.bin` com o XWindows, os caracteres japoneses em mensagens e arquivos de log podem ficar corrompidos. Ao instalar em japonês no UNIX ou Linux, primeiro configure as variáveis de ambiente LANG=C e LC_ALL=C (em que C é o código de idioma, por exemplo, ja_JP.PCK no Solaris) e inicie o assistente de instalação.

   Se não estiver usando o XWindows, execute uma instalação não assistida. Para obter mais informações, consulte Capítulo 11, “Instalação, desinstalação e configuração não assistidas”, na página 291.
4. Siga as instruções no assistente de instalação para copiar os arquivos para seu computador e implementar uma configuração básica.

- Ao selecionar o diretório, considere o seguinte:

  Instale o Content Manager em um diretório que contenha apenas caracteres ASCII no nome do caminho. Alguns servidores da Web UNIX e Linux não suportam caracteres não ASCII em nomes de diretório.

  Se você estiver instalando o IBM Cognos Analytics em um computador que possua uma versão anterior do IBM Cognos Analytics e desejar manter a versão anterior, a nova versão deverá ser instalada em um diretório diferente.
- Ao selecionar os componentes, desmarque todos os componentes, exceto para **Repositório de conteúdo**.

5. Clique em **Concluir**.
6. Anexe o diretório *install_location*/bin na variável de ambiente do caminho de biblioteca apropriado.
   - Para Solaris e Linux, LD_LIBRARY_PATH
   - Para AIX, LIBPATH
   - Para HP-UX, SHLIB_PATH

O que Fazer Depois

Não configure o IBM Cognos Analytics imediatamente, porque é necessário executar outras tarefas primeiro, para garantir que o ambiente esteja adequadamente configurado.

Posteriormente, é possível configurar o IBM Cognos Analytics usando o IBM Cognos Configuration digitando cogconfig.sh no diretório *install_location*/bin.

Instalando o Content Manager nos Sistemas Operacionais Windows

Use o seguinte procedimento para instalar o Content Manager em um sistema operacional Microsoft Windows.

Para computadores Windows, o local de instalação padrão usa o diretório **Arquivos de programa**. Se você instalar nesse local, assegure-se de executar o IBM Cognos Configuration como um administrador. Como alternativa, é possível instalar o produto em um diretório fora de **Arquivos de Programa**, como C:\IBM\cognos\analytics.

A instalação requer, no mínimo, 5 GB no diretório temporário. O diretório temporário é configurado com a variável de ambiente TMP.

Antes de Iniciar

Acesse IBM Software Product Compatibility Reports (www.ibm.com/support/docview.wss?uid=swg27047186) para verificar se as correções necessárias estão instaladas em seu computador.

Procedimento

1. Acesse o local em que os arquivos de instalação foram transferidos por download e extraídos e dê um clique duplo em ca_srv_<platform>_<build>.exe.

   Dica: Use novas versões de software de compactação arquivo para extrair os arquivos. Versões mais antigas desse software não podem extrair os arquivos.
2. Selecione o idioma para utilizar na instalação.

Essa seleção determina o idioma da interface com o usuário. Todos os idiomas suportados são instalados. É possível alterar a interface com o usuário para qualquer um dos idiomas instalados depois de concluída a instalação.

3. Selecione a opção de instalação **Customizada** e siga as instruções do assistente de instalação para copiar os arquivos para seu computador.
   - Ao selecionar o diretório, considere o seguinte:

     Instale o Content Manager em um diretório que contenha apenas caracteres ASCII no nome do caminho. Alguns servidores da Web do sistema operacional Microsoft Windows não suportam caracteres não ASCII em nomes de diretórios.

     Se estiver instalando o IBM Cognos Analytics em um computador que tem uma versão anterior do IBM Cognos Analytics e desejar manter a versão anterior, instale o IBM Cognos Analytics em um diretório diferente.
   - Ao selecionar os componentes, desmarque todos os componentes, exceto **Repositório de conteúdo** na opção de instalação **Customizada**.
4. Clique em **Concluir**.

O que Fazer Depois

Se você iniciar o IBM Cognos Configuration a partir do assistente de instalação, certifique-se de seguir as tarefas adicionais nessa seção para assegurar que o seu ambiente esteja apropriadamente configurado antes de iniciar os serviços.

É possível iniciar o IBM Cognos Configuration usando o atalho **IBM Cognos Configuration** do menu **Iniciar**.

Configure a conectividade do banco de dados para o banco de dados de armazenamento de conteúdo.

Pode ser necessário instalar o software do cliente de banco de dados, ou os drivers do Java Database Connectivity (JDBC), ou ambos, em cada computador em que o Content Manager está instalado. Fazer isso permite que o Content Manager acesse o banco de dados de armazenamento de conteúdo.

Configure a conectividade do banco de dados para um armazenamento de conteúdo do Microsoft SQL Server 11.0.5

O driver JDBC da Microsoft substitui o driver JSQLConnect para o SQL Server. Da versão 11.0.5 em diante, deve-se fazer o download, na Microsoft, e colocar o novo driver tipo 4 na pasta *install_location*/drivers.

O arquivo JAR do driver sqljdbc42.jar é o arquivo que é necessário para suportar a versão Java que é fornecida com o IBM Cognos Analytics.

Importante: Para conexão única (SSO) e autenticação do Windows, é necessário colocar o sqljdbc_auth.dll no diretório bin64. A autenticação do Windows é uma configuração de conexão única. A seleção no Configuration Manager para o Content Manager é denominada **Banco de dados Microsoft SQL Server (Autenticação do Windows)**.

Configure a conectividade do banco de dados para um armazenamento de conteúdo do IBM Db2

Este procedimento descreve como configurar a conectividade do banco de dados para um armazenamento de conteúdo do Db2. Você deve executar este procedimento em cada computador em que instalar Content Manager.

Deve-se usar um driver Java Database Connectivity (JDBC) tipo 4 para conectar-se ao seu armazenamento de conteúdo.

O driver tipo 4 é considerado um produto independente. Ele não requer que o cliente do Db2 seja instalado.

Procedimento

Copie os arquivos a seguir do diretório *DB2_installation*\sqllib\java para o diretório *install_location*\drivers:

- O arquivo do driver universal, db2jcc4.jar
- O arquivo de licença:

  Para o Db2 em sistemas operacionais Linux, UNIX ou Windows, use db2jcc_license_cu.jar.

  Para o Db2 on z/OS, use db2jcc_license_cisuz.jar.

  Se você estiver conectando-se ao Db2 on z/OS, use a versão do driver do fix pack 5 da versão 9.1 ou do fix pack 2 da versão 9.5 no Linux, UNIX ou Windows.

  Dica: Para verificar a versão do driver, execute o seguinte comando:

  ```
  java -cp path\db2jcc4.jar com.ibm.db2.jcc.DB2Jcc -version
  ```

Gerando um arquivo de script para criar um banco de dados para um armazenamento de conteúdo do IBM Db2:

É possível gerar um arquivo de script para criar automaticamente o armazenamento de conteúdo no Db2 em todas as plataformas. O arquivo de script é um arquivo DDL.

Procedimento

1. Inicie o **IBM Cognos Configuration**.
2. Na janela **Explorer**, em **Acesso a Dados** > **Content Manager**, clique em **Content Store**.

   A configuração padrão é para um banco de dados do Db2. Certifique-se de que o **Tipo** seja **Banco de Dados DB2**.
3. No campo **Servidor de banco de dados e número de porta**, insira o nome de seu computador e o número da porta na qual o Db2 está em execução. Por exemplo, localhost:50000. Em que 50000 é o número da porta padrão que é usada pelo Db2. Se você estiver usando um número de porta diferente, certifique-se de usar tal valor.
4. Clique no campo **Valor** próximo à propriedade **Senha e ID de Usuário** e, em seguida, clique no ícone de edição. Digite os valores apropriados e clique em **OK**.
5. Na janela **Propriedades**, para a propriedade **Nome do Banco de Dados**, digite o nome para o banco de dados de armazenamento de conteúdo.

Importante: Não use um nome com mais de oito caracteres e use apenas letras, números, sublinhados e hifens no nome.

6. Clique com o botão direito do mouse em **Content Store**, e clique em **Gerar DDL**.
7. Clique em **Detalhes** para registrar o local do arquivo DDL gerado.

   O arquivo DDL denominado `createDB.sql` é criado. O script é criado no diretório *install_location*`\configuration\schemas\content\db2`.

O que Fazer Depois

Use este script para criar um banco de dados no Db2. Para obter mais informações sobre o uso de um arquivo DDL, consulte sua documentação do Db2.

Se você usa a interface da linha de comandos do Db2, é possível executar o script inserindo o comando a seguir:

```
db2 -tvf createDB.sql
```

Criando espaços de tabela para um armazenamento de conteúdo no IBM Db2 for z/OS:

Um administrador de banco de dados deve executar scripts para criar um conjunto de espaços de tabelas necessário para o banco de dados de armazenamento de conteúdo. Modifique os scripts para substituir os parâmetros do marcador pelos apropriados para o seu ambiente.

Por padrão, o armazenamento de conteúdo é usado para notificações, tarefas manuais e anotações. É possível criar bancos de dados separados para cada um deles.

Sobre Esta Tarefa

Certifique-se de que você usa as convenções de nomenclatura para o Db2 on z/OS. Por exemplo, todos os nomes de parâmetros devem começar com uma letra e o comprimento não pode exceder oito caracteres. Há duas exceções para o limite de comprimento de caracteres:

- CMSCRIPT_CS_ID não possui mais de 2 caracteres.
- CMSCRIPT_TABLESPACE não possui mais de 6 caracteres.

O motivo para a exceção é que quando dois parâmetros são concatenados, o comprimento do caractere não pode ter mais de 8 caracteres.

Para obter mais informações, consulte o IBM Db2 for z/OS Knowledge Center (http://www.ibm.com/support/knowledgecenter/SSEPEK/db2z_prodhome.html).

Procedimento

1. Conecte-se ao banco de dados como um usuário que possui privilégios para criar e eliminar espaços de tabelas para permitir a execução de instruções SQL.
2. Vá até o diretório que contém os scripts:

   install_location`/configuration/schemas/content/db2zOS`
3. Faça uma cópia de backup do arquivo de script `tablespace_db2zOS.sql` e salve o arquivo em outro local.
4. Abra o arquivo de script `tablespace_db2zOS.sql` original.
   a. Inclua uma instrução de conexão no início do script.

Por exemplo,

```
connect to databasename;
```

b. Use a tabela a seguir para ajudá-lo a substituir os parâmetros genéricos pelos parâmetros apropriados para seu ambiente.

Nem todos os parâmetros listados estão no script, mas alguns podem ser incluídos no futuro.

Tabela 9. Nomes de Parâmetro e Descrição para o Script de Espaço de Tabela de Armazenamento de Conteúdo

Nome do parâmetro	Descrição
CMSCRIPT_STOGROUP	Especifica o nome do grupo de armazenamento.
CMSCRIPT_DATABASE	Especifica o nome do armazenamento de conteúdo Sybase.
CMSCRIPT_CS_ID	Especifica a identificação do subsistema para o banco de dados de armazenamento de conteúdo. O ID não deve ser mais longo que 2 caracteres.
CMSCRIPT_TABLESPACE	Especifica o nome do espaço de tabela que contém todas as tabelas base no armazenamento de conteúdo. Tabelas auxiliares não são incluídas. O nome não deve ser mais longo que 6 caracteres.
CMSCRIPT_LARGE_BP	Especifica o nome do pool de buffer grande alocado especialmente para objetos grandes. Esse buffer pool é aquele com 32 KB que foi criado quando o administrador do banco de dados criou o banco de dados de armazenamento de conteúdo no sistema z/OS.
CMSCRIPT_REGULAR_BP	Especifica o nome do pool de buffer de tamanho normal alocado especialmente para objetos grandes e de tamanho normal. Esse buffer pool é aquele com 16 KB que foi criado quando o administrador do banco de dados criou o banco de dados de armazenamento de conteúdo no sistema z/OS.
CMSCRIPT_USERNAME	Especifica a conta de usuário que acessa o banco de dados do armazenamento de conteúdo.

5. Salve e execute o script.

Por exemplo, se você configurar o arquivo `clp.properties` e seu alias do Db2 em seu perfil ou no arquivo de script `tcshrc`, digite o comando a seguir para executar o script:

```
db2 -tvf tablespace_db2zOS.sql
```

6. Conceda os direitos do usuário do IBM Cognos para os espaços de tabela que foram criados quando você executou o script de arquivo `tablespace_db2zOS.sql`:
   a. Faça uma cópia do arquivo de script `rightsGrant_db2zOS.sql` e armazene-a em outro local.
   b. Na ferramenta de acesso remoto, abra o arquivo de script `rightsGrant_db2zOS.sql` original e substitua os parâmetros de marcador com valores que são apropriados para o seu ambiente.

      Certifique-se de usar os mesmos valores usados quando você alocou recursos para os buffer pools e para a conta do usuário.
   c. Inclua uma instrução de conexão no início do script.

      Por exemplo,

      ```
      connect to databasename user username using password;
      ```
   d. Salve e, em seguida, execute o script.

      Por exemplo,

      ```
      db2 -tvf rightsGrant_db2zOS.sql
      ```
7. Para criar os espaços de tabela de notificação, acesse o diretório *install_location*/configuration/schemas/delivery/zosdb2.
   a. Faça uma cópia de backup do arquivo de script `NC_TABLESPACES.sql` e salve o arquivo em outro local.
   b. Abra o arquivo de script `NC_TABLESPACES.sql` original e use a tabela a seguir para ajudá-lo a substituir os parâmetros de marcador pelos parâmetros apropriados para seu ambiente.

Tabela 10. Nomes e descrições de parâmetros de espaços de tabela para o banco de dados de notificação do Db2 on z/OS

Nome do parâmetro	Descrição
NCCOG	Especifica o nome do banco de dados de notificação.
DSN8G810	Especifica o nome do grupo de armazenamento.
BP32K	Especifica o nome do pool de buffer.

      Nem todos os parâmetros listados estão no script, mas alguns podem ser incluídos no futuro.
   c. Salve e execute o script.

      Por exemplo,

      ```
      db2 -tvf NC_TABLESPACES.sql
      ```
   d. Abra o arquivo de script `NC_CREATE_DB2.sql` e substitua o parâmetro de marcador NCCOG pelo nome do banco de dados de notificação.
   e. Salve o script.

      Os serviços de tarefa e monitor de programação executarão o script automaticamente. No entanto, você mesmo pode executá-lo.
8. Para criar os espaços de tabela de tarefas manuais, acesse o diretório *install_location*/configuration/schemas/hts/zosdb2.
   a. Faça uma cópia de backup do arquivo de script `HTS_tablespaces.sql` e salve o arquivo em outro local.
   b. Abra o arquivo de script `HTS_TABLESPACES.sql` original e use a tabela a seguir para ajudá-lo a substituir os parâmetros genéricos pelos parâmetros apropriados para seu ambiente.

Tabela 11. Nomes e descrições de parâmetros de espaço de tabela para tarefas manuais noDb2 for z/OS

Nome do parâmetro	Descrição
NCCOG	Especifica o nome do banco de dados.
DSN8G810	Especifica o nome do grupo de armazenamento.
BP32K	Especifica o nome do buffer pool de 32 k.

Consulte o script para uma lista completa dos parâmetros necessários.

c. Salve e execute o script.

d. Abra o arquivo de script `HTS2_CREATE_Db2zos.sql` e use a tabela a seguir para ajudá-lo a substituir os parâmetros genéricos pelos parâmetros apropriados para seu ambiente.

Tabela 12. Nomes e descrições de parâmetros de espaço de tabela para tarefas manuais noDb2 for z/OS

Nome do parâmetro	Descrição
NCCOG	O nome do banco de dados.

Consulte o script para uma lista completa dos parâmetros necessários.

e. Salve e execute o script.

9. Para criar os espaços de tabela de anotações, acesse o diretório *install_location*`/configuration/schemas/ans/zosdb2`.

a. Faça uma cópia de backup do arquivo de script `ANN_TABLESPACES.sql` e salve o arquivo em outro local.

b. Abra o arquivo de script `ANN_TABLESPACES.sql` original e use a tabela a seguir para ajudá-lo a substituir os parâmetros genéricos pelos parâmetros apropriados para seu ambiente.

Tabela 13. Nomes e descrições de parâmetros de espaço de tabela para anotações noDb2 for z/OS

Nome do parâmetro	Descrição
NCCOG	O nome do banco de dados.
DSN8G810	O nome do grupo de armazenamento.
BP32K	O nome do buffer pool de 32 k.

Consulte o script para uma lista completa dos parâmetros necessários.

c. Salve e execute o script.

d. Abra o arquivo de script `ANS2_CREATE_Db2zos.sql` e use a tabela a seguir para ajudá-lo a substituir os parâmetros genéricos pelos parâmetros apropriados para seu ambiente.

Tabela 14. Nomes e descrições de parâmetros de espaço de tabela para anotações noDb2 for z/OS

Nome do parâmetro	Descrição
NCCOG	O nome do banco de dados.

Consulte o script para uma lista completa dos parâmetros necessários.

e. Salve e execute o script.

Configurar a Conectividade do Banco de Dados para um Armazenamento de Conteúdo Oracle

Este procedimento descreve como configurar a conectividade do banco de dados para um armazenamento de conteúdo do Oracle. Você deve executar este procedimento em cada computador em que instalar Content Manager.

Procedimento

1. No computador onde está instalado o cliente Oracle, acesse o diretório *ORACLE_HOME*/jdbc/lib.
2. Copie o arquivo de biblioteca correto para a sua versão do cliente Oracle no diretório *install_location*\drivers no computador em que o Content Manager estiver instalado e onde a notificação é enviada para um banco de dados Oracle.

   Se estiver usando o Oracle 12c, você deve ter ojdbc7.jar.

   Se estiver usando o Oracle 11g, você deve ter ojdbc5.jar.

   Os arquivos estão disponíveis de uma instalação do cliente ou servidor Oracle e também podem ser transferidos por download do Web site de tecnologia Oracle.

Configurar Conectividade do Banco de Dados para um Armazenamento de Conteúdo Informix

Este procedimento descreve como configurar a conectividade do banco de dados para um armazenamento de conteúdo do Informix. Você deve executar este procedimento em cada computador em que instalar Content Manager.

Procedimento

1. No computador onde o Informix está instalado, acesso o diretório *Informix_location*/sqllib/java.
2. Copie os arquivos a seguir no diretório *install_location*\drivers em cada computador em que o Content Manager estiver instalado.
   - o arquivo do driver universal, db2jcc4.jar
   - o arquivo de licença, db2jcc4_license_cisuz.jar

Ações de configuração críticas a serem executadas primeiro!

Essas ações de configuração são críticas ao sucesso da instalação. Execute estas ações depois de instalar os componentes.

Certifique-se de que os drivers JDBC estejam no local correto

Para a liberação do IBM Cognos Analytics 11.0.x, os drivers JDBC devem ser copiados para o diretório *install_location*\drivers.

O uso de *install_location*\webapps\p2pd\WEB-INF\lib para drivers JDBC não é suportado.

Substitua o driver JSQL para Microsoft SQL Server pelo driver JDBC Microsoft

A partir do IBM Cognos Analytics versão 11.0.5, o driver JSQL para Microsoft SQL Server foi substituído pelo driver JDBC Microsoft. Você deve fazer download e colocar o arquivo JAR necessário no diretório *install_location*\drivers. Para obter informações adicionais, consulte Configuração para um armazenamento de conteúdo do Microsoft SQL Server.

Especificar a propriedade Grupo de configurações

Se você usou a instalação **Customizada** para instalar o IBM Cognos Analytics, abra o IBM Cognos Configuration e configure a propriedade **Grupo de configurações**. Para obter mais informações, consulte Gerenciando o Grupo de Configurações.

Ativar ou desativar a modelagem baseada na web

Por padrão, as conexões de origem de dados JDBC que foram criadas no IBM Cognos Administration não são expostas na interface de administração **Gerenciar** > **Servidores de dados** para uso em módulos de dados. Se desejar usar suas conexões de origem de dados existentes (atualizadas) para criar módulos de dados, você deve ativar a modelagem baseada na web nessas conexões.

Algumas origens de dados são inapropriadas para uso como origens para criar módulos de dados. Nesse caso, é possível proibir o uso de modelagem baseada na web nas conexões de origem de dados.

Para ativar ou desativar a modelagem baseada na web para suas conexões de origem de dados, execute as seguintes etapas:

1. No IBM Cognos Analytics, acesse **Gerenciar** > **Console de administração**.
2. No IBM Cognos Administration, na guia **Configuração**, selecione **Conexões de origem de dados**.
3. Localize a origem de dados e clique em sua ação **Configurar propriedades**.
4. Na guia **Conexão**, selecione ou desmarque a caixa de seleção **Permitir modelagem baseada na web**.

Início do IBM Cognos Configuration

Use o IBM Cognos Configuration para configurar os componentes do IBM Cognos Analytics e para iniciar e parar os serviços do IBM Cognos.

Antes de Iniciar

Antes de iniciar o IBM Cognos Configuration, certifique-se de que o ambiente operacional esteja devidamente configurado. Por exemplo, certifique-se de que todas as variáveis de ambiente foram definidas.

Em um sistema operacional Microsoft Windows, é possível iniciar o IBM Cognos Configuration na última página do assistente de instalação somente se não for necessário fazer nenhuma configuração adicional. Por exemplo, se usar um servidor de banco de dados diferente do Microsoft SQL para o armazenamento de conteúdo, copie os drivers Java Database Connectivity (JDBC) na pasta *install_location*/drivers antes de iniciar a ferramenta de configuração.

Em sistemas operacionais UNIX ou Linux, não inicie oIBM Cognos Configuration na última página do assistente de instalação. É necessário fazer configurações adicionais para poder configurar o IBM Cognos Analytics. Por exemplo, você deve atualizar seu ambiente Java.

Assegure-se de que a conta do usuário ou do serviço usada para executar o IBM Cognos tenha sido configurada.

Leia “Ações de configuração críticas a serem executadas primeiro!” na página 1.

Procedimento

1. No Microsoft Windows, clique em **Iniciar** > **IBM Cognos Configuration**.

   Se você estiver usando um computador Windows e tiver instalado o produto no diretório `Program Files (x86)`, inicie o IBM Cognos Configuration como um Administrador.
2. Nos sistemas operacionais UNIX ou Linux, acesse o diretório *install_location*`/bin64` e digite o seguinte comando:

   `./cogconfig.sh`

   Se o IBM Cognos Configuration não abrir, certifique-se de que você configurou a variável de ambiente DISPLAY.

   Se você vir uma mensagem `JAVA.Lang.unsatisfied link`, verifique se está usando uma versão suportada do Java.

   Se você vir uma mensagem `Java.lang.unsupportedClassVersionError`, certifique de que está usando uma versão de 64 bits do Java.

Definição de propriedades de conexão com o banco de dados para o armazenamento de conteúdo

Deve-se especificar as informações do servidor de banco de dados para garantir que o Content Manager possa ser conectado ao banco de dados que você utiliza para o armazenamento de conteúdo. O Content Manager usa o logon do banco de dados para acessar o armazenamento de conteúdo. Após definir as propriedades de conexão com o banco de dados, é possível testar a conexão entre o Content Manager e o armazenamento de conteúdo.

Em um ambiente de produção, use um banco de dados de nível empresarial para armazenamento do conteúdo. Para obter mais informações, consulte o tópico sobre como implantar todo o armazenamento de conteúdo no Guia de administração e segurança.

Se você estiver fazendo upgrade do IBM Cognos Business Intelligence ou de uma liberação anterior do IBM Cognos Analytics, configure o IBM Cognos Analytics para apontar para uma cópia do banco de dados de armazenamento de conteúdo existente. Após salvar a configuração e iniciar o serviço do IBM Cognos, os dados no armazenamento de conteúdo serão automaticamente atualizados e não poderão ser usados pela versão anterior. Usando uma cópia do banco de dados original com a nova versão, é possível manter o IBM Cognos Analytics ou a versão anterior em execução com os dados originais.

Certifique-se de que um dos servidores suportados foi usado para criar o armazenamento de conteúdo.

Configurando propriedades de conexão com o banco de dados para um armazenamento de conteúdo do IBM Db2

Deve-se especificar as informações do servidor de banco de dados para garantir que o Content Manager possa ser conectado ao banco de dados que você utiliza para o armazenamento de conteúdo.

Procedimento

1. No local em que o Content Manager foi instalado, inicie o IBM Cognos Configuration.
2. Na janela **Explorer**, em **Acesso a dados**, **Content Manager**, clique em **Armazenamento de conteúdo**.

3. Na janela **Propriedades**, na propriedade **Nome do banco de dados**, digite o nome ou alias do banco de dados.
4. Altere as credenciais de logon para especificar uma ID e senha de usuário válidas:
   - Clique na caixa de seleção **Valor** próxima à propriedade **ID do usuário e senha** e clique no botão de edição quando ele aparecer.
   - Digite os valores apropriados e clique em **OK**.
5. No campo **Servidor de banco de dados e número de porta**, insira o nome de seu computador e o número da porta na qual o Db2 está em execução. Por exemplo, `localhost:50000`. Em que 50000 é o número da porta padrão usado pelo Db2. Se você estiver usando um número de porta diferente, certifique-se de usar tal valor.
6. No menu **Arquivo**, clique em **Salvar**.
7. Para testar a conexão entre o Content Manager e o banco de dados de armazenamento de conteúdo, no menu **Ações**, clique em **Testar**.

   O Content Manager se conecta ao banco de dados, verifica as permissões do banco de dados e cria e preenche uma tabela. A tabela não é excluída e será usada todas as vezes que o teste for repetido.

Configurando propriedades de conexão do banco de dados para um armazenamento de conteúdo no IBM Db2 for z/OS

Deve-se especificar as informações do servidor de banco de dados para garantir que o Content Manager possa ser conectado ao banco de dados que você utiliza para o armazenamento de conteúdo.

Procedimento

1. No local em que o Content Manager foi instalado, inicie o IBM Cognos Configuration.
2. Na janela **Explorer**, em **Acesso a Dados** > **Content Manager**, clique em **Content Store**.
3. Na janela **Propriedades**, na propriedade **Nome do banco de dados**, digite o nome ou alias do banco de dados.
4. Altere as credenciais de logon para especificar uma ID e senha de usuário válidas:
   - Clique na caixa **Valor** próxima à propriedade **ID do usuário e senha** e clique no ícone de edição quando ele aparecer. Certifique-se de especificar o ID do usuário igual ao valor especificado para **`CMSCRIPT_USERNAME`** durante a criação dos espaços de tabela.
   - Digite os valores adequados e clique em **OK**.
5. Para a propriedade **Servidor de banco de dados e número de porta**, digite as in formações do banco de dados, como *`hostname:port`*.
6. Na janela **Explorer**, clique em **Configuração Local**.
7. Clique na caixa **Valor** de **Propriedades avançadas** e, em seguida, clique no ícone de edição.

   A caixa de diálogo **Valor - Propriedades avançadas** será exibida.
8. Clique em **Incluir** para incluir os parâmetros para a conexão com o banco de dados.

   Os valores na tabela são exemplos, assegure-se de digitar os valores corretos para seu ambiente.

Tabela 15. Parâmetros de conexão do Content Store para o Db2 for z/OS

Nome do parâmetro	Exemplo de valor
CMSCRIPT_CREATE_IN	COGUCS.T1TSCS
CMSCRIPT_STOGROUP	DBOIUSR
CMSCRIPT_DATABASE	COGUCS
CMSCRIPT_CS_ID	T1
CMSCRIPT_TABLESPACE	TSCS
CMSCRIPT_LARGE_BP	BP32K
CMSCRIPT_REGULAR_BP	BP16K0

9. Clique em **Arquivo** > **Salvar**.
10. Para testar a conexão entre o Content Manager e o banco de dados de armazenamento de conteúdo, no menu **Ações**, clique em **Testar**.

Configurando as propriedades de conexão do banco de dados para um armazenamento de conteúdo Microsoft SQL Server, Oracle, Informix

Deve-se especificar as informações do servidor de banco de dados para garantir que o Content Manager possa ser conectado ao banco de dados que você utiliza para o armazenamento de conteúdo.

Procedimento

1. No computador no qual foi instalado o Content Manager, inicie o IBM Cognos Configuration.
2. Na janela do **Explorer**, em **Acesso a dados**, **Content Manager**, clique com o botão direito do mouse em **Armazenamento de conteúdo** e clique em **Excluir**.

   Esta etapa exclui a conexão para o recurso padrão. O Content Manager pode acessar apenas um armazenamento de conteúdo.
3. Clique com o botão direito em **Content Manager**, e clique em **Novo recurso**, **Banco de dados**.
4. Na caixa **Nome**, digite um nome para o recurso.
5. Na caixa de seleção **Tipo**, selecione o tipo de banco de dados e clique em **OK**.

   Dica: Se quiser usar um Oracle PDB (11.0.4) ou a funcionalidade do Oracle RAC, selecione **Banco de dados do Oracle (Avançado)**.
6. Na janela **Propriedades**, forneça valores para o seu tipo de banco de dados:
   - Se você usa um banco de dados Microsoft SQL Server, digite os valores apropriados para as propriedades **Servidor de banco de dados com número da porta ou nome da instância** e **Nome do banco de dados**.

     Para um banco de dados Microsoft SQL Server, é possível escolher usar um número da porta, como 1433, uma instância denominada como valor para a propriedade **Servidor de banco de dados com número da porta ou nome da instância**.

     Para a propriedade **Servidor de banco de dados com número da porta ou nome da instância**, inclua o nome da instância, se houver diversas instâncias do Microsoft SQL Server.

     Para conectar-se a uma instância denominada, você deve especificar o nome da instância como uma propriedade URL Java Database Connectivity (JDBC) ou uma propriedade de origem de dados. Por exemplo, é possível

digitar `localhost\instance1`. Se não forem especificadas propriedades de nome de instância, é criada uma conexão com a instância padrão.

As propriedades especificadas para a instância denominada, junto com a ID e senha de usuário e nome do banco de dados, são usados para criar um JDBC URL. Eis um exemplo:

```
jdbc:JSQLConnect://localhost\\instance1/user=sa/mais propriedades
conforme necessário
```

- Se você usar um banco de dados Oracle, digite os valores apropriados para as propriedades **Servidor de Banco de Dados e Número da Porta** e **SID**.
- 11.0.4 Se você usar um Oracle PDB, para a propriedade **Especificador do banco de dados**, digite `//<server>/<servicename>`. Por exemplo, `//corpserv1:1522/PDB1`
- Se você usar um banco de dados Oracle Net 8 avançado, para a propriedade **Especificador do banco de dados**, digite o par de valor de palavra-chave do Oracle Net8 para a conexão.

  Aqui está um exemplo de par de valor de palavra-chave do Oracle Net8:

  ```
  (description=(address=(host=myhost)(protocol=tcp)(port=1521)
  (connect_data=(sid=(orcl)))))
  ```

  Ao selecionar o banco de dados Oracle avançado, o IBM Cognos Analytics utiliza recursos do Oracle orientados para empresas para selecionar um listener, alternar para outro listener se o primeiro listener falhar, reconectar-se automaticamente ao banco de dados se a conexão falhar, equilibrar as solicitações de conexão entre listeners e equilibrar as solicitações de conexão entre dispatchers.
- Se estiver usando um banco de dados Informix, digite os valores apropriados para as propriedades **Servidor de banco de dados e número da porta** e **Nome do banco de dados**.

7. Para configurar credenciais de logon, especifique uma ID e senha de usuário:
   - Clique na caixa **Valor** próxima à propriedade **ID do usuário e senha** e clique no ícone de edição quando ele aparecer.
   - Digite os valores apropriados e clique em **OK**.
8. Se hospedar mais de um banco de dados de armazenamento de conteúdo em uma instância do Informix, crie a propriedade avançada CMSCRIPT_CS_ID e especifique a conta na qual a instância será executada:
   - Na janela **Explorer**, clique em **Configuração Local**.
   - Na janela **Propriedades**, clique na coluna **Valor** de **Propriedades Avançadas** e, em seguida, clique no ícone de edição.
   - Na caixa de diálogo **Valor - Propriedades avançadas**, clique em **Adicionar**.
   - Na coluna **Nome**, digite `CMSCRIPT_CS_ID`
   - Na coluna **Valor**, digite o ID do usuário da conta na qual a instância do armazenamento de conteúdo é executada.

     Use uma conta do usuário diferente para cada instância do banco de dados de armazenamento de conteúdo do Informix.
9. No menu **Arquivo**, clique em **Salvar**.

   As credenciais de logon são imediatamente criptografadas.
10. Para testar a conexão entre o Content Manager e o banco de dados de armazenamento de conteúdo, no menu **Ações**, clique em **Testar**.

    O Content Manager se conecta ao banco de dados, verifica as permissões do banco de dados e cria e preenche uma tabela. A tabela não é excluída e será usada todas as vezes que o teste for repetido.

Resultados

Agora o Content Manager poderá criar as tabelas necessárias no armazenamento de conteúdo quando o serviço IBM Cognos for iniciado pela primeira vez. Se as propriedades da conexão não estiverem especificadas corretamente, não será possível iniciar os serviços do IBM Cognos.

Configuração de propriedades do ambiente para computadores com Content Manager

Os computadores do Content Manager devem conhecer a localização do armazenamento de conteúdo, outros computadores com Content Manager e o banco de dados utilizado para notificação.

Depois de instalar o Content Manager em computadores utilizados para proteção de failover, é preciso configurar o Content Manager nesses computadores. Se mais de um Content Manager foi instalado, liste todos os URIs de Content Manager em cada computador com Content Manager.

Após a conclusão das tarefas de configuração necessárias e o início do serviço do IBM Cognos Analytics, o serviço de autoridade de certificação ficará disponível para emitir certificados para outros computadores. É possível então executar as tarefas de configuração exigidas em outros computadores, como o computador de Application Tier Components e computadores de gateway. Caso contrário, é possível continuar configurando os computadores com Content Manager alterando as configurações de propriedade padrão (consulte "Alteração de definições de configuração padrão" na página 149) para adequá-las ao seu ambiente. Por exemplo, é possível configurar os componentes do IBM Cognos Analytics para usar um provedor de autenticação (consulte Capítulo 8, "Configurando provedores de autenticação", na página 233), ativar e desativar serviços (consulte "Ativação e desativação de serviços" na página 163) nos computadores com Content Manager ou alterar configurações globais (consulte "Alteração de definições globais" na página 211).

Observe que, caso as configurações globais sejam alteradas em um computador com Content Manager, é necessário fazer as mesmas mudanças nos outros computadores com Content Manager.

Configurando o Content Manager Ativo

Os computadores do Content Manager devem conhecer a localização do armazenamento de conteúdo, outros computadores com Content Manager e o banco de dados utilizado para notificação.

Procedimento

1. No computador com Content Manager que você quer designar como o Content Manager ativo padrão, inicie o IBM Cognos Configuration.
2. Na janela **Explorer**, clique em **Ambiente**.
3. Na janela **Propriedades**, clique no valor para **URIs do Content Manager** e clique no botão de edição.
4. Especifique os URIs para os outros computadores com Content Manager:
   - Na caixa de diálogo **Valor - URIs do Content Manager**, clique em **Adicionar**.
   - Na linha em branco da tabela, clique e digite o URI completo do computador com Content Manager.

Não exclua o primeiro valor na tabela. O valor identifica o computador local com Content Manager e é solicitado.

Substitua a parte do localhost do URI por um nome do host ou endereço IP. Todas as propriedades do URI devem usar o mesmo formato: todos os nomes de host ou todos os endereços IP.

- Repita as duas etapas anteriores para cada URI a ser adicionado.

  É necessário incluir todos os URIs do Content Manager na lista.
- Clique em **OK**.

5. No menu **Arquivo**, clique em **Salvar**.

Configurando Content Managers em Espera

Os computadores do Content Manager devem conhecer a localização do armazenamento de conteúdo, outros computadores com Content Manager e o banco de dados utilizado para notificação.

Procedimento

1. Certifique-se de já ter configurado as propriedades de Ambiente em pelo menos um computador com Content Manager e que os componentes do IBM Cognos Analytics estejam em execução nesse computador.
2. No computador com Content Manager em espera, inicie o IBM Cognos Configuration.
3. Na janela **Explorer**, clique em **Ambiente**.
4. Na janela **Propriedades**, clique no valor de **URIs do Content Manager** e no botão de edição.
5. Especifique os URIs para os outros computadores com Content Manager:
   - Na caixa de diálogo **Valor - URIs do Content Manager**, clique em **Adicionar**.
   - Na linha em branco da tabela, clique e digite o URI completo do computador com Content Manager.

     Não exclua o primeiro valor na tabela. O valor identifica o computador local com Content Manager e é solicitado.

     Substitua a parte do localhost do URI por um nome do host ou endereço IP. Todas as propriedades do URI devem usar o mesmo formato: todos os nomes de host ou todos os endereços IP.
   - Repita as duas etapas anteriores para cada URI a ser adicionado.

     É necessário incluir todos os URIs do Content Manager na lista.
   - Clique em **OK**.
6. Na janela **Explorer**, em **Segurança** > **Criptografia**, clique em **Cognos**, o provedor de criptografia padrão.
7. Certifique-se de que as definições criptográficas correspondam ao que foi definido no computador ativo padrão com Content Manager.
8. Na janela **Explorer**, em **Acesso a Dados** > **Content Manager**, clique em **Armazenamento de Conteúdo**.
9. Certifique-se de que os valores para todas as propriedades coincidam com o que foi configurado no computador ativo padrão com Content Manager.
10. No menu **Arquivo**, clique em **Salvar**.

Especifique uma conexão com um servidor de e-mail

Se desejar enviar relatórios por e-mail, deve-se configurar uma conexão com seu servidor de e-mail.

Procedimento

1. Na janela **Explorer**, em **Acesso a dados**, clique em **Notificação**.
2. Na janela **Propriedades**, para a propriedade **Servidor de e-mail SMTP**, digite o nome do host e a porta do servidor de e-mail SMTP (saída).

   Para poder abrir relatórios que são enviados por e-mail, deve-se mudar a parte do nome do host do **URI do gateway** de host local para o endereço IP do computador ou para o nome do computador. Caso contrário, a URL no e-mail conterá host local e os usuários remotos não poderão abrir o relatório.

   Para poder abrir relatórios que são enviados como links, certifique-se de que o **URI do gateway** nos servidores de relatório e servidores de notificação especifique um servidor da web acessível que hospede o conteúdo do IBM Cognos. Se tiver usuários móveis acessando os links remotamente, considere o uso de um URI externo.
3. Clique na caixa **Valor** ao lado da propriedade **Conta e senha** e clique no botão de edição quando ele aparecer.
4. Digite os valores na caixa de diálogo **Valor - conta e senha** e clique em **OK**.

   Se as credenciais de logon não forem necessárias para o servidor SMTP, remova as informações padrão da propriedade **Conta e senha**. Quando for solicitada a confirmação para deixar essa propriedade em branco, clique em **OK**. Certifique-se de que o nome do usuário padrão seja removido. Caso contrário, a conta padrão será usada e as notificações não funcionarão corretamente.
5. Na janela **Propriedades**, digite o valor apropriado para a conta do remetente padrão.
6. Na janela **Explorer**, clique com o botão direito em **Notificação** e clique em **Testar**.

   O IBM Cognos Analytics testa a conexão do servidor de e-mail.

Ativando uma conexão TLS segura com seu servidor de e-mail

Ative uma conexão TLS segura para seu servidor de e-mail para permitir a comunicação TLS criptografada.

Nota: Se a Criptografia SSL estiver configurada, mas uma conexão TLS segura não estiver ativada, a conexão falhará e a mensagem a seguir aparecerá:

502 Comando desconhecido

Antes de Iniciar

Deve-se ter um certificado, geralmente no formato .crt, que seja comum para o servidor de e-mail.

Procedimento

1. Importe o certificado para ativar uma confiança entre o Cognos Analytics e o servidor de e-mail.
   a. Se você está usando HTTP no URI do dispatcher, deve-se importar o certificado para o keystore do JRE:
      - No Windows, digite *install_location*\bin\DLS_SSL_CertImportTool.bat *certificate_location**email_certificate*.crt -p *keystore_password*
      - No Unix ou Linux, digite *install_location*/bin/DLS_SSL_CertImportTool.sh *certificate_location*/*email_certificate*.crt -p *keystore_password*

b. Se você está usando HTTPS no URI do dispatcher, deve-se importar o certificado para o keystore do Cognos:
   - No Windows, digite *install_location*\bin\ ThirdPartyCertificateTool.bat -T -i -r *certificate_location*\ *email_certificate*.crt -p *keystore_password*
   - No Unix ou Linux, digite *install_location*/bin/ ThirdPartyCertificateTool.sh -T -i -r *certificate_location*/ *email_certificate*.crt -p *keystore_password*

2. Em Cognos Configuration, selecione **Acesso a dados** > **Notificação** e edite a propriedades conforme a seguir:

Nome	valor
Servidor de Correio SMTP	*email_server_name*:*port_number*, em que *port_number* representa uma porta que está ativada para TLS/SSL ou STARTTLS
Conta e senha	Um ID do usuário e senha quando a autenticação para o servidor de e-mail é necessária.
Emissor Padrão	A conta de e-mail que envia e-mails por meio do servidor de e-mail.
Criptografia SSL Ativada	Verdadeiro

3. Em Cognos Configuration, selecione **Configuração local**.
   a. Clique no campo **Valor** para **Propriedades avançadas**.
   b. Clique no ícone de lápis .
   c. Clique em **Incluir**.
   d. No campo **Nome**, digite `emf.mail.tls.enabled`
   e. No campo **Valor**, digite `true`
   f. Clique em **OK**.
4. Em Cognos Administration, defina a configuração avançada `emf.mail.tls.enabled` com um valor de `true`. Para obter mais informações, veja *Definindo configurações avançadas para serviços específicos*.

   Nota: Deve-se reiniciar o serviço de entrega depois de fazer essa mudança.

Ativação da segurança

Por padrão, o IBM Cognos Analytics permite o acesso anônimo. Se quiser usar a segurança no ambiente do IBM Cognos Analytics, você deve desativar o acesso anônimo e configurar o IBM Cognos Analytics para usar um provedor de autenticação.

Procedimento

1. Na janela IBM Cognos Configuration **Explorer**, clique em **Segurança** >**Autenticação** > **Cognos**.
2. Clique na caixa **Valor** para **Permitir acesso anônimo** e selecione **Falso**.
3. Clique com o botão direito do mouse em **Autenticação** e clique em **Novo Recurso** > **Namespace**.
4. Na caixa **Nome**, digite um nome para o namespace de autenticação.
5. Na lista **Tipo**, clique no tipo de namespace apropriado e clique em **OK**.

   O novo recurso provedor de autenticação aparece na janela **Explorer**, no componente **Autenticação**.

6. Na janela **Propriedades**, na propriedade **ID do namespace**, especifique um identificador exclusivo para o namespace.
7. No menu **Arquivo**, clique em **Salvar**.

Início do Content Manager

Depois de ter configurado as propriedades de conexão do banco de dados para o armazenamento de conteúdo e configurado o namespace de segurança, é possível iniciar o computador com o Content Manager.

Antes de Iniciar

Certifique-se de que a conta de usuário ou serviço esteja definida. Para obter mais informações, consulte "Configurar uma conta do usuário ou uma conta do serviço de rede para o IBM Cognos Analytics" na página 14.

Procedimento

1. Inicie o IBM Cognos Configuration.

   Se estiver atualizando, será exibida uma mensagem indicando que os arquivos de configuração foram detectados e atualizados para a nova versão.
2. Certifique-se de que suas configurações foram salvas, caso contrário, não será possível iniciar o serviço do IBM Cognos.
3. No menu **Ações**, clique em **Testar**.

   O IBM Cognos Configuration verifica a disponibilidade da chave simétrica comum (CSK), testa a configuração do namespace e testa as conexões com o armazenamento de conteúdo e outros recursos.

   Dica: Se **Teste** não estiver disponível para seleção, na janela **Explorer**, clique em **Configuração Local**.
4. Se o teste falhar, configure novamente as propriedades afetadas e faça o teste de novo.

   É possível testar alguns componentes individualmente clicando com o botão direito no componente na área de janela **Explorer** e selecionando **Testar**.

   Não inicie o serviço até que todos os testes estejam livres de erro.
5. No menu **Ações**, clique em **Iniciar**.

   Pode levar alguns minutos para o serviço do IBM Cognos iniciar.

   Essa ação inicia todos os serviços instalados que não estão em execução e registra o serviço do IBM Cognos no Windows.

Testar a instalação do Content Manager

É possível testar a instalação utilizando um navegador da web.

Procedimento

1. Abra um navegador web.
2. Teste se o Content Manager está sendo executado digitando a URI do Content Manager. Por exemplo, `http://host_name:port/p2pd/servlet`

   O valor padrão para *nome_host:porta* é localhost:9300.

   O Content Manager está disponível quando o valor de **State** é **Running** ou **Standby**.

Instalando e configurando os serviços de aplicativo

É possível instalar os componentes de serviço de aplicativo em computadores diferentes ou no mesmo computador.

Instalar os componentes de serviço de aplicativo

Certifique-se de que o computador no qual o Content Manager ativo foi instalado esteja configurado e disponível antes de configurar os computadores dos componentes de serviço de aplicativo.

Se você estiver fazendo upgrade, o IBM Cognos Analytics usará os dados de configuração existentes para os computadores de componentes de serviços de aplicativo. No entanto, caso você tenha instalado os componentes de serviço de aplicativo em um novo local, deverá configurar as propriedades de ambiente.

Instalações de 64 bits

O componente do servidor de relatório, incluído com os componentes de serviço de aplicativo, é fornecido nas versões de 32 bits e de 64 bits. A seleção da versão usada é feita com o IBM Cognos Configuration após a instalação. Por padrão, o componente do servidor de relatório está configurado para usar o modo de 32 bits, mesmo em um computador de 64 bits. O modo de 32 bits permite executar todos os relatórios, enquanto o modo de 64 bits permite executar apenas os relatórios criados para o modo de consulta dinâmica.

Requisitos de impressora

Para certificar-se de que os relatórios sejam impressos corretamente em um sistema operacional Microsoft Windows, o Adobe Reader requer a configuração de pelo menos uma impressora no sistema operacional no qual os componentes de serviço de aplicativo estão instalados. Todos os relatórios, independente do formato de impressão escolhido, são enviados como arquivos PDF temporários para o Adobe Reader para impressão.

Instalando os componentes de serviços de aplicativo em sistemas operacionais UNIX ou Linux

É possível instalar os componentes de serviço de aplicativo em um ou mais computadores, dependendo do ambiente.

Antes de Iniciar

Acesse IBM Software Product Compatibility Reports (www.ibm.com/support/docview.wss?uid=swg27047186) para verificar se as correções necessárias estão instaladas em seu computador.

Procedimento

1. Acesse o local em que os arquivos de instalação foram transferidos por download e extraídos.

   Dica: Use novas versões de software de compactação arquivo para extrair os arquivos. Versões mais antigas desse software não podem extrair os arquivos.
2. Para iniciar o assistente de instalação, acesse o diretório do sistema operacional e, em seguida, digite `./ca_srv_<platform>_<build>.bin`

Dica: Ao usar o comando `ca_srv_<platform>_<build>.bin` com o XWindows, os caracteres japoneses em mensagens e arquivos de log podem ficar corrompidos. Ao instalar em japonês no UNIX ou Linux, primeiro configure as variáveis de ambiente LANG=C e LC_ALL=C (em que C é o código de idioma, por exemplo, ja_JP.PCK no Solaris) e inicie o assistente de instalação.

Se não estiver usando o XWindows, execute uma instalação não assistida. Para obter mais informações, consulte "Use uma instalação não assistida" na página 291.

3. Siga as instruções do assistente de instalação e copie os arquivos para seu computador.
   - Ao selecionar o diretório, considere o seguinte:

     Instale os componentes de serviço de aplicativo em um diretório que contém somente caracteres ASCII no nome do caminho. Alguns servidores da Web UNIX e Linux não suportam caracteres não ASCII em nomes de diretório.
   - Ao selecionar os componentes, desmarque todos os componentes, exceto **Serviços de aplicativo**.
4. Clique em **Concluir**. Não configure o IBM Cognos Analytics imediatamente, porque é necessário executar outras tarefas primeiro, para garantir que o ambiente esteja adequadamente configurado.
5. Anexe o diretório *install_location*`/bin` na variável de ambiente do caminho de biblioteca apropriado.
   - Para Solaris e Linux, LD_LIBRARY_PATH
   - Para AIX, LIBPATH
   - Para HP-UX, SHLIB_PATH

O que Fazer Depois

Configure o IBM Cognos Analytics usando o IBM Cognos Configuration. Abra essa ferramenta digitando `cogconfig.sh` no diretório *install_location*`/bin64`.

Instalando os componentes de serviços de aplicativo em um sistema operacional Windows

É possível instalar os componentes de serviços de aplicativo em um ou mais computadores, dependendo de seu ambiente.

Para computadores Windows, o local de instalação padrão usa o diretório **Arquivos de programa**. Se você instalar nesse local, assegure-se de executar o IBM Cognos Configuration como um administrador. Como alternativa, é possível instalar o produto em um diretório fora de **Arquivos de Programa**, como `C:\IBM\cognos\analytics`.

Procedimento

1. Acesse o local em que os arquivos de instalação foram transferidos por download e extraídos e dê um clique duplo em `ca_srv_<platform>_<build>.exe`.

   Dica: Use novas versões de software de compactação arquivo para extrair os arquivos. Versões mais antigas desse software não podem extrair os arquivos.
2. Selecione o idioma para utilizar na instalação.

   Essa seleção determina o idioma da interface com o usuário. Todos os idiomas suportados são instalados. É possível alterar a interface com o usuário para qualquer um dos idiomas instalados depois de concluída a instalação.

3. Selecione a opção de instalação **Customizada** e siga as instruções do assistente de instalação para copiar os arquivos para seu computador.
   - Ao selecionar o diretório, considere o seguinte:

     Instale os componentes de serviços de aplicativo em um diretório que contenha somente caracteres ASCII no nome do caminho. Alguns servidores da Web não suportam caracteres não ASCII nos nomes de diretório.
   - Ao selecionar os componentes, desmarque todos os componentes, exceto **Serviços de aplicativo**.
4. Clique em **Concluir**.

O que Fazer Depois

É possível iniciar o IBM Cognos Configuration usando o atalho **IBM Cognos Configuration** do menu **Iniciar**.

Configurar a Conectividade de Banco de Dados para Bancos de Dados de Relatório

Para suportar a comunicação entre o IBM Cognos Analytics e as fontes de dados, é preciso instalar software adicional para as suas fontes de dados no mesmo computador que hospeda o servidor de relatórios. Dependendo da origem de dados e do modo de consulta, o software necessário pode incluir clientes de banco de dados e/ou arquivos do driver Java Database Connectivity (JDBC).

Para o IBM Cognos Analytics, o banco de dados de consulta (também conhecido como o banco de dados de relatório) é acessado apenas pelo mecanismo de relatório que executa relatórios. O mecanismo de relatório é instalado com os Componentes da Camada de Aplicativos e também é usado pelo Framework Manager e IBM Cognos Transformer.

Modo de consulta compatível

Para executar relatórios que usam modo de consulta compatível, você deve usar bibliotecas de clientes de origem de dados de 32 bits e configurar o servidor de relatório para 32 bits. O modo de consulta compatível usa cliente nativo e conexões ODBC para se comunicar com origens de dados.

Modo de consulta dinâmica

O modo de consulta dinâmica fornece comunicação a origens de dados usando conexões Java/XMLA.

Para bancos de dados relacionais compatíveis, exige-se uma conexão JDBC tipo 4. O driver JDBC tipo 4 converte as chamadas JDBC diretamente para o protocolo de banco de dados específico do fornecedor. Ele está escrito em Java puro e é independente de plataforma.

Para origens de dados OLAP compatíveis, a conectividade Java/XMLA otimiza o acesso ao oferecer MDX customizado e aprimorado para a origem e a versão específicas da tecnologia OLAP e se conecta aos smarts da origem de dados OLAP.

Para revisar uma lista atualizada de ambientes suportados pelos produtos do IBM Cognos Analytics, incluindo informações sobre sistemas operacionais, correções, navegadores, servidores da web, servidores de diretório, servidores de banco de dados e servidores de aplicativos, consulte a página IBM Software Product

Compatibility Reports (www.ibm.com/support/docview.wss?uid=swg27047186).

Acessar Origens de Dados OLAP em Sistemas Operacionais Windows

Para acessar os bancos de dados relacionais e as origens de dados OLAP para relatórios, você deve instalar o software de API do cliente disponibilizado pelo fornecedor da origem de dados. O software deve ser instalado no mesmo computador no qual os Componentes da Camada de Aplicativos estão instalados.

Procedimento

1. Instale o software de API do banco de dados para os bancos de dados relacionais e as origens de dados OLAP no computador host do servidor de relatórios (no qual Componentes da Camada de Aplicativos estão instalados).

   Nos sistemas operacionais Microsoft Windows, o mecanismo de relatório suporta a conectividade do banco de dados nativo ou ODBC.
2. Se o Framework Manager estiver instalado em um local separado dos Componentes da Camada de Aplicativos, também é necessário instalar o software da API cliente no computador no qual o Framework Manager está instalado. Para obter mais informações, consulte "Configurando variáveis para conexões de origem de dados para o Framework Manager" na página 133.

Acessar Origens de Dados ODBC em Sistemas Operacionais UNIX ou Linux

Para usar uma origem de dados ODBC no UNIX ou Linux para conectar-se a uma origem de dados suportada, é necessário configurar o ambiente para localizar o arquivo `.odbc.ini` que contém as referências para a origem de dados, as bibliotecas de conectividade e suas bibliotecas do Gerenciador de Drivers acompanhantes.

Para revisar as origens de dados ODBC suportadas, consulte IBM Software Product Compatibility Reports (www.ibm.com/support/docview.wss?uid=swg27047186).

Após configurar as conexões do ODBC, você deve criar conexões com as origens de dados no IBM Cognos Administration. Para obter informações, consulte o *Guia de Administração e Segurança do IBM Cognos*.

Se seu fornecedor de banco de dados não fornecer um gerenciador de drivers, é possível usar o unixODBC ou iODBC, dependendo do seu sistema operacional.

Nos sistemas operacionais Linux, o pacote unixODBC fornecido com o sistema operacional fornece o ODBC Driver Manager. É necessário instalar o unixODBC versão 2.2.11 ou posterior antes de poder configurar as conexões de origem de dados. Para verificar a versão instalada, use o comando a seguir: `odbcinst --version`. Verifique qual versão do unixODBC é necessária para o banco de dados que está sendo usado e assegure-se de usar essa versão.

Nos sistemas operacionais UNIX, o gerenciador de drivers iODBC de software livre é fornecido como parte da instalação do IBM Cognos.

Procedimento

1. Crie uma variável de ambiente para especificar o local do arquivo `.odbc.ini`.

   Por exemplo,

   ```
   export ODBCINI=/usr/local/etc/.odbc.ini
   ```

2. Configure a variável de ambiente apropriada do caminho da biblioteca para especificar o local das bibliotecas de conectividade de 32 bits e do Driver Manager para seu banco de dados.

   A tabela a seguir lista as variáveis de ambiente para cada sistema operacional que deve especificar o local das bibliotecas do gerenciador de drivers.

Tabela 16. Variáveis de Ambiente para seu Sistema Operacional

Sistema operacional	Variável do ambiente
AIX	LIBPATH
Solaris e Linux	LD_LIBRARY_PATH

3. Se seu fornecedor de banco de dados não fornecer um gerenciador de drivers, configure o caminho da biblioteca para incluir o caminho do gerenciador de drivers local.
   - No UNIX, iODBC é fornecido como parte da instalação do IBM Cognos. Os arquivos de biblioteca estão localizados no diretório *install_location*/bin. O caminho da biblioteca já deve conter o diretório *install_location*/bin.

     Por exemplo,

     ```
     LIBPATH=/usr/IBM/cognos/bin:$LIBPATH
     ```
   - No Linux, o pacote unixODBC fornece as bibliotecas do gerenciador de drivers necessárias.

     Por exemplo,

     ```
     LD_LIBRARY_PATH=/usr/lib:$LD_LIBRARY_PATH
     ```

O que Fazer Depois

Se você estiver usando diversas origens ODBC nos sistemas operacionais UNIX ou Linux, é possível encontrar dependências dos arquivos de biblioteca com nomes comuns, mas implementações diferentes para a conectividade e o gerenciador de drivers. Em um cenário no qual uma origem ODBC é validada enquanto outra falha com base em uma dependência, entre em contato com o Suporte ao Cliente. Usar um `.odbc.ini` comum pode resultar em ter entradas incompatíveis para diferentes gerenciadores de drivers. Para resolver o problema, revise os requisitos de estrutura entre os gerenciadores de drivers que você está usando e tente usar a sintaxe que é comum entre os gerenciadores de drivers conflitantes.

Configurando o IBM Cognos Analytics para usar o Oracle Essbase

Se você usar o IBM Cognos Analytics com uma origem de dados Oracle Essbase versão 11.1.1, deverá editar um arquivo de configuração para informar ao servidor IBM Cognos Analytics a sua versão.

Por padrão, o IBM Cognos Analytics é configurado para usar o Oracle Essbase versão 11.1.2. Portanto, nenhuma configuração é necessária se você usar esta versão. Se você usar outra versão suportada do Oracle Essbase, deverá editar o arquivo qfs.config.xml para sua versão.

Além disso, se você usar o Oracle Essbase versão 11.1.2, deverá instalar o Oracle Foundation Services, bem como o cliente Oracle Essbase.

Procedimento

1. Acesse o diretório *install_location*/configuration.
2. Abra o arquivo qfs_config.xml em um xml ou editor de texto.

3. Localize as seguintes linhas:

```
<!--provider name="DB2OlapODP" libraryName="essodp111" connectionCode="DO"-->
<provider name="DB2OlapODP" libraryName="essodp1112" connectionCode="DO">
```

4. Para Oracle Essbase 11.1.1, altere-as da seguinte maneira:

```
<provider name="DB2OlapODP" libraryName="essodp111" connectionCode="DO">
<!--provider name="DB2OlapODP" libraryName="essodp1112" connectionCode="DO"-->
```

5. Para Oracle Essbase 11.1.2, assegure-se de que as linhas aparecem da seguinte maneira:

```
<!--provider name="DB2OlapODP" libraryName="essodp111" connectionCode="DO"-->
<provider name="DB2OlapODP" libraryName="essodp1112" connectionCode="DO">
```

6. Salve o arquivo e reinicie o serviço do IBM Cognos

Configurando o Oracle Essbase em um Sistema Operacional UNIX ou Microsoft Windows de 64 Bits

Se usar uma origem de dados Oracle Essbase versão 11.1.2 com o IBM Cognos Analytics em um sistema operacional UNIX ou Microsoft Windows de 64 bits, deve-se configurar manualmente as variáveis de ambiente **ARBORPATH** e **ESSBASEPATH**.

As variáveis de ambiente **ARBORPATH** e **ESSBASEPATH** são criadas durante a instalação do cliente Oracle Essbase. O IBM Cognos Analytics usa essas variáveis para encontrar o local do cliente Oracle Essbase.

Para usar o Oracle Essbase com o IBM Cognos Analytics em um sistema operacional UNIX ou Microsoft Windows de 64 bits, você deve instalar o cliente Oracle Essbase de 64 bits. Esse cliente de 64 bits inclui um cliente de 32 bits que é usado pelo IBM Cognos Analytics. Para apontar para esse cliente de 32 bits, deve-se alterar manualmente as variáveis de ambiente **ARBORPATH** e **ESSBASEPATH** para substituir o `EssbaseClient` pelo `EssbaseClient-32`. O exemplo a seguir supõe que o cliente esteja instalado na unidade C. O local de instalação pode ser diferente.

```
ARBORPATH=C:\Hyperion\EPMSystem11R1\products\Essbase\EssbaseClient-32
ESSBASEPATH=C:\Hyperion\EPMSystem11R1\products\Essbase\EssbaseClient-32
```

Se você usar um sistema operacional Microsoft Windows de 32 bits com o cliente Oracle Essbase de 32 bits, não será necessário alterar essas variáveis de ambiente.

Início do IBM Cognos Configuration

Use o IBM Cognos Configuration para configurar os componentes do IBM Cognos Analytics e para iniciar e parar os serviços do IBM Cognos.

Antes de Iniciar

Antes de iniciar o IBM Cognos Configuration, certifique-se de que o ambiente operacional esteja devidamente configurado. Por exemplo, certifique-se de que todas as variáveis de ambiente foram definidas.

Em um sistema operacional Microsoft Windows, é possível iniciar o IBM Cognos Configuration na última página do assistente de instalação somente se não for necessário fazer nenhuma configuração adicional. Por exemplo, se usar um servidor de banco de dados diferente do Microsoft SQL para o armazenamento de conteúdo, copie os drivers Java Database Connectivity (JDBC) na pasta *install_location*/drivers antes de iniciar a ferramenta de configuração.

Em sistemas operacionais UNIX ou Linux, não inicie oIBM Cognos Configuration na última página do assistente de instalação. É necessário fazer configurações adicionais para poder configurar o IBM Cognos Analytics. Por exemplo, você deve atualizar seu ambiente Java.

Assegure-se de que a conta do usuário ou do serviço usada para executar o IBM Cognos tenha sido configurada.

Leia "Ações de configuração críticas a serem executadas primeiro!" na página 1.

Procedimento

1. No Microsoft Windows, clique em **Iniciar** > **IBM Cognos Configuration**.

   Se você estiver usando um computador Windows e tiver instalado o produto no diretório `Program Files (x86)`, inicie o IBM Cognos Configuration como um Administrador.
2. Nos sistemas operacionais UNIX ou Linux, acesse o diretório *`install_location`*`/bin64` e digite o seguinte comando:

   `./cogconfig.sh`

   Se o IBM Cognos Configuration não abrir, certifique-se de que você configurou a variável de ambiente DISPLAY.

   Se você vir uma mensagem `JAVA.Lang.unsatisfied link`, verifique se está usando uma versão suportada do Java.

   Se você vir uma mensagem `Java.lang.unsupportedClassVersionError`, certifique de que está usando uma versão de 64 bits do Java.

Configurar propriedades do ambiente para computadores de componentes de serviço de aplicativo

Ao instalar os componentes de serviço de aplicativo em um computador diferente do Content Manager, deve-se configurar o computador dos componentes de serviço de aplicativo para que ele saiba o local do Content Manager. Os componentes distribuídos podem então se comunicar um com o outro.

O computador dos componentes de serviço de aplicativo devem saber o local dos computadores com Content Manager e o banco de dados de notificação a ser usado para obter informações de tarefas e planejamento. O computador dos componentes de serviço de aplicativo deve usar o banco de dados de notificação usado pelos computadores com Content Manager. Para obter mais informações, consulte "Alterar o Banco de Dados de Notificação" na página 174.

Caso você tenha instalado mais de um Content Manager, deve-se listar todos os URIs do Content Manager em cada computador dos componentes de serviço de aplicativo.

Procedimento

1. Inicie o IBM Cognos Configuration.
2. Na janela **Explorer**, clique em **Ambiente**.
3. Na janela **Propriedades**, altere a porção **localhost** da propriedade **URIs do Content Manager** para o nome de qualquer computador com o Content Manager.
4. Especifique os URIs para os outros computadores com Content Manager:
   - Na caixa de diálogo **Valor - URIs do Content Manager**, clique em **Adicionar**.

- Na linha em branco da tabela, clique e digite o URI completo do computador com Content Manager.

  Substitua a parte do localhost do URI por um nome do host ou endereço IP. Todas as propriedades do URI devem usar o mesmo formato: todos os nomes de host ou todos os endereços IP.
- Repita as duas etapas anteriores para cada URI a ser adicionado.

  É necessário incluir todos os URIs do Content Manager na lista.
- Clique em **OK**.

5. Altere a parte **localhost** da propriedade **URI do gateway** para o nome do computador no qual planeja instalar o componente do gateway.

   Isso garantirá que os usuários em locais diferentes possam se conectar a relatórios e áreas de trabalho enviados por e-mail.
6. Altere a parte **localhost** das propriedades de URI restantes para o nome ou endereço IP do servidor IBM Cognos Analytics.
7. Na janela **Explorer**, em **Segurança** > **Criptografia**, clique em **Cognos**, o provedor de criptografia padrão.
8. No grupo de propriedades **Configuração da autoridade de certificação**, defina a propriedade **Senha** para coincidir com as configurações do computador com Content Manager ativo padrão.
9. Certifique-se de que as definições criptográficas coincidam com o que foi definido no computador com Content Manager ativo padrão.
10. No menu **Arquivo**, clique em **Salvar**.

Ativando a versão de 64 bits de um servidor de relatório

É possível escolher o uso de uma versão de 32 bits ou de 64 bits do componente do servidor de relatório. Para usar a versão de 64 bits, é necessário ativá-la usando o IBM Cognos Configuration. A opção padrão é 32 bits.

Um servidor de relatório de 32 bits pode ser usado com os pacotes de modo de consulta dinâmica e modo de consulta compatível. Um servidor de relatório de 64 bits pode ser usado apenas com pacotes de modo de consulta dinâmica.

O servidor de relatório trabalha com o serviço de consulta. O serviço de consulta é o mecanismo que ativa o modo de consulta dinâmica e os cubos dinâmicos. Em uma instalação de 64 bits, o serviço de consulta é de 64 bits, independentemente de o componente do servidor de relatório estar configurado para 32 bits ou 64 bits.

O uso da versão de 64 bits do servidor de relatório permite mais memória endereçável para renderização de saídas de relatório. Por exemplo, condições de falta de memória durante o estágio de renderização da execução de um relatório podem ser evitadas. Apenas saídas de relatório grandes, por exemplo, relatórios em PDF com mais de mil páginas, requerem a versão de 64 bits do componente do servidor de relatório.

Você deve utilizar a versão de 32 bits do servidor de relatório para pacotes que não utilizam o modo de consulta dinâmica. Por exemplo, se o seu pacote se basear no IBM Cognos PowerCubes, você deve usar a versão de 32 bits do servidor de relatório.

Se você tiver várias instâncias de Componentes da Camada de Aplicativos em seu ambiente, você pode configurar uma instância para utilizar o servidor de relatório de 32 bits. Em seguida, você pode utilizar regras de roteamento para que pedidos de relatório para pacotes de modo de consulta não dinâmica sejam roteados para a

instância que está executando a versão de 32 bits de servidor de relatório. Para obter mais informações sobre regras de roteamento, consulte o *Guia de Administração e Segurança*.

Para ativar a versão de 64 bits, você deve instalar a versão de 64 bits dos Componentes da camada de Aplicativos em um computador de 64 bits. Se você instalar a versão de 32 bits dos Componentes da Camada de Aplicativos ou estiver usando um computador de 32 bits, não ative o servidor de relatório de 64 bits.

Procedimento

1. Na janela **Explorer** do IBM Cognos Configuration, clique em **Ambiente**.
2. Clique na caixa **Valor** para **Modo de Execução do Servidor de Relatório** e selecione **64 Bits**.
3. No menu **Arquivo**, clique em **Salvar**.
4. Reinicie os serviços do IBM Cognos se eles estiverem em execução.

Iniciar os componentes de serviço de aplicativo

Depois de configurar as propriedades do ambiente, é possível iniciar os serviços no computador dos componentes de serviço de aplicativo.

Antes de Iniciar

Para usar o IBM Cognos Analytics para relatórios, você deve instalar e configurar os componentes do servidor, iniciar o serviço do IBM Cognos e ter um pacote que faça referência a uma origem de dados disponível. Observe que se estiver atualizando, é possível continuar a usar as mesmas origens de dados.

Certifique-se de que a conta de usuário ou serviço esteja definida. Para obter mais informações, consulte “Configurar uma conta do usuário ou uma conta do serviço de rede para o IBM Cognos Analytics” na página 14.

Procedimento

1. Inicie o IBM Cognos Configuration.

   Se estiver atualizando, será exibida uma mensagem indicando que os arquivos de configuração foram detectados e atualizados para a nova versão.
2. Certifique-se de que suas configurações foram salvas, caso contrário, não será possível iniciar o serviço do IBM Cognos.
3. No menu **Ações**, clique em **Testar**.

   O IBM Cognos Configuration verifica a disponibilidade da chave simétrica comum (CSK), testa a configuração do namespace e testa as conexões com o armazenamento de conteúdo e outros recursos.

   Dica: Se **Teste** não estiver disponível para seleção, na janela **Explorer**, clique em **Configuração Local**.
4. Se o teste falhar, configure novamente as propriedades afetadas e faça o teste de novo.

   É possível testar alguns componentes individualmente clicando com o botão direito no componente na área de janela **Explorer** e selecionando **Testar**.

   Não inicie o serviço até que todos os testes estejam livres de erro.
5. No menu **Ações**, clique em **Iniciar**.

   Pode levar alguns minutos para o serviço do IBM Cognos iniciar.

Essa ação inicia todos os serviços instalados que não estão em execução e registra o serviço do IBM Cognos no Windows.

Testar os componentes de serviço de aplicativo

É possível testar a instalação utilizando um navegador web.

Procedimento

1. Abra um navegador da Web.
2. Teste a disponibilidade do dispatcher digitando o valor **URI do dispatcher externo** do IBM Cognos Configuration. Por exemplo,

   `http://host_name:port/bi`

   O valor padrão para *nome_host:porta* é localhost:9300.

   O dispatcher está disponível quando o portal aparece.

Configurando um banco de dados do Cognos Mobile

Por padrão, tabelas do Cognos Mobile são criadas no banco de dados de armazenamento de conteúdo do IBM Cognos Analytics. Se o Cognos Analytics Content Manager e os componentes da camada de aplicativos não estiverem instalados no mesmo local, será possível configurar um banco de dados do Cognos Mobile alternativo.

Para configurar o banco de dados do Cognos Mobile, deve-se primeiramente criar o banco de dados, criar uma conta do usuário sob a qual o banco de dados operará e, em seguida, configurar o Cognos Analytics para usar o banco de dados.

Procedimento

1. Crie um banco de dados usando as mesmas instruções para criação de um banco de dados de armazenamento de conteúdo. Para obter mais informações, consulte "Diretrizes para Criar o Armazenamento de Conteúdo" na página 8.
2. Crie uma conta de usuário, que será usada para operar o banco de dados.
3. No computador no qual os componentes da camada de aplicativos estão instalados, inicie o IBM Cognos Configuration.
4. No **Explorer**, em **Acesso a dados**, clique com o botão direito em **Móvel** e selecione **Novo recurso** > **Banco de dados**.
5. No campo **Tipo**, selecione o tipo de banco de dados.
6. Digite um nome para o banco de dados e clique em **OK**.
7. Na janela **Banco de dados - Propriedades do recurso**, especifique o nome do servidor de banco de dados e número da porta e o ID do usuário e a senha, conforme especificado na etapa 2.
8. No menu **Arquivo**, clique em **Salvar**.

   As credenciais de logon são imediatamente criptografadas.
9. Para testar a conexão com o novo banco de dados, no menu **Ações**, clique em **Testar**.
10. No menu **Ações**, **Inicie** ou **Reinicie** o serviço do **IBM Cognos**.

    As tabelas do Cognos Mobile são criadas automaticamente depois de o serviço do Mobile ser iniciado pela primeira vez.

    Dica: Se as tabelas não forem criadas, talvez porque as credenciais de segurança do Cognos Analytics não permitem isso, elas poderão ser criadas manualmente. Os scripts de criação estão disponíveis no diretório *install_location*`\configuration\schemas\mobile`.

O que Fazer Depois

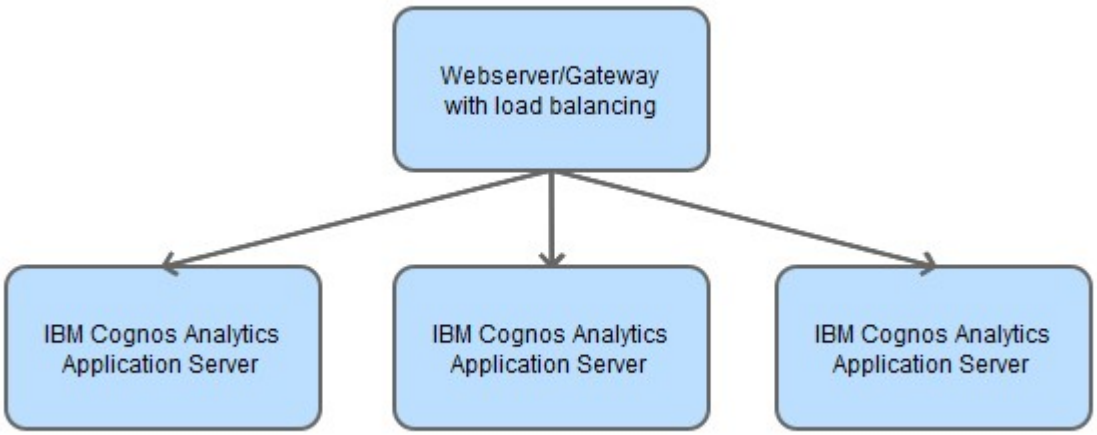
Os usuários podem instalar o aplicativo IBM Cognos Mobile em seus dispositivos móveis para acessar relatórios ou análises do IBM Cognos Analytics. A versão iOS do aplicativo pode ser transferida por download a partir do Apple App Store e a versão Android a partir do Google Play Store.

Capítulo 5. Instalar e configurar o gateway

É possível instalar o gateway opcional em um ou mais computadores. Instale o gateway se você planeja configurar opções avançadas, como conexão única com segurança Kerberos com IIS ou uma arquitetura em que o servidor da web está publicamente disponível fora de um firewall. O IBM Cognos Analytics usa o servidor da web para balanceamento de carga de determinadas solicitações, além de hosting e atendimento de conteúdo estático, como ícones e arquivos de imagem.

Certifique-se de que o computador no qual você instalou os serviços de aplicativos ativos esteja configurado e disponível antes de configurar computadores de gateway.

O diagrama a seguir mostra o servidor gateway e vários servidores Cognos Analytics. Com o balanceamento de carga ativado, a carga de trabalho pode ser distribuída entre os servidores.



Essa configuração também é recomendada em um único ambiente de camada do aplicativo já que o roteamento iria para um servidor e está pronto para incluir servidores de camada adicionais quando necessário.

Realize as seguintes tarefas para instalar e configurar o gateway:

- Instale os componentes de gateway. Consulte “Instalando o gateway do Cognos Analytics” na página 96.
- Configure o IBM Cognos Analytics. Consulte “Configure o Cognos Analytics com o seu servidor da web” na página 96.
- Se o seu servidor da web for o Servidor HTTP Apache ou o Servidor HTTP IBM, execute os procedimentos em “Configurar o Servidor HTTP Apache ou o Servidor HTTP IBM” na página 100.
- Se o seu servidor da web for o Microsoft Internet Information Services, execute os procedimentos em “Configurar o Microsoft Internet Information Services” na página 114.
- Teste a instalação do gateway.

Instalando o gateway do Cognos Analytics

É possível instalar o gateway do IBM Cognos Analytics em um ou mais computadores. Se você tiver um formulário da web, será possível instalar um gateway do IBM Cognos Analytics em cada servidor da web.

Antes de Iniciar

Acesse IBM Software Product Compatibility Reports (www.ibm.com/support/docview.wss?uid=swg27047186) para verificar se as correções necessárias estão instaladas em seu computador.

Assegure-se de que o diretório temporário tenha pelo menos 5 GB de memória.

Dica: O diretório temporário é configurado com a variável de ambiente *IATEMPDIR* para o sistema operacional UNIX ou Linux ou com *TMP* para o sistema operacional Microsoft Windows.

Procedimento

1. Inicie o assistente de instalação.
   a. Para UNIX ou Linux, acesse o diretório do sistema operacional e digite: `./ca_srv_platform_build.bin`

      Dica: Ao usar o comando `ca_srv_<platform>_<build>.bin` com o XWindows, os caracteres japoneses em mensagens e arquivos de log podem ficar corrompidos. Ao instalar em japonês no UNIX ou Linux, primeiro configure as variáveis de ambiente LANG=C e LC_ALL=C (em que C é o código de idioma, por exemplo, ja_JP.PCK no Solaris) e inicie o assistente de instalação.

      Se não estiver usando o XWindows, execute uma instalação não assistida. Para obter mais informações, consulte Capítulo 11, “Instalação, desinstalação e configuração não assistidas”, na página 291.
   b. Para Microsoft Windows, acesse o diretório do sistema operacional ou o local em que os arquivos de instalação foram transferidos por download e dê um clique duplo em `ca_srv_platform_build.exe`.
2. Selecione o idioma para utilizar na instalação.

   Essa seleção determina o idioma da interface com o usuário. Todos os idiomas suportados são instalados. É possível alterar a interface com o usuário para qualquer um dos idiomas instalados depois de concluída a instalação.
3. Selecione a opção de instalação **Customizada** e siga as instruções no assistente de instalação para copiar os arquivos necessários para seu computador.
   - Ao selecionar o diretório, considere o seguinte:

     Instale os componentes de gateway em um diretório que contenha somente caracteres ASCII no nome do caminho. Alguns servidores da web UNIX e Linux não suportam caracteres não ASCII em nomes de diretório.
   - Ao selecionar os componentes, desmarque todos, exceto **Gateway**.
4. Clique em **Concluir**.

Configure o Cognos Analytics com o seu servidor da web

Deve-se configurar seu servidor da web antes que os usuários possam se conectar ao portal do IBM Cognos Analytics.

Para obter relatórios do IBM Cognos Analytics, deve-se também configurar a validade do conteúdo para o diretório de imagens em seu servidor da web, para que o navegador da web não verifique o status da imagem após o primeiro acesso.

Permissões de arquivo

A conta sob a qual o servidor da web é executado deve ter privilégios de leitura, gravação e execução para o local de instalação do Cognos. O acesso de leitura é necessário para o diretório `./configuration` para o arquivo `cogstartup.xml`. O acesso de gravação é necessário para `./logs` se o rastreio de depuração for necessário. O acesso de execução é necessário para o diretório `./cgi-bin` para que os módulos SSO para o Servidor HTTP Apache, o Servidor HTTP IBM ou o Microsoft Internet Information Services possam ser executados pelo servidor da web.

Valores de referência para os procedimentos de configuração

Consulte os seguintes valores quando necessário:

- Nome do servidor: nome do host do servidor da web
- porta #: 80 (não SSL) ou 443 (SSL)
- Nome do diretório virtual: ibmcognos
- Nome do servidor Cognos Analytics: nome do host do servidor IBM Cognos Analytics(n)

  Importante: Se o seu ambiente contiver mais de um servidor Cognos Analytics, não inclua o servidor que executa o Serviço do Content Manager nas etapas abaixo. Inclua apenas os servidores Cognos Analytics que têm os componentes do servidor de aplicativos instalados e configurados.
- Nº da porta do Cognos Analytics: `9300`

Algumas ou todas essas configurações de URI estão no Cognos Configuration, dependendo do tipo de instalação utilizada:

- **URI de gateway**: para não SSL, use `http://`*`web_server_host_name`*`:80/ibmcognos/bi/v1/disp`. Para SSL, use `https://`*`web_server_host_name`*`:443/ibmcognos/bi/v1/disp`

  Esta é a URL para o conteúdo desconectado, como links em PDFs, Excel e relatórios ativos. Ela também é usada em links enviados por e-mail.
- **URIs de dispatcher para o gateway**: `http(s)://`*`IBM_Cognos_Analytics_server_host_name`*`:9300/bi/v1/disp`

  Essa é a lista de URIs os quais o módulo do Cognos Apache ou o código ISAPI se conectam ao encaminhar solicitações. Várias entradas são usadas para failover. Inclua todos os servidores de aplicativos relevantes do IBM Cognos Analytics.
- **URI de dispatcher para aplicativos externos**: `http(s)://`*`IBM_Cognos_Analytics_server_host_name`*`:9300/bi/v1/disp`

  Os aplicativos externos como o Framework Manager se conectam nessa URL para executar operações de SDK.

Microsoft Internet Information Services

Se você deseja configurar a conexão única (SSO), certifique-se de que IsapiModule e WindowsAuthenticationModule estão instalados e ativados.

Instale a extensão de Roteamento de solicitação de aplicativo para o IIS. Para informações sobre como fazer isso, consulte https://www.iis.net/downloads/microsoft/application-request-routing. Isto também instalará a extensão de Regravação de URL.

A regravação de URL permite que os administradores da web criem regras sólidas para implementar URLs que são mais fáceis para os usuários se lembrarem e mais fáceis para os mecanismos de procura encontrarem. O roteamento de solicitação de aplicativo permite que os administradores do servidor da web aumentem a escalabilidade e a confiabilidade do aplicativo da web por meio de roteamento baseado em regra, de afinidade de nome de cliente e de host, de balanceamento de carga de solicitações de servidor HTTP e de armazenamento de disco distribuído em cache.

Se você estiver fazendo upgrade do Cognos Analytics 11.0.3 para o Cognos Analytics 11.0.4 (ou mais recente) e tiver modificado `server.xml` para configurar um caminho `sso/login` que aponta para `/ibmcognos/cgi-bin/cognosisapi.dll`, remova a seguinte entrada de *install_location*`/wlp/usr/servers/cognosserver/server.xml`:

```
<jndiEntry jndiName="glass/sso/login" value="/ibmcognos/cgi-bin/cognosisapi.dll"/>
```

Para obter detalhes sobre a configuração do Active Directory Server, consulte "Ativar a Conexão Única entre o Active Directory Server e os Componentes do IBM Cognos" na página 246

Ativando o gateway da web de 32 bits

Para um servidor da web de 32 bits, deve-se mover manualmente os arquivos de gateway de 32 bits em seu diretório de instalação.

Procedimento

1. Acesse *install_location*`/cgi-bin`.
2. Digite o seguinte comando:
   - Nos sistemas operacionais UNIX ou Linux, digite `./copyGateMod.sh 32bit`
   - Em sistemas operacionais Windows, digite `copyGateMod.bat 32bit`

Resultados

Os arquivos de gateway de 32 bits são copiados do diretório `cgi-bin/lib` para o diretório `cgi-bin`.

Nota: Se você precisar restaurar os arquivos de gateway de 64 bits padrão, siga o procedimento e digite `./copyGateMod.sh 64bit` ou `copyGateMod.bat 64bit`. Os arquivos de gateway de 64 bits são copiados do diretório `cgi-bin/lib64` para o diretório `cgi-bin`.

Configurando URIs do dispatcher

Se instalar o componente de gateway em um computador diferente do Content Manager ou Application Tier Components, configure o computador do gateway para que saiba a localização de um dispatcher. Um dispatcher está instalado em cada computador com o Content Manager e Application Tier Components. Configure o gateway para utilizar o dispatcher em um computador com Application Tier Components.

Para obter proteção de failover, configure mais de um dispatcher para um computador com gateway. Quando vários dispatchers estão configurados, as solicitações são normalmente roteadas para o primeiro dispatcher da lista. Se esse dispatcher tornar-se indisponível, o gateway determinará o próximo dispatcher funcional na lista e fará o roteamento de solicitações para ele. O status do dispatcher principal é monitorado pelo gateway, e as solicitações são roteadas de volta para esse componente quando retorna ao serviço.

Depois de executar as tarefas de configuração exigidas, o computador com gateway pode trabalhar no ambiente.

Antes de Iniciar

Verifique se os computadores onde o Content Manager foi instalado estão configurados e o computador com o Content Manager ativo padrão está disponível antes de configurar computadores com gateway.

Procedimento

1. Inicie o IBM Cognos Configuration.
   a. No Microsoft Windows, clique em **Iniciar** > **IBM Cognos Configuration**.

      Se você estiver usando um computador com Windows 7 ou com Windows 2008 e tiver instalado o produto no diretório `Program Files (x86)`, inicie a Configuração do IBM Cognos como um Administrador.
   b. Nos sistemas operacionais UNIX ou Linux, acesse o diretório *`install_location`*`/bin64` e digite o seguinte comando:

      ```
      ./cogconfig.sh
      ```

      Se o IBM Cognos Configuration não abrir, certifique-se de que você configurou a variável de ambiente *DISPLAY*.

      Se você vir uma mensagem `JAVA.Lang.unsatisfied link`, verifique se está usando uma versão suportada do Java.

      Se você vir uma mensagem `Java.lang.unsupportedClassVersionError`, certifique de que está usando uma versão de 64 bits do Java.
2. Na janela **Explorer**, clique em **Ambiente**.
3. Na janela **Propriedades**, em **Configurações de Gateway**, especifique os valores de **URIs de dispatchers do gateway**:
   - Clique na coluna **Valor**.
   - Clique no botão **Editar**.
   - Mude a parte *localhost* do URI para o nome ou o endereço IP de um computador com Componentes da Camada de Aplicativos.

     Isso garantirá que os usuários em locais diferentes possam se conectar a relatórios e áreas de trabalho enviados por e-mail.

     Dica: Se desejar enviar solicitações para o dispatcher a partir de um aplicativo de kit de desenvolvimento de software ou de uma ferramenta de modelagem do IBM Cognos Analytics que esteja fora de um firewall de rede, conecte-se a um gateway dedicado que esteja configurado para se conectar ao dispatcher usando a URI do dispatcher interno para seu ambiente (por exemplo: http://localhost:9300/p2pd/servlet/dispatch). Por questões de segurança, a configuração padrão da propriedade URI de dispatchers de gateway impede o dispatcher de aceitar solicitações para um aplicativo Software Development Kit ou ferramenta de modelagem que esteja fora do firewall. Certifique-se de configurar a segurança apropriada para esse

gateway dedicado, como SSL (consulte "Configurando o Protocolo SSL para Componentes do IBM Cognos" na página 184). Não altere o gateway principal para utilizar o URI do dispatcher interno. Isso reduzirá a segurança do portal e dos studios do IBM Cognos Analytics.

- Se você deseja incluir outro URI, clique em **Incluir** e mude a parte *localhost* do novo URI para o nome ou o endereço IP de outro computador com Componentes da Camada de Aplicativos.

  Dica: Se quiser usar o dispatcher em um computador do Content Manager em espera, certifique-se de incluí-lo após incluir os computadores dos Componentes da Camada de Aplicativos. Se adicionar o dispatcher do computador com Content Manager ativo, verifique se é o último da lista.
- Depois de especificar todos os URIs, clique em **OK**.

4. Na janela **Explorer**, em **Segurança** > **Criptografia**, clique em **Cognos**, o provedor de criptografia padrão.
5. No grupo de propriedades **Configuração da autoridade de certificação**, defina a propriedade **Senha** para coincidir com as configurações do computador com Content Manager ativo padrão.
6. Certifique-se de que as definições criptográficas coincidam com o que foi definido no computador com Content Manager ativo padrão.
7. Teste para saber se a chave simétrica pode ser recuperada. Na janela **Explorer**, clique com o botão direito em **Criptografia** e clique em **Testar**.

   Os componentes do IBM Cognos Analytics verificam a disponibilidade das chaves simétricas comuns (CSK).
8. No menu **Arquivo**, clique em **Salvar**.

Configurar o Servidor HTTP Apache ou o Servidor HTTP IBM

Esta seção descreve como configurar o Servidor HTTP Apache ou o Servidor HTTP IBM como seu servidor da web no IBM Cognos Analytics.

Configurando o IBM HTTP Server V9 no Cognos Analytics 11.0.10+

11.0.10

É possível usar o servidor da web IBM HTTP Server (IHS) V9 para suportar o balanceamento de carga e o failover entre múltiplos servidores de aplicativos do IBM Cognos Analytics.

Para fazer isso, deve-se instalar o IHS V9 e o Web Server Plug-ins for IBM WebSphere Application Server V9 e, em seguida, configurar o IHS V9 para usar o arquivo `cognos.conf`.

Para obter mais informações sobre como instalar o Web Server Plug-ins for IBM WebSphere Application Server V9, consulte este artigo (www.ibm.com/support/knowledgecenter/en/SSAW57_9.0.0/com.ibm.websphere.installation.nd.doc/ae/rins_plugins_info.html).

Procedimento

1. Instale o IBM Installation Manager (IIM), de preferência a versão 1.8.5 ou mais recente, se você ainda não o instalou.

   É possível fazer download do IIM a partir deste local (www.ibm.com/support/docview.wss?uid=swg24041188).

2. Usando o IIM, instale o IBM HTTP Server (IHS) V9 e o Web Server Plug-ins for IBM WebSphere Application Server V9 a partir de Repositórios on-line do produto para ofertas do Liberty (www.ibm.com/support/knowledgecenter/SSEQTP_liberty/com.ibm.websphere.wlp.nd.multiplatform.doc/ae/cwlp_ins_repositories.html).

   Certifique-se de usar os caminhos de instalação a seguir:

   - `/opt/IHS90` como a raiz de instalação do IHS V9
   - `/opt/IHS90Plugin` como a raiz de instalação do Web Server Plug-ins for IBM WebSphere Application Server

     Não é possível instalar os Plug-ins dentro da raiz de instalação do IHS V9.

3. Associe os WAS Web Server Plug-ins V9 e o IHS V9 executando os comandos a seguir:

   ```
   . cd /opt/IHS90
   . bin/simplepct.sh /opt/IHS90Plugin
   ```

   Dica: No UNIX, verifique o arquivo `httpd.conf` em sua instalação do IHS V9 após executar esse comando. Se `$PLG_ROOT` for exibido, substitua-o pela pasta raiz de instalação do WAS Web Server Plug-ins V9, como `/opt/IHS90Plugin`.

4. Gere o arquivo `plugin-cfg.xml` para o WAS Web Server Plug-ins. Para obter mais informações, consulte "Gerando o plugin-cfg.xml para servidores Cognos Analytics" na página 103.

5. Copie o arquivo `plugin-cfg.xml` que foi gerado na etapa 4 para o diretório *`WAS_Web_Server_Plugins_install_root`*`/config/webserver1`, como `/opt/IHS90Plugin/config/webserver1`.

   Dica: No UNIX, certifique-se de que o arquivo `plugin-cfg.xml` tenha permissões de leitura e de execução após copiar o arquivo.

6. Configure o IHS V9 usando as seguintes etapas:

   a. Acesse o arquivo de modelo `cognos_IHS9_SSO.conf` ou `cognos_IHS9.conf` no diretório *`cognos_analytics_gateway_component_install_location`*`/cgi-bin/templates`.

   b. Copie o arquivo de modelo no diretório *`IHS9_install_root`*`/conf`, como `/opt/IHS90/conf`, e renomeie-o para `cognos.conf`. Modifique o arquivo `cognos.conf` para apontar para o local de instalação apropriado.

   c. Configure o `httpd.conf`, conforme documentado no artigo Configurando o Cognos Analytics com o Servidor HTTP Apache ou o Servidor HTTP IBM.

   d. Reinicie o servidor da web IHS V9.

Configurando o IBM HTTP Server V9 com o SSL

Se você usa o Secure Sockets Layer (SSL) no IBM Cognos Analytics com o IBM HTTP Server V9 como seu servidor da web, deve-se configurar o SSL entre o WAS Web Server Plug-ins e o servidor de aplicativos do Cognos Analytics extraindo o certificado do IBM Cognos e incluindo-o no armazenamento confiável do WAS Web Server Plug-ins.

Se você usa o SSL no IBM HTTP Server V9, configure seu ambiente conforme documentado no artigo "Configurando o Servidor HTTP IBM com SSL" na página 105.

Procedimento

1. Inicie o servidor de aplicativos do IBM Cognos Analytics que está configurado para usar o SSL.

2. Copie a seção Server do arquivo *Cognos_Analytics_applicaton_server_install_root*/wlp/usr/servers/cognosserver/logs/state/plugin-cfg.xml para o arquivo plug-in/config/webserver1/plugin-cfg.xml. Certifique-se de que o ponto de entrada https do Cognos Analytics esteja especificado, conforme mostrado no exemplo a seguir:

```
<Server CloneID="a4949c5e-cb36-40dd-9f43-58702daf7b1a" ConnectTimeout="5"
ExtendedHandshake="false" LoadBalanceWeight="20" MaxConnections="-1"
Name="default_node_cognosserver" ServerIOTimeout="900" WaitForContinue="false">
   <Transport Hostname="hostname" Port="xxx" Protocol="https">
   <Property Name="keyring" Value="D:\install\IBM\WebSphere\Plugins\config\
         webserver1\plugin-key.kdb"/>
   <Property Name="stashfile" Value="D:\install\IBM\WebSphere\Plugins\config\
         webserver1\plugin-key.sth"/>
   </Transport>
</Server>
```

3. No arquivo Plug-in/config/webserver1/plugin-cfg.xml, inclua o atributo a seguir na seção Config:

```
AutoSecurity="false"
```

4. Obtenha o certificado do IBM Cognos usando as seguintes etapas:
   a. Acesse o diretório *applicaton_server_install_root*/bin do Cognos Analytics.
   b. Extraia o certificado digitando um comando que seja apropriado para seu sistema operacional.

      Nos sistemas operacionais UNIX ou Linux, digite

      ```
      ThirdPartyCertificateTool.sh -E -T -r destination file -p NoPassWordSet
      ```

      Nos sistemas operacionais Windows, digite

      ```
      ThirdPartyCertificateTool.bat -E -T -r destination file -p NoPassWordSet
      ```

5. Copie o arquivo .cert, por exemplo, ca-host1.cert, que foi gerado na etapa 4 para o host do WAS Web Server Plug-ins.
6. Inclua o arquivo .cert do Cognos Analytics no keystore do WAS Web Server Plug-ins, plugin-key.kdb. Se o arquivo plugin-key.kdb não existir, crie um conforme descrito na etapa 7.

   É possível usar diferentes métodos para incluir o arquivo .cert no keystore. As etapas a seguir descrevem como fazer isso usando a ferramenta gskcapicmd que é fornecida com o IHS V9.
   a. Acesse a pasta IHS9 ROOT.
   b. Digite um comando apropriado para seu sistema operacional.

      Nos sistemas operacionais UNIX ou Linux, digite

      ```
      bin/gskcapicmd -cert -add -db WAS_Plugin_root/config/webserver1/plugin-key.kdb
      -stashed -label ca-host1 -file ca-host1.cert
      ```

      Nos sistemas operacionais Windows, digite

      ```
      bin\gskcapicmd.bat -cert -add -db WAS_Plugin_root\config\webserver1\plugin-key.kdb
      -stashed -label ca-host1 -file ca-host1.cert
      ```

      Para obter informações sobre outros métodos de inclusão de arquivos de certificado no keystore, procure no IBM Knowledge Center (www.ibm.com/support/knowledgecenter/SSEP7J_11.0.0).
7. Crie um keystore vazio para o WAS Web Server Plug-ins:
   a. Acesse a pasta IHS9 ROOT.
   b. Digite um comando apropriado para seu sistema operacional.

      Nos sistemas operacionais UNIX ou Linux, digite

      ```
      bin/gskcapicmd -keydb -create -db WAS_Plugin_root/config/webserver1
        /plugin-key.kdb -pw xxx -stash
      ```

Nos sistemas operacionais Windows, digite

```
bin\gskcapicmd.bat -keydb -create -db WAS_Plugin_root\config\webserver1
   \plugin-key.kdb -pw xxx -stash
```

Gerando o plugin-cfg.xml para servidores Cognos Analytics

Em um ambiente com o WebSphere Application Server, o arquivo `plugin-cfg.xml` contém informações de configuração que determinam como o plug-in de servidor da web encaminha solicitações.

Dica: O procedimento a seguir não é aplicável aos servidores IBM Cognos Analytics que são usados para executar o serviço do Content Manager.

Procedimento

1. Acesse o local de instalação do servidor de aplicativos do Cognos Analytics.
2. Abra o arquivo *ca_applicaton_server_install_root*`/wlp/usr/servers/cognosserver/server.xml` e inclua a seguinte configuração no arquivo:

   ```
   <pluginConfiguration pluginInstallRoot="WAS_Web_Server_Plugin_install_root"
   webserverPort="IHS9_port"/>
   ```

   Por exemplo:

   ```
   <pluginConfiguration pluginInstallRoot="/opt/IHS90Plugin" webserverPort="8080"/>
   ```

3. Configure e inicie o servidor de aplicativos do Cognos Analytics.

   Depois que o servidor é iniciado, um arquivo denominado `plugin-cfg.xml` é gerado no diretório *applicaton_server_install_root*`/wlp/usr/servers/cognosserver/logs/state` do Cognos Analytics.
4. Abra o arquivo `plugin-cfg.xml` e modifique a seção `UriGroup` excluindo tudo, exceto os dois elementos a seguir:

   ```
   <UriGroup Name="default_host_cognosserver_default_node_Cluster_URIs">
       <Uri AffinityCookie="JSESSIONID" AffinityURLIdentifier="jsessionid"
           Name="/bi/*"/>
       <Uri AffinityCookie="JSESSIONID" AffinityURLIdentifier="jsessionid"
           Name="/bi/v1/*"/>
   </UriGroup>
   ```

   Dica: A segunda entrada de URL não existe no arquivo. É necessário incluí-la.
5. Salve o arquivo `plugin-cfg.xml`.

   Você configurou um servidor de aplicativos do Cognos Analytics para o `ServerCluster`.
6. Para incluir outro servidor de aplicativos do Cognos Analytics no `ServerCluster`, execute as etapas a seguir:
   a. No diretório *application_server_install_root*`/wlp/usr/servers/cognosserver/logs/state` do Cognos Analytics, abra o arquivo `plugin-cfg.xml`. Copie o elemento `Server` na seção `ServerCluster`. Por exemplo, copie o elemento `Server` a seguir:

      ```
      <Server CloneID="081cd7c5-bb6c-4a93-a074-33fa07e587f3" ConnectTimeout="5"
      ExtendedHandshake="false" LoadBalanceWeight="20" MaxConnections="-1"
      Name="default_node_cognosserver" ServerIOTimeout="900" WaitForContinue="false">
      <Transport Hostname="caserverhost" Port="9300" Protocol="http"/>
      </Server>
      ```

   b. Cole o elemento `Server` na seção `ServerCluster` no arquivo `plugin-cfg.xml` que foi gerado na etapa 4. Certifique-se de que o terminal especificado no elemento `Server` esteja acessível a partir do seu host do servidor da web.

c. Mude o nome do servidor modificando o valor do atributo `Name`. Certifique-se de que o nome seja diferente de outros nomes de servidores no `ServerCluster`. Por exemplo, mude o valor de `default_node_cognosserver` para `default_node_cognosserver_1`.

d. Inclua o novo servidor na seção `PrimaryServers`, conforme mostrado abaixo:

```
<PrimaryServers>
    <Server Name="default_node_cognosserver"/>
    <Server Name="default_node_cognosserver_1"/>
</PrimaryServers>
```

e. Salve o arquivo `plugin-cfg.xml`. O novo servidor é incluído no `ServerCluster`.

7. Para incluir mais servidores, repita a etapa 6.

O que Fazer Depois

Para obter mais informações sobre como mesclar o arquivo `plugin-cfg.xml` a partir de múltiplos servidores WebSphere Liberty Profile independentes, consulte este artigo (www.ibm.com/support/knowledgecenter/en/SSAW57_9.0.0/com.ibm.websphere.nd.multiplatform.doc/ae/twsv_merge_configfiles.html).

Configurando o WebDAV no Servidor HTTP IBM ou no Servidor HTTP Apache

Para visualizar e procurar imagens no Relatórios, configure o Web Distributed Authoring and Versioning (WebDAV) no servidor da web. Os autores de relatório podem navegar pelas imagens para incluir nos relatórios de uma maneira semelhante à navegação pelo sistema de arquivos. No Servidor HTTP IBM ou no Servidor HTTP Apache, deve-se incluir diretivas em seu arquivo de configuração do servidor e, em seguida, configurar o acesso de diretório.

Procedimento

1. No diretório *webserver_location*`/conf`, abra o arquivo `httpd.conf` em um editor de texto.
2. Remova o comentário das diretivas que carregam `modules/mod_dav.so` e `modules/mod_dav_fs.so`.

```
LoadModule dav_module modules/mod_dav.so
LoadModule dav_fs_module modules/mod_dav_fs.so
```

3. Forneça um local para a diretiva `DAVLockDB`.

   Por exemplo,

   `DAVLockDB "`*webserver_location*`/var/DavLock"`

   Certifique-se de que o diretório exista.

4. Crie um alias para o diretório no qual as imagens são armazenadas.
5. Inclua `Dav On` nas informações `<Directory>` para o alias.

   Por exemplo,

```
Alias /images "path/shared_images"

<Directory "path/shared_images">
   Dav On
       Options Indexes MultiViews
   AllowOverride None
   Order allow,deny
   Allow from all
</Directory>
```

6. Salve o arquivo.

7. Reinicie o servidor da web.

Resultados

Com o WebDAV ativado, os usuários do Relatórios podem incluir imagens em seus relatórios. Quando os usuários clicam em **Navegar** no navegador de imagens, o local padrão para a navegação é `http://servername/ibmcognos/bi/samples/images`. Se você tiver criado outro local, os usuários podem inserir esse local.

Configurando o Servidor HTTP IBM com SSL

Se estiver usando o Secure Sockets Layer (SSL) no Servidor HTTP IBM, será necessário mudar os valores da **URI do Gateway** no IBM Cognos Configuration para poder acessar o portal.

Para ativar o SSL em seu servidor da web, deve-se obter um certificado do servidor da web assinado por uma Autoridade de Certificação (CA) e instalá-lo em seu servidor da web. Para obter mais informações sobre como usar certificados com o servidor da web, consulte a documentação do servidor da web. Esses certificados não são fornecidos com os produtos IBM Cognos.

Para permitir que os usuários acessem o portal do IBM Cognos usando SSL, será necessário alterar os valores da **URI do Gateway** no IBM Cognos Configuration para cada computador em que os Componentes da camada de aplicativos e o Framework Manager estiverem instalados.

Antes de Iniciar

O Servidor HTTP IBM deve ter o IBM Global Security Kit (GSKit) instalado. Para obter mais informações sobre as versões suportadas do GSKit no Servidor HTTP IBM, consulte Versões do Global Security Kit (GSKit) suportadas para liberações do Servidor HTTP IBM (www.ibm.com/support/docview.wss?rs=177 &context=SSEQTJ&uid=swg21173214) no Portal de Suporte IBM.

Procedimento

1. Em cada computador em que os Componentes da camada de aplicativos ou o Framework Manager estejam instalados, inicie o IBM Cognos Configuration.
2. Em **Configuração Local**, clique em **Ambiente** e altere o valor da **URI do Gateway** de `http` para `https`.
3. No valor do **URI do Gateway**, mude o número da porta para o número da porta SSL definido para seu servidor da web. Por exemplo, o número da porta padrão para conexões SSL é normalmente 443.
4. Em cada computador em que os Componentes da Camada de Aplicativos ou o Framework Manager estão instalados, acesse o diretório *install_location*`/bin` e importe todos os certificados que compõem a cadeia de confiança a fim de iniciar com o certificado de autoridade de certificação raiz no armazenamento confiável do IBM Cognos.

   Importe os certificados digitando o comando a seguir:

   No UNIX ou LINUX, digite

   `ThirdPartyCertificateTool.sh -T -i -r` *path/certificate_fileName* `-p` *password*

   No Windows, digite

   `ThirdPartyCertificateTool.bat -T -i -r` *path\certificate_fileName* `-D` *install_location*`\configuration\certs -p` *password*

Nota: Se a senha não estiver configurada, a senha padrão será NoPassWordSet.

5. Digite o comando a seguir no diretório *ihs_install_root*/bin do servidor da web: *ihs_install_root*/bin/*script_name*

   Em que *ihs_install_root* é o diretório no qual o Servidor HTTP IBM está instalado e *script_name* é gskver.bat para o Microsoft Windows ou gskver.sh para o UNIX ou o Linux. As bibliotecas compartilhadas e as informações de versão do GSKit são exibidas. Verifique se a versão exibida é a versão mínima suportada, conforme mostrado no documento de suporte mencionado na seção *Antes de iniciar* deste procedimento.

6. Inicie o utilitário iKeyman digitando o seguinte comando: *ihs_install_root*/bin/*script_name*

   Em que *ihs_install_root* é o diretório no qual o Servidor HTTP IBM está instalado e *script_name* é ikeyman.bat para o Microsoft Windows ou ikeyman.sh para o UNIX ou o Linux.

7. No menu, selecione **Arquivo do banco de dados de chave** > **Novo**.

8. Insira os seguintes valores e clique em **OK**:

   Nome do arquivo
   Nome do Arquivo do banco de dados de chave. O valor padrão é key.kdb.

   Localização
   Local para armazenar o arquivo key.kdb. O valor padrão é *ihs_install_root*/bin.

9. Na janela Prompt de senha, insira uma senha, marque a caixa de seleção **Armazenar em arquivo stash uma senha para um arquivo** e clique em **OK**. Quando você marca a caixa de seleção **Armazenar uma senha para um arquivo**, a senha é criptografada e salva como um arquivo .sth no mesmo diretório do Arquivo do banco de dados de chave.

   Nota: Para obter informações sobre como criar uma solicitação de certificado para enviar para uma autoridade de certificação, consulte Usando o iKeyman para criar um Arquivo do banco de dados de chave (www.ibm.com/support/docview.wss?rs=177&context=SSEQTJ&uid=swg21006430).
   Uma mensagem de conclusão com êxito é exibida.

10. Abra o arquivo *ihs_install_root*/conf/httpd.conf em um editor de texto.

11. Inclua a diretiva Keyfile com o caminho para o Arquivo do banco de dados de chave. Coloque-a após a seção VirtualHost no arquivo. Por exemplo,

    ```
    <VirtualHost *:443>
    ...
    </VirtualHost>
    KeyFile ihs_install_root/key.kdb
    ```

12. Salve e feche o arquivo httpd.conf.

13. Extraia o certificado do Cognos Analytics para um arquivo. Execute o comando a seguir no servidor IBM Cognos Analytics em *ca_install*/bin.

    script_name -E -T -r *ca_cert_file* -p NoPassWordSet

    Em que *script_name* é ThirdPartyCertificateTool.bat para o Microsoft Windows ou ThirdPartyCertificateTool.sh para o UNIX ou o Linux e *ca_cert_file* é o nome do arquivo de certificado.

14. Copie o arquivo de certificado para *ihs_install_root*/*key_database_file_directory*, em que *ihs_install_root* é o diretório no qual o Servidor HTTP IBM está instalado e *key_database_file_directory* é o diretório no qual o Arquivo do banco de dados de chave está armazenado.

15. Em *ihs_install_root*/bin, digite o seguinte comando:

    ```
    script_name -cert -import -db ca_cert_file
    -pw NoPassWordSet -target key.kdb -target_pw key_database_file_password
    ```

    Em que *script_name* é gskcapicmd.bat para o Microsoft Windows ou gskcapicmd.sh para o UNIX ou o Linux e *key_database_file_password* é a senha para o Arquivo do banco de dados de chave.
16. Inicie o Servidor HTTP IBM. Insira o seguinte comando em ihs_install_root/bin:

    ```
    script_name -k start
    ```

    Em que *script_name* é apchectl.bat para Microsoft Windows ou ./apachectl para UNIX ou Linux. No Microsoft Windows, também é possível iniciar o script como um serviço.
17. Verifique se o Servidor HTTP IBM está em execução inserindo o URI a seguir no campo de endereço de um navegador da web:

    ```
    https://web_server_host_name:port
    ```

    Em que *web_server_host_name* é o nome do host do Servidor HTTP IBM e *port* é o número da porta do Servidor HTTP IBM.
18. Salve sua configuração e reinicie os serviços.

Resultados

Ao acessar o portal usando https://**servername**:443/ibmcognos, você é solicitado a instalar um certificado. Para evitar ser solicitado por um alerta de segurança para cada nova sessão, instale o certificado em um dos armazenamentos de certificados do navegador da web.

Configurando o Servidor HTTP Apache ou o Servidor HTTP IBM no Cognos Analytics 11.0.5+

11.0.5+

Depois de concluir esse procedimento, o servidor pode manipular solicitações para arquivos estáticos (como .js, .html, .css), solicitações de balanceamento de carga para o IBM Cognos Analytics e rotear solicitações de SSO por meio do código de gateway do IBM Cognos Analytics.

Sobre Esta Tarefa

É possível usar um dos arquivos de configuração de amostra que são fornecidos com o IBM Cognos Analytics. Os arquivos de amostra estão em *gateway_component_install_location*/cgi-bin/templates, em que *gateway_component_install_location* é o diretório no qual o componente de gateway está instalado. A tabela a seguir descreve os arquivos de amostra. Escolha o arquivo para o seu ambiente:

Ambiente	Nome do arquivo de amostra
Apache 2.2 não SSO	cognos_apache22_loadbalance.conf
Apache 2.2 SSO	cognos_apache22_loadbalance_SSO.conf
Apache 2.4 não SSO	cognos_apache24_loadbalance.conf
Apache 2.4 SSO	cognos_apache24_loadbalance_SSO.conf
Servidor HTTP IBM 8.5 não SSO	cognos_IHS85_loadbalance.conf
Servidor HTTP IBM 8.5 SSO	cognos_IHS85_loadbalance_SSO.conf

Procedimento

1. Copie o arquivo de configuração de amostra para *apache_or_ihs_install_root*/conf e renomeie-o para cognos.conf.
2. Abra cognos.conf em um editor de texto e mude a diretiva BalancerMember para usar https e um nome completo do domínio. Por exemplo,

```
<Proxy balancer://mycluster>
 BalancerMember https://ica-host1.domain:9300 route=1
 BalancerMember https://ica-host2.domain:9300 route=2
</Proxy>
```

3. Certifique-se de que a seção a seguir esteja presente no arquivo de amostra.

```
# Rewrite Saved-Output and Viewer static references
RewriteRule ^/ibmcognos/bi/rv/(.*)$ /ibmcognos/rv/$1 [PT,L]
```

   Se essa sessão estiver ausente, inclua-a após a seção # Rewrite Event Studio static references.

4. Localize a seção Directory e certifique-se de que ela esteja apontando para o local de instalação do IBM Cognos Analytics.
5. Salve o arquivo cognos.conf.

Configurando o Servidor HTTP Apache ou o Servidor HTTP IBM no Cognos Analytics 11.0.4

11.0.4

Depois de concluir esse procedimento, o servidor pode manipular solicitações para arquivos estáticos (como .js, .html, .css), solicitações de balanceamento de carga para o IBM Cognos Analytics e rotear solicitações de SSO por meio do código de gateway do IBM Cognos Analytics.

Antes de Iniciar

Pelo menos uma instância de um servidor Cognos Analytics deve estar configurada e em execução. Ela deve estar acessível no servidor da web com uma URL semelhante a: http://*host name of the IBM Cognos Analytics server*1:9300/bi. Use mod_proxy_balancer para o balanceamento de carga de solicitações entre diversas instâncias do Cognos Analytics. Para as opções de balanceamento de carga, consulte a documentação do Apache.

Sobre Esta Tarefa

A configuração nesta tarefa configura o balanceamento de carga da sessão adesiva. É possível monitorar e configurar o balanceador de carga em http://*web_server_host_name*/ibmcognos/balancer-manager

O expires_module inclui cabeçalhos de resposta em solicitações que indicam ao navegador quanto tempo ele pode manter o recurso retornado antes de verificar novas versões. O deflate_module executa a compactação dos recursos antes de serem enviados, salvando a largura da banda.

As diferenças por plataformas estão indicadas abaixo com **comentários** . As referências ao cognos_module na configuração abaixo serão necessárias somente se você estiver configurando a conexão única (SSO). Se a SSO não for necessária, você não precisará do cognos_module.

Procedimento

1. No diretório apache/conf, crie um arquivo vazio denominado cognos.conf.
2. Abra o arquivo cognos.conf em um editor de texto.

   O seguinte aplica-se ao Apache 2.2 e ao Cognos Analytics versões 11.0.4 Faça as mudanças no código, como mostram os exemplos a seguir, conforme elas se aplicarem ao seu ambiente. Alguns valores no código são apenas de exemplo. Para obter mais informações sobre as diretivas Apache que podem ser usadas, consulte http://httpd.apache.org/docs/2.2/mod/mod_authnz_ldap.html.

```
# cognos.conf para Apache 2.2 e IHS 8
LoadModule headers_module modules/mod_headers.so
LoadModule rewrite_module modules/mod_rewrite.so
LoadModule expires_module modules/mod_expires.so
LoadModule filter_module modules/mod_filter.so
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_http_module modules/mod_proxy_http.so
LoadModule proxy_balancer_module modules/mod_proxy_balancer.so
LoadModule deflate_module modules/mod_deflate.so

# Apache 2.2 UNIX
 LoadModule cognos_module "/opt/IBM/cognos/analytics/cgi-bin/mod2_2_cognos.so"

# Apache 2.2 Windows
 LoadModule cognos_module "c:/IBM/cognos/analytics/cgi-bin/mod2_2_cognos.dll"

<IfModule mod_expires.c>
    <FilesMatch "\.(jpe?g|png|gif|js|css|json|html|woff2?|template)$">
        ExpiresActive On
        ExpiresDefault "acesso mais 1 dia"
    </FilesMatch>
</IfModule>

 <IfModule mod2_2_cognos.c>
    CGIBinDir "/opt/IBM/cognos/analytics/cgi-bin"
 </IfModule>

<Directory /opt/IBM/cognos/analytics>
    <IfModule mod_deflate>
        AddOutputFilterByType DEFLATE text/
html application/json text/
css application/javascript
    </IfModule>
        Options Indexes MultiViews
    AllowOverride None
    Order allow,deny
    Allow from all
</Directory>

#Configure um cluster para balanceamento de carga
# Include all Cognos Analytics servers that have the Application server components
# installed and configured.
# Important: do not include Cognos Analytics servers that are used to run the
# Content Manager service.
<Proxy balancer://mycluster>
    BalancerMember http://ca-host1:9300 route=1
    BalancerMember http://ca-host2:9300 route=2
    BalancerMember http://ca-host3:9300 route=3
</Proxy>

# UI para monitorar/configurar o balanceador de carga
<Local /ibmcognos/balancer-manager>
    SetHandler balancer-manager
</Local>


# Usar o ScriptAlias se planejar usar o cognos.cgi em vez de mod_cognos para SSO
ScriptAlias /ibmcognos/cgi-bin /opt/IBM/cognos/analytics/cgi-bin
```

```
Alias /ibmcognos /opt/IBM/cognos/analytics/webcontent

RewriteEngine On

# Enviar URL padrão ao serviço
RewriteRule ^/ibmcognos/bi/$ balancer://mycluster/bi/ [P]

# Enviar solicitações de login e UIs anteriores por meio do cognos_module para SSO
RewriteRule ^/ibmcognos/bi/v1/(login|disp)(/.*)?
    /ibmcognos/sso/bi/v1/$1$2 [PT,L]

#Ou Enviar solicitações de login e UIs anteriores por meio do cognos.cgi para SSO
RewriteRule ^/ibmcognos/bi/v1/(login|disp)(/.*)?
    /ibmcognos/bi/v1/disp/bi/v1/$1$2 [PT,L]


# Regravar referências estáticas do Event Studio
RewriteCond %{HTTP_REFERER} v1/disp [NC]
RewriteRule ^/ibmcognos/bi/(ags|cr1|prompting|ccl|common|skins|ps)/(.*)
/ibmcognos/$1/$2 [PT,L]

# Rewrite Saved-Output and Viewer static references
RewriteRule ^/ibmcognos/bi/rv/(.*)$ /ibmcognos/rv/$1 [PT,L]

# Definir a localização do Cognos
<Location /ibmcognos>
    RequestHeader set X-BI-PATH /ibmcognos/bi/v1
</Local>

# Rotear as solicitações de serviço REST CA por meio de proxy com balanceamento de carga
<Location /ibmcognos/bi/v1>
    Header add Set-Cookie "ROUTEID=.%{BALANCER_WORKER_ROUTE}e;
    path=/ibmcognos/bi/v1"
    env=BALANCER_ROUTE_CHANGED
    ProxyPass balancer://mycluster/bi/v1 stickysession=ROUTEID
</Local>

# Rotear login e solicitações de UI anterior por meio do mod_cognos
<Location /ibmcognos/sso>
    SetHandler cognos-handler
    # Incluir Diretivas de SSO aqui; por exemplo...
    AuthType basic
    AuthName "LDAP"
    AuthBasicProvider ldap
    AuthLDAPURL "ldap://ldap:389/ou=people, o=example.com?uid?sub?(objectClass=*)"

    Require valid-user
</Local>


# Este é apenas um exemplo.
# Para obter mais informações sobre as diretivas apache que podem ser usadas,
# consulte http://httpd.apache.org/docs/2.2/mod/mod_authnz_ldap.html
# Rotear login e solicitações de UI anterior por meio do cognos.cgi
<Location /ibmcognos/cgi-bin>
    # Incluir Diretivas de SSO aqui; por exemplo...
    AuthType basic
    AuthName "LDAP"
    AuthBasicProvider ldap
    AuthLDAPURL "ldap://ldap:389/ou=people, o=example.com?uid?sub?(objectClass=*)"

    Require valid-user
</Location>
```

3. Se você estiver utilizando o Servidor HTTP IBM 8.5, mude a linha a seguir em cognos.conf:

```
LoadModule proxy_balancer_module modules/WebSphereCE/mod_proxy_balancer.so
```

4. Salve o arquivo `cognos.conf`.
5. Reinicie o servidor.

Configurando o Servidor HTTP Apache ou o IBM HTTP Server no Cognos Analytics 11.0.3

11.0.0+ 11.0.3

Não é possível usar os módulos Apache com a versão do Apache Server 2.2 que é fornecida com o Red Hat Enterprise Linux versão 5.3 e posterior.

Antes de Iniciar

Este tópico presume que tenha instalado um componente de gateway opcional, que tenha um Servidor HTTP Apache instalado e em execução e que possa administrar ambientes Linux e UNIX.

Ao usar o Servidor HTTP Apache, fique atento aos seguintes recursos que estão disponíveis nas diferentes versões.

Variável	Apache 2.2	Apache 2.4
Balanceamento de Carga	Não suportado	Sim
Módulo Gateway	Sim	Não
Proxy	Sim	Sim

Configure o Apache HTTP Server para aceitar um novo arquivo de configuração que manterá todas as configurações necessárias para o IBM Cognos Analytics.

Apache 2.2

Procedimento

1. Edite o arquivo `cognos.conf` e inclua as seguintes linhas:

```
LoadModule headers_module modules/mod_headers.so
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_http_module modules/mod_proxy_http.so
LoadModule cognos_module "<gateway_location>/cgi-bin/mod2_2_cognos.<xx>"

<Location /<alias>/bi>
RequestHeader set X-BI-PATH /alias/bi/v1
 ProxyPass http(s)://<app_server:port>/bi
 ProxyPassReverse http(s)://<app_server:port>/bi
 ProxyPassReverseCookieDomain "." "<domain>"
</Local>

# Aliases for the CA web content
ScriptAlias /<alias>/cgi-bin "<gateway_location>/cgi-bin"
<Directory "<gateway_location>/cgi-bin">
AllowOverride None
Options None
Order allow,deny
Allow from all
</Directory>

Alias /<alias> "<gateway_location>/webcontent"
<Directory "<gateway_location>/webcontent">
    Options Indexes MultiViews
AllowOverride None
Order allow,deny
Allow from all
```

```
</Directory>

<Location /<alias>/cgi-bin/mod2_2_cognos.<xx>>
       SetHandler cognos-handler
 CGIBinDir "<gateway_location>/cgi-bin/"
       Order allow,deny
       Allow from all
</Location>
```

2. Na seção acima que foi incluída, substitua os itens temporários pelos valores apropriados:
   - *<alias>* - forneça um nome para o alias da web. Por exemplo, `ibmcognos`
   - *<app_server:port>* - especifique o nome e o número da porta de um servidor Cognos Analytics Application. Por exemplo, `appserver.ibm.com:9300`
   - *<domain>* - especifique o domínio no qual os servidores estão localizados. Por exemplo, `ibm.com`
   - *<gateway_location>* - especifique o local físico do Gateway do Cognos Analytics que foi instalado. Por exemplo, `/opt/ibm/cognos/analytics`
   - *<xx>* - forneça o sufixo da extensão dependendo do sistema operacional no qual o Apache está instalado. Por exemplo, `Windows = dll, Unix/Linux = so`
3. Salve o arquivo `cognos.conf`.
4. Se você tiver configurado a conexão única para o IBM Cognos Analytics, chame-a usando a URL a seguir:

```
http://ICA_Web_Server:80/ibmcognos/cgi-bin/mod2_2_cognos.so?
      b_action=xts.run&m=portal/main.xts&m_redirect=/ibmcognos/bi/
```

Apache 2.4

Procedimento

1. Edite o arquivo `cognos.conf` e inclua o seguinte:

```
LoadModule headers_module modules/mod_headers.so
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_http_module modules/mod_proxy_http.so
LoadModule slotmem_plain_module modules/mod_slotmem_plain.so
LoadModule slotmem_shm_module modules/mod_slotmem_shm.so
LoadModule proxy_balancer_module modules/mod_proxy_balancer.so
LoadModule lbmethod_byrequests_module modules/mod_lbmethod_byrequests.so

# Header to add a cookie for sticky sessions
Header add Set-Cookie "ROUTEID=.%{BALANCER_WORKER_ROUTE}e; path=/"
    env=BALANCER_ROUTE_CHANGED

# Send everything which goes to BI Services through balanced proxy
#
# Add/Remove the number of BalanceMember lines depending on the server in your
# environment
<Proxy balancer://mycluster>
 BalancerMember http://<app_server_x:port> route=1
 BalancerMember http://<app_server_x:port> route=2
 ProxySet stickysession=ROUTEID
</Proxy>

<LocationMatch ^/<alias>/bi/(.*)$>
 RequestHeader set X-BI-PATH /<alias>/bi/v1
 ProxyPass balancer://mycluster/bi/$1
 ProxyPassReverseCookieDomain "." "<domain>"
</LocationMatch>
ProxyRequests off

# Aliases for the CA web content
ScriptAlias /<alias>/cgi-bin "<gateway_location>/cgi-bin"
<Directory "<gateway_location>/webcontent/cgi-bin">
```

```
AllowOverride None
Options None
Requerer todos concedidos
</Directory>

Alias /<alias> "<gateway_location>/webcontent"
<Directory "<gateway_location>/webcontent">
    Options Indexes MultiViews
AllowOverride None
Requerer todos concedidos
</Directory>
```

2. Mude os seguintes itens para refletir o ambiente:
   - *<alias>* - forneça um nome para o alias da web. Por exemplo, `ibmcognos`
   - *<app_server_x:port>* - especifique o nome e o número da porta de um servidor de aplicativos do ICA. Por exemplo, `appserver.ibm.com:9300`
   - *<domain>* - especifique o domínio no qual os servidores estão localizados. Por exemplo, `ibm.com`
   - *<gateway_location>* - especifique o local físico em que o Gateway do ICA foi instalado. Por exemplo, `/opt/ibm/cognos/analytics`
3. Para incluir ou remover servidores da camada do aplicativo da configuração de proxy, ajuste o número de linhas `BalancerMember` de forma apropriada na seção `Proxy`.

   Por exemplo, se tiver um servidor de aplicativos, então deverá haver somente uma entrada.

   ```
   <Proxy balancer://mycluster>
    BalancerMember http://app_server_1:port route=1
    ProxySet stickysession=ROUTEID
   </Proxy>
   ```

   Se tiver 4 servidores de aplicativos, então deverá haver 4 entradas.

   ```
   <Proxy balancer://mycluster>
    BalancerMember http://app_server_1:port route=1
    BalancerMember http://app_server_2:port route=2
    BalancerMember http://app_server_3:port route=3
    BalancerMember http://app_server_4:port route=4
    ProxySet stickysession=ROUTEID
   </Proxy>
   ```

   O parâmetro `route=` determina a ordem na qual a solicitação será enviada.
4. Salve o arquivo `cognos.conf`.
5. Reinicie o servidor HTTP Apache.
6. Supondo que a conexão única tenha sido configurada para o IBM Cognos Analytics, a conexão única pode ser chamada com a URL a seguir: `http://ICA_Web_Server:80/ibmcognos/bi/v1/disp?b_action=xts.run&m=portal/main.xts&m_redirect=/ibmcognos/bi/`
7. Como alternativa, se desejar remover a seção de redirecionamento da URL, será possível fazer o seguinte:
   a. Acesse o diretório analytics/webcontent.
   b. Edite o arquivo `default.htm` modificando a seguinte linha.

      Altere `<meta http-equiv="refresh" content="0; URL=/bi">` para `<meta http-equiv="refresh" content="0; URL=/<alias>/bi">`
   c. Salve o `default.htm`
   d. Faça o mesmo com `index.htm`
   e. Teste a conexão usando `http:// ICA_Web_Server:80/ibmcognos/bi/v1/disp` ou `http:// ICA_Web_Server:80/ibmcognos/cgi-bin/mod2_2_cognos.so`

Configurar o Microsoft Internet Information Services

Esta seção descreve como configurar o Microsoft Internet Information Services (IIS) como seu servidor da web no IBM Cognos Analytics.

Configurando o WebDAV no IIS

Para visualizar e procurar imagens no Relatórios, configure o Web Distributed Authoring and Versioning (WebDAV) no servidor da web. Os autores de relatório podem navegar pelas imagens para incluir nos relatórios de uma maneira semelhante à navegação pelo sistema de arquivos. Nos servidores da web Microsoft Internet Information Services (IIS), você deve primeiro ativar o recurso WebDAV e, em seguida, configurar seu servidor da web para acessar o local da imagem.

Procedimento

1. No **Painel de Controle** do Microsoft Windows, clique em **Programas** > **Programas e Recursos**.

   Se estiver usando o Microsoft Windows 8 ou 2012 Server, **Programas e Recursos** está disponível diretamente no **Painel de Controle**.
2. Clique em **Ativar ou desativar recursos**.
3. Se você estiver usando o Microsoft Windows 2008 Server, use as etapas a seguir:
   a. Clique em **Gerenciador de Servidor** > **Funções** > **Servidor da Web (IIS)**.
   b. Na seção **Serviços de Função**, selecione **Incluir Serviços de Função**.
   c. Em **Servidor da Web** > **Recursos HTTP Comuns**, selecione **Publicação WebDAV**.
   d. Clique em **Avançar** e, em seguida, clique em **Instalar**.
4. Se você estiver usando o Microsoft Windows 2012 Server, use as etapas a seguir:
   a. No **Assistente de Incluir Funções e Recursos**, clique em **Instalação baseada em função ou baseada em recurso**, e clique em **Avançar**.
   b. Selecione seu servidor e clique em **Avançar**.
   c. Expanda **Servidor da Web (IIS)** > **Servidor da Web** > **Recursos HTTP Comuns**, e selecione **Publicação WebDAV**.
   d. Clique em **Avançar** > **Avançar**, e depois clique em **Instalar**.
5. Se estiver usando o Microsoft Windows 7 ou 8, use as etapas a seguir:
   a. Expanda **Internet Information Services** > **World Wide Web Services** > **Recursos HTTP Comuns**.
   b. Selecione **Publicação WebDAV** e clique em **OK**.
6. No console **Gerenciador do Internet Information Services (IIS)**, em **Conexões**, selecione seu nome de servidor.
   - Se você estiver usando o Microsoft Windows 2012 Server, no **Gerenciador de Servidor**, selecione **IIS**, e depois dê um clique direito no nome do seu servidor e clique em **Gerenciador do Internet Information Services (IIS)**.
   - Se você estiver usando o Microsoft Windows 2008 Server, no **Gerenciador de Servidor**, expanda **Funções** > **Web Server (IIS)**, e depois clique em **Gerenciador do Internet Information Services (IIS)**.
   - Se você estiver usando o Microsoft Windows 8, no **Painel de Controle**, clique em **Ferramentas Administrativas** para acessar o console do **Gerenciador do Internet Information Services (IIS)**.

- Se você estiver usando o Microsoft Windows 7, no **Painel de Controle**, clique em **Sistema e Segurança** > **Ferramentas Administrativas** para acessar o console do **Gerenciador do Internet Information Services (IIS)**.

7. Em **Conexões**, expanda seu servidor da web, **Sites** e selecione seu website. Por exemplo, selecione **Website Padrão**.
8. Dê um clique duplo em **Autoria WebDAV**.
9. Clique em **Ativar WebDAV**.
10. Clique em **Configurações de WebDAV**.
11. Se você tiver acesso anônimo ativado, selecione **True** para **Permitir Consultas de Propriedade Anônimas** e clique em **Aplicar**.
12. Selecione o diretório ou diretório virtual para o qual deseja permitir acesso ao WebDAV.
13. Dê um clique duplo em **Autoria WebDAV**.
14. Clique em **Incluir Regra de Autoria** e inclua as regras apropriadas para o seu ambiente. Por exemplo, se você instalou as amostras e deseja usar o caminho padrão, no diretório virtual `ibmcognos`, expanda `bi/samples`, selecione `images` e inclua uma regra de criação para os arquivos de imagem.
15. Clique com o botão direito no diretório ou diretório virtual no qual incluiu regras de autoria e clique em **Editar Permissões**.
16. Clique em **Segurança** e inclua as permissões apropriadas. Por exemplo, se você permitir acesso anônimo para seu servidor da web, inclua permissões para o usuário de acesso anônimo. Você pode localizar esse usuário selecionando o website, dando um clique duplo em **Autenticação** e visualizando as propriedades para os usuários exibidos.

Resultados

Com o WebDAV ativado, os usuários do Relatórios podem incluir imagens em seus relatórios. Quando os usuários clicam em **Navegar** no navegador de imagens, o local padrão para a navegação é `http://`*`servername`*`/ibmcognos/bi/samples/images`. Se você tiver criado outro local, os usuários podem inserir esse local.

Configurando o IIS com SSL

Para configurar o Microsoft Internet Information Services (IIS) com Secure Sockets Layer (SSL), você extrai o certificado do IBM Cognos e, em seguida, o inclui no armazenamento confiável no IIS.

Procedimento

1. Acesse o diretório *`install_location`*`/bin`.
2. Extraia os certificados do IBM Cognos digitando o seguinte comando:

   Em sistemas operacionais UNIX ou Linux, digite
   `ThirdPartyCertificateTool.sh -E -T -r destination_file -p NoPassWordSet`

   Em sistemas operacionais Microsoft Windows, digite
   `ThirdPartyCertificateTool.bat -E -T -r destination_file -p NoPassWordSet`
3. Execute Copiando o certificado de autoridade de certificação em servidores IBM Cognos.
4. Importe o certificado para o armazenamento confiável no IIS. Para obter mais informações sobre como importar o certificado para o armazenamento confiável no IIS, consulte Incluindo certificados no armazenamento de autoridade de certificação de raiz confiável de um computador local.

Configurando o IIS no Cognos Analytics 11.0.4 e versões mais recentes

Nota:

Este é um documento em tempo real que será atualizado conforme necessário.

Nota:

O script Automatizado do IIS está disponível aqui.

Este tópico descreve a configuração para o Microsoft Internet Information Services (IIS) para suportar o IBM Cognos Analytics. Quando concluída, o IIS estará configurado para entregar conteúdo estático (como `.js`, `.html`, `.css`) diretamente do IIS enquanto envia REST e outras solicitações do servidor aos servidores backend do Cognos Analytics.

Procedimento

1. Instale a extensão Application Request Routing do IIS.
   a. Instale a extensão de Roteamento de solicitação de aplicativo para o IIS, acessando a seguinte URL: http://www.iis.net/downloads/microsoft/application-request-routing
   b. Ao ser apresentada a Página da Web da Microsoft, clique no botão verde "Instalar esta extensão". Siga as instruções para fazer o download e executar a extensão ARR.
   c. Para garantir que a extensão ARR tenha sido instalada com êxito, ative o IIS Manager no menu **Iniciar\Ferramentas Administrativas** do Windows. Assim que o IIS Manager é ativado, clique no nome do servidor na lateral superior esquerda da tela para exibir os recursos disponíveis. Na área de janela central do IIS, o recurso **Regravação de URL** agora deve estar visível; ele é instalado quando o ARR é instalado.
2. Crie um novo conjunto de aplicativos dedicado. Por exemplo, chamado `CAPool`.
   a. Clique com o botão direito em **Conjuntos de Aplicativos**. Clique em **Incluir Conjuntos de Aplicativos**.
3. Como opção, crie um server farm para fornecer balanceamento de carga e failover para solicitações de serviço do Cognos Analytics. Inclua todos os servidores Cognos Analytics que tiverem os componentes do servidor de aplicativos instalados e configurados.
   a. Clique com o botão direito em **Server Farms** na árvore à esquerda e selecione **Criar Server Farm**.
   b. Nomeie o novo server farm. Por exemplo, `ca_servers`.
   c. Para cada servidor Cognos Analytics, execute as seguintes etapas:
      - Insira o endereço do servidor. Por exemplo, `ca-host1`.
      - Clique em **Configurações avançadas** e expanda **applicationRequestRouting**. Configure o `httpPort` ou o `httpsPort` (se estiver usando HTTPS). Por exemplo, `9300`.
   d. Clique em **Concluir**.
   e. Clique em **Não** quando perguntado se quer permitir que o IIS Manager crie uma regra de regravação.
   f. Selecione o server farm na árvore à esquerda e clique duas vezes em **Afinidade do Servidor**.

g. Selecione a caixa de seleção **Afinidade do Cliente**.
h. Clique em **Aplicar**.
i. Selecione o server farm na árvore à esquerda e clique duas vezes em **Armazenamento em Cache**.
j. Mude **Suporte de Sequência de Consultas** para **Incluir Sequência de Consultas**.
k. Clique em **Aplicar**.
l. Selecione o server farm na árvore à esquerda e clique duas vezes em **Teste de Funcionamento**.
m. Na seção **Teste de URL**, insira a URL: `http://ca_servers/bi/v1/ping`
n. Clique em **Aplicar**.
o. Selecione seu servidor na árvore esquerda e clique duas vezes em **Proxy**.
p. No campo **Tempo limite (segundos)**, mude o valor para `120`.
q. Clique em **Aplicar**.

4. Clique com o botão direito em **Website padrão** e, em seguida, clique em **Incluir aplicativo**.
   - O alias é `ibmcognos`.
   - O conjunto de aplicativos é aquele criado na etapa 1.
   - O caminho físico é *`install_location`*`\webcontent`

   a. Ative a validade do Conteúdo da Web
      1) Selecione `ibmcognos` e dê um clique duplo em **Cabeçalhos de Resposta de HTTP**.
      2) Clique em **Configurar Cabeçalhos Comuns**.
      3) Verifique **Expirar Conteúdo da Web** e configure uma validação que seja melhor para você.
   b. Selecione `ibmcognos` e dê um clique duplo em **Tipos MIME**.

      Importante: Inclua os seguintes tipos MIME em sua configuração do IIS, caso ainda não estejam presentes.
      - `.svg : image/svg+xml`
      - `.woff : application/x-font-woff`
      - `.json : application/json`
      - `.woff2 : font/woff2`
      - `.template : text/html`
      - `.txt : text/plain`

5. Se você estiver configurando a conexão única entre o IIS e o Cognos, clique com o botão direito em `ibmcognos` e clique em **Incluir aplicativo**.
   - **Alias** para `sso`.
   - **Conjunto de aplicativos** é aquele criado na etapa 1.
   - **Caminho físico** é *`install_location`*`\cgi-bin`

   a. Selecione **sso** e dê um clique duplo em **Mapeamentos do manipulador**.
   b. Clique em **Incluir mapeamento de módulo** na área de janela **Ações** à direita.
      - O caminho da solicitação é `cisapi`.
      - O módulo é **IsapiModule**.
      - O executável é `install_location\cgi-bin\cognosisapi.dll`
      - O nome é `Conexão única do Cognos`.

- Clique em **Restrições de solicitação** e certifique-se de que **Chamar o manipulador** esteja desmarcado.
- Dê um clique duplo em **OK**.
- No diálogo **Editar Mapa do Script**, clique em **Sim**.
- Selecione **sso** e clique duas vezes em **Módulos**. Se o WebDAVModule aparecer na lista, remova-o.

6. Crie regras de regravação para mapear solicitações para os manipuladores corretos.
   a. Clique no diretório `bi` em **ibmcognos**.
   b. Clique duas vezes em **Regravação de URL**.
   c. Inclua uma variável do servidor para identificar o local do Cognos Analytics clicando em **Visualizar Variáveis do Servidor**.
      - Clique em **Incluir**.
      - Nomeie a variável como `HTTP_X_BI_PATH`.
      - Clique em **Voltar para regras**.
      - Clique em **Incluir**.
      - Nomeie a variável `HTTP_X_WEBCONTENTROOT`
      - Clique em **Voltar para regras**.
      - Clique em **Incluir**.
      - Nomeie a variável `HTTP_X_FORWARDED_HOST`.
      - Clique em **Voltar para regras**.
   d. Inclua uma regra para passar o local do Cognos Analytics para as máquinas `ca-host` clicando em **Incluir regras** > **Regras de entrada** > **Regra em branco**.
      - O nome é `Cabeçalhos`.
      - O padrão é `(.*)`
      - O tipo de ação é **none**.
      - Expanda **Variáveis do servidor** e
        – Clique em **Incluir**. Selecione `HTTP_X_BI_PATH` e configure o valor para `/ibmcognos/bi/v1`.
        – Clique em **Incluir**. Selecione `HTTP_X_FORWARDED_HOST` e configure o valor para `{HTTP_HOST}`.
        – Clique em **Incluir**. Selecione `HTTP_X_WEBCONTENTROOT` e configure o valor para `/ibmcognos`.
      - Desmarque **Parar processamento de regras subsequentes**.
      - Clique em **Aplicar** e **Voltar para regras**.
   e. Se você configurou o aplicativo SSO em uma etapa anterior, inclua regras para mapear solicitações de login e de serviço da UI anterior para o manipulador de SSO.
      1) Clique em **Incluir regras** > **Regras de entrada** > **Regra em branco**.
         - O nome é `Login de conexão única`.
         - O padrão é `v1/login$`
         - O tipo de ação é **Regravar**.
         - A URL de regravação é `/ibmcognos/sso/cisapi/bi/v1/login`
         - Marque **Parar processamento de regras subsequentes**.
         - Clique em **Aplicar** e **Voltar para regras**.
      2) Clique em **Incluir regras** > **Regras de entrada** > **Regra em branco**.

- O nome é `Conexão única anterior`.
- O padrão é `(v1/disp(/.*)?)`
- O tipo de ação é **Regravar**
- A URL de regravação é `/ibmcognos/sso/cisapi/bi/{R:1}`
- Marque **Parar processamento de regras subsequentes**.
- Clique em **Aplicar** e **Voltar para regras**.

f. Inclua uma regra para mapear as solicitações de serviço REST do Cognos Analytics para os servidores backend do Cognos Analytics.

1) Clique em **Incluir regras** > **Regras de entrada e de saída** > **Proxy reverso** .
   - Se os proxies ainda não estiverem ativados, será solicitado que ative. Clique em **OK**.
   - O nome do servidor é `ca-host:9300/bi`
     ou se você configurou um server farm, `http://ca_servers/bi`

   Selecione a regra recém-criada e clique em **Editar**.
   - O padrão é `(^$)|(^v1(/.*)?)|(^[^/]+\.jsp)`
   - O tipo de ação é **Regravar**.
   - A URL de regravação é `http://ca-host:9300/bi/{R:0}`
     ou se você configurou um server farm, `http://ca_servers/bi/{R:0}`
   - Marque **Parar processamento de regras subsequentes**.
   - Clique em **Aplicar** e **Voltar para regras**.
2) Clique em **Incluir regras** > **Regras de entrada** > **Regra em branco**.
   - O nome é `Event Studio`.
   - O padrão é `^(ags|cr1|prompting|ccl|common|skins|ps)/(.*)`
   - Abra a seção **Condições**.
   - Mude o **Agrupamento local** para **Corresponder qualquer um**
   - Clique em **Incluir**.
     - A **entrada de condição** é `{HTTP_REFERER}`
     - **Verifique se a sequência de entrada** é `Corresponde ao Padrão`
     - O padrão é `v1/disp`
     - Verifique **Ignorar maiúsculas e minúsculas**.
   - Clique em **Incluir**
     - A **entrada de condição** é `{HTTP_REFERER}`
     - **Verifique se a sequência de entrada** é `Corresponde ao Padrão`
     - O padrão é `(ags|cr1|prompting|ccl|common|skins|ps)/(.*)\.css`
     - Verifique **Ignorar maiúsculas e minúsculas**.
   - Clique em **Incluir**.
     - A **entrada de condição** é `{HTTP_REFERER}`
     - **Verifique se a sequência de entrada** é `Corresponde ao Padrão`
     - O padrão é `pat/rsapp.htm`
     - Verifique **Ignorar maiúsculas e minúsculas**.
   - O tipo de ação é **Regravar**
   - A URL de regravação é `/ibmcognos/{R:0}`
   - Marque **Parar processamento de regras subsequentes**.
   - Clique em **Aplicar** e **Voltar para regras**.

3) Clique em **Incluir regras** > **Regras de entrada** > **Regra em branco**
   - O nome é `Visualizador de Relatório`
   - O padrão é `^rv/(.*)`
   - O tipo de ação é **Regravar**
   - A URL de regravação é `/ibmcognos/{R:0}`
   - Marque **Parar processamento de regras subsequentes**.
   - Clique em **Aplicar** e **Voltar para regras**.

7. Ajustar limites de tamanho solicitado.
   a. Selecione o diretório `bi` no aplicativo **ibmcognos** criado anteriormente.
   b. Clique duas vezes em **Filtro de solicitação**.
   c. Clique em **Configurações do recurso de edição...** no painel direito.
      - Configure o **Comprimento máximo de URL (bytes)** para `8192`.
      - Configure a **Sequência máxima de consultas (bytes)** para `8192`.
      - Clique em **OK**.
   d. Clique duas vezes em **Filtro de solicitação**.
   e. Selecione a guia **Cabeçalhos** e clique em **Incluir cabeçalho**.
   f. Na **Xaixa de cabeçalho**, digite o nome do campo de cabeçalho como `Referente`.
   g. Na caixa **Limite de tamanho**, digite `8192`.
   h. Clique em **OK**.
   i. Repita o processo para um nome de campo de cabeçalho chamado `Cookie` com o **Limite de tamanho** de `4096`.
   j. Clique em **OK**.
   k. Clique no diretório virtual **ibmcognos**.
   l. Na visualização **Início**, na seção **Gerenciamento**, clique em **Editor de configuração**.
   m. Na lista suspensa **Seção**, expanda **system.web**e selecione **httpRuntime**.
   n. Configure a propriedade **maxQueryStringLength** para 8192.
   o. Aplique a mudança na configuração.
8. Configure o IIS para permitir que passe por erros 441 customizados que são usados para exceções recuperáveis do CAM. Caso contrário, o IIS pode bloquear esses erros e o cliente vê o erro "Resposta de logon inválida" quando tentar efetuar logon.
   a. Clique no diretório virtual `ibmcognos`.
   b. Na visualização Início, seção **Gerenciamento**, dê um clique duplo em **Editor de configuração**.
   c. Na lista suspensa **Seção**, expanda **system.webServer** e selecione **httpErrors**.
   d. Configure a propriedade **existingResponse** como **PassThrough**.
   e. Aplique a mudança na configuração.
9. Se você configurou o aplicativo SSO em etapas anteriores, ative **Autenticação do Windows**.
   a. Selecione o aplicativo de SSO. Para o navegador Microsoft Edge, selecione o aplicativo `ibmcognos`.
   b. Dê um clique duplo em **Autenticação**. Desative **Autenticação anônima** e ative **Autenticação do Windows**.

   O Cognos Analytics deve agora estar disponível em: `http://iis-host/ibmcognos`.

Nota: Se você configurou uma pasta de diretório virtual de vários níveis acima do aplicativo ibmcognos, ou seja, Website padrão > MyVirtualDirectoryFolder > ibmcognos, use /MyVirtualDirectoryFolder/ibmcognos em vez de /ibmcognos nas regras de reescrita de URL que você criou na etapa 6.

Configurando o IIS no Cognos Analytics 11.0.3

Se você estiver usando um Microsoft Internet Information Services (IIS) versão 7 ou 8, configure o IBM Cognos para usar o gateway ISAPI em vez do gateway CGI padrão. Isso será necessário se você estiver implementando uma conexão única.

Nota: Este tópico é útil nas versões 11.0.0 - 11.0.3 Para obter uma técnica mais simples na versão 11.0.4 consulte "Configurando o IIS no Cognos Analytics 11.0.4 e versões mais recentes" na página 116.

Antes de Iniciar

Você instalou um componente de gateway opcional para o Cognos Analytics.

Sobre Esta Tarefa

Se estiver usando o Microsoft IIS como o servidor da web e planeja executar mais de um produto IBM Cognos Analytics, ou diversas instâncias do mesmo produto, em um computador, deve-se executar uma série de procedimentos:

1. Instale a extensão Application Request Routing (ARR) do IIS.
2. Configure o conjunto de aplicativos do IIS.
3. Configure os diretórios virtuais e o aplicativo do IIS.
4. Configure o ISAPI.
5. Configure o proxy reverso.

Importante: Se você estiver usando a versão de 32 bits do gateway ISAPI, deve ativar o aplicativo de 32 bits para o conjunto de aplicativos usado para o gateway do IBM Cognos. No Internet Information Services (IIS) Manager, selecione o conjunto de aplicativos usado para o IBM Cognos e clique em **Configurações Avançadas**. Altere o valor para **Ativar Aplicativos de 32 Bits** para **True**.

Procedimento

1. Instale a extensão Application Request Routing do IIS.
   a. Instale a extensão de Roteamento de solicitação de aplicativo para o IIS, acessando a seguinte URL: http://www.iis.net/downloads/microsoft/application-request-routing
   b. Ao ser apresentada a Página da Web da Microsoft, clique no botão verde "Instalar esta extensão". Siga as instruções para fazer o download e executar a extensão ARR.
   c. Para garantir que a extensão ARR tenha sido instalada com êxito, ative o IIS Manager no menu **Iniciar\Ferramentas Administrativas** do Windows. Assim que o IIS Manager é ativado, clique no nome do servidor na lateral superior esquerda da tela para exibir os recursos disponíveis. Na área de janela central do IIS, o recurso **Regravação de URL** agora deve estar visível; ele é instalado quando o ARR é instalado.
2. Configure o conjunto de aplicativos do IIS.
   a. Abra o Gerenciador do Internet Information Services clicando em **Iniciar\Ferramentas Administrativas\Gerenciador do Internet Information Services (IIS)**.

b. Expanda no **<nome do servidor>** localizado na página inicial e, então, clique em **Conjuntos de Aplicativos**.

c. Clique em **Incluir Conjunto de Aplicativos...** na área de janela **Ações**.

d. Forneça os detalhes necessários no diálogo **Novo Conjunto de Aplicativos**. No campo **Nome**, forneça um nome como IBM Cognos Analytics para o novo conjunto de aplicativos. Mantenha os campos **Versão do .Net Framework** e **Modo de pipeline gerenciado** como o padrão. Clique em **OK** para criar o conjunto de aplicativos.

3. Configure os diretórios virtuais e o aplicativo do IIS.

   O IIS entrega seus conteúdos a clientes expondo uma árvore de diretórios virtuais. Esse diretório virtual determinará o elemento de caminho (ou alias) a ser usado na URL logo após o nome ou endereço do host do servidor da web. Para este exemplo, o alias será `ibmcognos`. O Aplicativo IIS para `cgi-bin` mapeará os módulos de gateway do IBM Cognos Analytics para o conjunto de aplicativos criado anteriormente.

   a. Na área de janela esquerda do explorador do Gerenciador do IIS, expanda **Sites** e **Website Padrão**.

   b. Clique com o botão direito no **Website Padrão** e selecione **Incluir Diretório Virtual**.

   c. Forneça os detalhes necessários para o diálogo **Incluir Diretório Virtual** e, em seguida, clique em **OK**.

      No campo **Alias**, forneça um nome para o diretório virtual, como `ibmcognos`. O restante desse tópico usará o `ibmcognos` como o nome de diretório virtual.

      No campo **Caminho físico**, especifique o local do subdiretório `webcontent` na instalação de gateway do IBM Cognos Analytics. Se necessário, procure o diretório.

   d. Na área de janela esquerda do Gerenciador do IIS, localize o diretório virtual criado anteriormente.

   e. Clique com o botão direito no diretório virtual e selecione **Incluir Aplicativo...**

   f. Forneça os detalhes necessários no diálogo **Incluir Aplicativo** e, em seguida, clique em **OK**.

      - No campo **Alias**, especifique um valor de `cgi-bin`.
      - No campo **Caminho físico**, especifique o local do subdiretório `cgi-bin` na instalação de gateway do IBM Cognos Analytics. Se necessário, procure o diretório.
      - No campo **Conjunto de aplicativos**, selecione o conjunto de aplicativos criado na etapa 3. Configure o conjunto de aplicativos do IIS clicando no botão **Selecionar...**.

4. Configure o ISAPI.

   O IBM Cognos Analytics oferece duas implementações de módulos de gateway a serem usadas com o IIS: a Interface de Programação de Aplicativos do Servidor da Internet e a Interface Gateway Comum (CGI). Usar o ISAPI com o IIS é considerada a melhor prática devido a seu melhor desempenho e alocação de recurso com o CGI. Esta seção descreve somente a configuração do do módulo ISAPI.

   Há duas etapas para o funcionamento do módulo ISAPI. Primeiro, deve-se configurar um mapeamento de módulo que roteia solicitações que chamam o `cognosisapi.dll` para o executável. Depois, o módulo deve ser incluído como uma extensão permitida para que o IIS não bloqueie sua execução.

a. Selecione o aplicativo **cgi-bin** na árvore **Site da Web Padrão\ibmcognos**, na área de janela esquerda do Gerenciador do IIS, e selecione **Visualização de Recursos** na barra inferior, na área de janela central.

b. Clique duas vezes em **Mapeamentos do Manipulador** na área de janela central. Isso faz com que a lista de mapeamentos do manipulador para este aplicativo seja exibida.

c. Na área de janela superior direita **Ações**, clique em **Incluir Mapeamento do Módulo...** para incluir o mapeamento de ISAPI.

d. Forneça os detalhes necessários para o diálogo **Incluir Mapeamento do Módulo** e, em seguida, clique em **OK**.

   - No campo **Caminho da solicitação**, especifique o valor `cognosisapi.dll`. Esse é um valor obrigatório e não pode ser nenhum outro valor.
   - No campo **Módulo**, selecione **IsapiModule** na lista suspensa.
   - No campo **Executável (opcional)**, especifique o caminho para o `cognosisapi.dll` na instalação do IBM Cognos Gateway. Esse arquivo será *`install_location`*`/cgi-bin`, em que *install_location* refere-se ao diretório de instalação do IBM Cognos BI. Neste exemplo, o diretório seria `D:\Apps\IBM\Cognos\Analytics\cgi-bin`.
   - No campo **Nome**, especifique um nome para este módulo. Por exemplo, `IBMCOGNOS-ISAPI`

e. Quando aparecer o diálogo para confirmar se esta nova extensão ISAPI deve ser permitida, clique em **Sim**.

   De volta à tela Mapeamentos do Manipulador, o manipulador recém-incluído aparecerá na seção **Ativado**. Neste exemplo, o manipulador é denominado `IBMCOGNOS-ISAPI`.

5. Configure o proxy reverso.

   Este procedimento fornece as etapas necessárias para configurar o proxy reverso para permitir que o IIS reescreva as solicitações de gateway e passe-as para a camada do aplicativo. Estas etapas presumem uma arquitetura de dois servidores, na qual o gateway do IBM Cognos Analytics está instalado no e o aplicativo IBM Cognos Analytics está instalado no `Server2_Application`

   a. No servidor `Server1_Gateway`, ative o Gerenciador do IIS e selecione a pasta "**bi**" no diretório virtual `ibmcognos` configurado anteriormente.

   b. Na visualização de recursos, inicie o recurso **Regravação de URL**.

   c. Na área de janela **Ações**, clique em **Incluir Regra(s)** e, em seguida, selecione **Proxy Reverso**. Clique em **OK**.

   d. Na caixa de diálogo **Incluir Regra de Proxy Reverso**, na seção **Regras de Entrada**, preencha o campo **Inserir o nome do servidor ou o endereço IP...** no seguinte formato. `<`*`Server2_Application:Port`*`>/bi`. Por exemplo, `Server2_Application:9300/bi`

   e. Certifique-se de que a caixa de seleção **Ativar Transferência de SSL** esteja marcada e, então, clique em **OK**.

   f. Na página **Regras**, na área de janela **Ação**, clique em **Visualizar Variáveis do Servidor**.

   g. Clique em **Incluir** e inclua no `Server1_Gateway` uma variável chamada `HTTP_X_BI_PATH`. Assim que tiver concluído, clique em **OK** para criar a variável.

   h. Na área de janela **Ações**, clique em **Retornar às Regras**.

   i. Selecione a regra criada anteriormente e na área de janela **Regras de entrada**, à direita, clique em **Editar...**

   j. Expanda a seção **Variáveis do Servidor**.

k. Na seção **Variáveis do Servidor**, clique no botão **Incluir**.
l. No diálogo **Configurar Variável do Servidor**, selecione a variável do servidor **HTTP_X_BI_PATH** e configure o campo **Valor** como `/ibmcognos/bi/v1`
m. Certifique-se de que a caixa de seleção **Substituir valor existente** esteja marcada.
n. Clique em **OK** para salvar e, então, na área de janela **Ação**, clique em **Aplicar**.
o. Na área de janela de ação **Ação**, na parte superior direita, clique em **Retornar às Regras** para concluir a definição da regra.
p. Teste a configuração inserindo o seguinte padrão de URL usando um navegador: `http(s)://<web_server>:<web_server_port>/<alias>/bi/`. Para esse exemplo, a URL seria: `http://Server1_Gateway:80/ibmcognos/bi/`

Resultados

Acessando o Gateway do IBM Cognos Analytics Diretamente

Supondo que a conexão única para o provedor de autenticação do IBM Cognos Analytics tenha sido configurada, é possível chamar a conexão única acessando o ambiente do IBM Cognos Analytics, usando a URL completa para o gateway do ISAP, adotando o seguinte padrão: `HTTP(S)://<web_server>:<web_server_port>/<alias>/cgibin/cognosisapi.dll?b_action=xts.run&m=portal/main.xts&m_redirect=/<alias>/bi/`

Para que a URL seja resolvida corretamente, a Configuração do IBM Cognos no servidor `Server1_Gateway` precisa estar configurada de forma que os URIs do Despachante para a entrada do gateway estejam configurados para apontar para o `servidor Server2_Application`.

Teste a URL completa, inserindo o padrão de URL `HTTP(S)://<web_server>:<web_server_port>/<alias>/cgibin/cognosisapi.dll?b_action=xts.run&m=portal/main.xts&m_redirect=/<alias>/bi/`

Para este exemplo, a URL seria: `http://Server1_Gateway:80/ibmcognos/cgibin/cognosisapi.dll?b_action=xts.run&m=portal/main.xts&m_redirect=/IBMCognos/bi/`

Configurando o gateway de CGI no IIS versão 7 ou 8

Se você estiver usando o Microsoft Internet Information Services (IIS) versão 7 ou mais recente, configure o gateway de CGI. Isso é necessário para conexão única.

O gateway de CGI está disponível para servidores da web de 32 bits e de 64 bits.

Sobre Esta Tarefa

Se estiver usando o Microsoft IIS como seu servidor da web e planejar executar mais de um produto IBM Cognos Analytics, ou várias instâncias do mesmo produto, em um computador, crie um conjunto de aplicativos separado para cada produto ou instância e, em seguida, associe os alias desse produto ou instância ao conjunto de aplicativos.

Para obter mais informações sobre como criar um conjunto de aplicativos, consulte sua documentação do servidor da web.

Procedimento

1. No **Painel de Controle** do Microsoft Windows, clique em **Programas** > **Programas e Recursos**.

   Se estiver usando o Microsoft Windows 8 ou 2012 Server, **Programas e Recursos** está disponível diretamente no **Painel de Controle**.
2. Clique em **Ativar ou desativar recursos**.
3. Se você estiver usando o Microsoft Windows 2008 Server, use as etapas a seguir:
   a. Clique em **Gerenciador de Servidor** > **Funções** > **Servidor da Web (IIS)**.
   b. Assegure-se de que o **Common HTTP Features** ou os recursos solicitados estejam ativados.
   c. Se **CGI** estiver configurado como **Não Instalado**, selecione **CGI** e clique em **Incluir Serviço de Função**.
4. Se você estiver usando o Microsoft Windows 2012 Server, use as etapas a seguir:
   a. No Incluir Funções e Assistente de Recursos, clique em **Instalação baseada em função ou baseada em recursos**, e clique em **Avançar**.
   b. Selecione seu servidor e clique em **Avançar**.
   c. Selecione **Servidor da Web (IIS)**, caso ele não esteja instalado ainda, assegure-se de que o **Common HTTP Features** esteja selecionado e clique em **Avançar** até que você chegue à seção **Serviços da Função** do assistente.
   d. Expanda **Desenvolvimento de Aplicativo**.
   e. Selecione **CGI** caso ele não esteja ainda selecionado e clique em **Avançar**.
   f. Clique em **Instalar**.
5. Se estiver usando o Microsoft Windows 7 ou 8, use as etapas a seguir:
   a. Selecione **Internet Information Services** se ainda não estiver selecionado.
   b. Expanda **Internet Information Services** > **World Wide Web Services**.
   c. Assegure-se de que o **Common HTTP Features** ou os recursos solicitados estejam ativados.
   d. Expanda **Recursos de Desenvolvimento de Aplicativo**.
   e. Se **CGI** não estiver selecionado, selecione **CGI**.
   f. Clique em **OK**.
6. No console **Gerenciador do Internet Information Services (IIS)**, em **Conexões**, selecione seu nome de servidor.
   - Se você estiver usando o Microsoft Windows 2012 Server, no **Gerenciador de Servidor**, selecione **IIS**, e depois dê um clique direito no nome do seu servidor e clique em **Gerenciador do Internet Information Services (IIS)**.
   - Se você estiver usando o Microsoft Windows 2008 Server, no **Gerenciador de Servidor**, expanda **Funções** > **Web Server (IIS)**, e depois clique em **Gerenciador do Internet Information Services (IIS)**.
   - Caso esteja usando o Microsoft Windows 8, a partir do **Painel de Controle**, clique em **Ferramentas Administrativas** para acessar o console do **Internet Information Services (IIS) Manager**.
   - Caso esteja usando o Microsoft Windows 7, a partir do **Painel de Controle**, clique em **Sistema e Segurança** > **Ferramentas Administrativas** para acessar o console do **Internet Information Services (IIS) Manager**.
7. Clique duas vezes em **Restrições ISAPI e CGI**.
8. Em **Ações**, clique em **Incluir**.

9. Insira o caminho até o arquivo cognos.cgi. O arquivo está no diretório *install_location*\cgi-bin.

   Você deve inserir o caminho completo, incluindo o nome do arquivo. Se o caminho incluir espaços, certifique-se de usar as aspas ao redor do caminho. Por exemplo, digite:

   "C:\Program Files\ibm\cognos\analytics\cgi-bin\cognos.cgi"

10. Insira uma **Descrição**, tal como CognosCGI.
11. Selecione **Permitir que o caminho de extensão seja executado** e clique em **OK**.
12. Em **Conexões**, expanda **Sites** e em seu website, inclua os diretórios virtuais conforme mostrado na tabela:

Tabela 17. Diretórios Virtuais Necessários

Alias	Localização
ibmcognos	*install_location*/webcontent
ibmcognos/cgi-bin	*install_location*/cgi-bin

Importante: O bi é o valor padrão usado nos valores **URI do Gateway** e **URI do Controlador para o gateway** no IBM Cognos Configuration. Se você não usar o bi para os valores de Alias, certifique-se de ter mudado para os valores **URI do Gateway** e **URI do Controlador para gateway** para corresponder aos valores que são utilizados.

13. Selecione o diretório virtual cgi-bin que você criou.
14. Clique duas vezes em **Mapeamentos do Manipulador**.
15. Em **Ações**, clique em **Incluir Mapeamento de Módulo**.
    a. Em **Caminho de Solicitação**, digitecognos.cgi.
    b. Em **Módulo**, selecione CgiModule.
    c. Deixe **Executável (opcional)** em branco.
    d. Em **Nome**, insira um nome para a entrada, tal como CognosCGI.
    e. Clique em **OK**.
16. Configure o proxy reverso.

    Este procedimento fornece as etapas necessárias para configurar o proxy reverso para permitir que o IIS reescreva as solicitações de gateway e passe-as para a camada do aplicativo. Essas etapas assumem uma arquitetura de dois servidores em que o gateway do IBM Cognos Analytics está instalado no Server1_Gateway e o aplicativo IBM Cognos Analytics está instalado no Server2_Application

    a. No servidor Server1_Gateway, ative o Gerenciador do IIS e selecione a pasta "**bi**" no diretório virtual ibmcognos configurado anteriormente.
    b. Na visualização de recursos, inicie o recurso **Regravação de URL**.
    c. Na área de janela **Ações**, clique em **Incluir Regra(s)** e, em seguida, selecione **Proxy Reverso**. Clique em **OK**.
    d. Na caixa de diálogo **Incluir Regra de Proxy Reverso**, na seção **Regras de Entrada**, preencha o campo **Inserir o nome do servidor ou o endereço IP...** no seguinte formato. <*Server2_Application:Port*>/bi. Por exemplo, Server2_Application:9300/bi
    e. Certifique-se de que a caixa de seleção **Ativar Transferência de SSL** esteja marcada e, então, clique em **OK**.

f. Na página **Regras**, na área de janela **Ação**, clique em **Visualizar Variáveis do Servidor**.
g. Clique em **Incluir** e inclua uma variável denominada `HTTP_X_BI_PATH`. Assim que tiver concluído, clique em **OK** para criar a variável.
h. Na área de janela **Ações**, clique em **Retornar às Regras**.
i. Selecione a regra criada anteriormente e na área de janela **Regras de entrada**, à direita, clique em **Editar...**
j. Expanda a seção **Variáveis do Servidor**.
k. Na seção **Variáveis do Servidor**, clique no botão **Incluir**.
l. No diálogo **Configurar Variável do Servidor**, selecione a variável do servidor **HTTP_X_BI_PATH** e configure o campo **Valor** como `/ibmcognos/bi/v1`
m. Certifique-se de que a caixa de seleção **Substituir valor existente** esteja marcada.
n. Clique em **OK** para salvar e, então, na área de janela **Ação**, clique em **Aplicar**.
o. Na área de janela de ação **Ação**, na parte superior direita, clique em **Retornar às Regras** para concluir a definição da regra.
p. Teste a configuração inserindo o seguinte padrão de URL usando um navegador: `http(s)://<web_server>:<web_server_port>/<alias>/bi/`. Para este exemplo, a URL seria: `http://Server1_Gateway:80/ibmcognos/bi/`.

Resultados

Os usuários podem acessar o gateway do CGI inserindo `http://servername/ibmcognos/bi/` em seus navegadores da web.

Testando o gateway

É possível testar a instalação utilizando um navegador da web.

Procedimento

1. Certifique-se de que seu servidor da web esteja em execução.
2. Abra um navegador web.
3. No campo de endereço, digite o **URI de gateway** do IBM Cognos Configuration. Por exemplo,

   `http://host_name:port/ibmcognos`

   A página de **Boas-vindas** do portal do IBM Cognos Analytics aparecerá.

Capítulo 6. Instalar e configurar componentes de modelagem opcionais

Depois de instalar e configurar os componentes do servidor do IBM Cognos Analytics, será possível instalar e configurar o IBM Cognos Framework Manager, o componente de modelagem para relatório e o IBM Cognos Transformer, a ferramenta de modelagem para criar PowerCubes.

Instale o Framework Manager e o Transformer em um local diferente do Cognos Analytics.

IBM Cognos Framework Manager

O IBM Cognos Framework Manager é a ferramenta de modelagem de metadados para o IBM Cognos Analytics.

É possível instalá-lo no mesmo computador que outros componentes do IBM Cognos Analytics ou em um computador diferente.

Se tiver atualizado de uma versão anterior do Framework Manager, utilize os mesmos modelos e projetos que utilizou com a versão anterior. Para atualizar projetos existentes, abra-os na nova versão do Framework Manager.

Se estiver fazendo upgrade do Framework Manager a partir de uma versão anterior, deve-se primeiramente desinstalar a versão anterior do Framework Manager. Para obter mais informações, consulte Capítulo 12, “Desinstalando o IBM Cognos Analytics”, na página 299.

Antes de instalar o Framework Manager, feche todos os programas que estão atualmente em execução para garantir que os programas de instalação copiem todos os arquivos necessários para seu computador.

Além disso, certifique-se de ter privilégios de administrador para o computador Windows no qual está instalando. Se você não for um administrador, peça ao administrador de seu sistema para incluí-lo no grupo Administrador de seu computador. Privilégios de administrador também são necessários para a conta utilizada para executar o Framework Manager.

Instale e configure todos os componentes do servidor IBM Cognos Analytics antes de instalar o Framework Manager.

Instale em um diretório que contenha somente caracteres ASCII no nome do caminho. Alguns servidores não aceitam caracteres que não sejam ASCII em nomes de diretórios. A instalação do Framework Manager em um diretório que tem um apóstrofo no nome do caminho pode fazer com que a ajuda não abra corretamente.

Para ajudar a gerenciar, compartilhar e proteger diferentes versões dos metadados, é possível configurar o Framework Manager para utilizar um sistema de controle de fontes externo. Para obter mais informações, consulte a seção sobre o uso do controle do repositório externo no *Guia do Usuário do IBM Cognos Framework Manager*.

Requisitos do sistema para o IBM Cognos Framework Manager

Antes de instalar o IBM Cognos Framework Manager, certifique-se de que o computador Windows atenda aos requisitos de software e hardware do IBM Cognos Analytics. O tamanho de seus modelos determina os requisitos de hardware, como espaço em disco.

A tabela a seguir lista os requisitos mínimos de hardware e software para executar o Framework Manager.

Tabela 18. Requisito do Sistema para Framework Manager

Exigência	Especificação
Sistema operacional	Windows
RAM	Mínimo: 512 MB Ideal: 1 GB
Espaço em disco	Mínimo: 500 MB de espaço livre na unidade que contém o diretório temporário utilizado pelo IBM Cognos Analytics
Banco de Dados	O software do cliente de banco de dados deve estar instalado no mesmo computador que o Framework Manager se você estiver usando o modo de consulta compatível Configuração da conectividade do banco de dados
Outro	Microsoft Data Access Component (MDAC) 2.6 ou posterior para uso com amostras de produto

Para ajudar a gerenciar, compartilhar e proteger diferentes versões dos metadados, é possível configurar o Framework Manager para utilizar um sistema de controle de fontes externo. Para obter mais informações, consulte a seção sobre a utilização do controle do armazenamento externo no Framework Manager *User Guide*.

Instalando o IBM Cognos Framework Manager

Para obter uma instalação completa do IBM Cognos Analytics, você deve instalar o Cognos Framework Manager em um computador Windows.

O local de instalação deve ser diferente do local de instalação do IBM Cognos Analytics.

Procedimento

1. Acesse o local em que os arquivos de instalação foram transferidos por download e extraídos e dê um clique duplo no arquivo `ca_model_<platform>_<build>.exe`.
2. Selecione o idioma para utilizar na instalação.

   Essa seleção determina o idioma da interface com o usuário. Todos os idiomas suportados são instalados. É possível alterar a interface com o usuário para qualquer um dos idiomas instalados depois de concluída a instalação.
3. Siga as instruções do assistente de instalação e copie os arquivos necessários para seu computador.
4. Proteja o diretório de instalação contra acesso não autorizado.

O que Fazer Depois

Definições padrão são utilizadas para a configuração. É possível alterar essas configurações padrão durante a instalação, ou posteriormente, para melhor adequar ao seu ambiente.

Configurando o IBM Cognos Framework Manager

Deve-se configurar o IBM Cognos Framework Manager para comunicar-se com o IBM Cognos Analytics e com seus componentes.

Antes de Iniciar

Instale e configure o IBM Cognos Analytics antes de configurar o Framework Manager. Deve-se primeiramente instalar e configurar o Content Manager e iniciar o serviço do **IBM Cognos** em pelo menos um computador com Content Manager. Isso garante que o serviço da autoridade de certificação emita um certificado para o computador com o Framework Manager.

Também é necessário configurar as origens de dados que você planeja usar em projetos do Framework Manager.

Sobre Esta Tarefa

Se você instalar o Framework Manager no mesmo computador que o IBM Cognos Analytics (em um diretório diferente), a configuração não é necessária se as seguintes condições se aplicam:

- O servidor da web está configurado para usar os diretórios virtuais padrão.
- Configurações padrão de portas, recursos e criptográficas são usadas.

Quando o Framework Manager é instalado fora do firewall de rede que protege os componentes da camada de aplicativos, podem surgir problemas de comunicação com o dispatcher. Para evitar esses problemas, é possível instalar o Framework Manager com os componentes da camada de aplicativos ou instalar e configurar um gateway que seja dedicado às comunicações do dispatcher do Framework Manager. Para obter mais informações, consulte “Configurando o Framework Manager no Firewall de Rede” na página 132 ou “Configurando o Framework Manager Fora do Firewall de Rede” na página 132.

Procedimento

1. No computador no qual você instalou o Framework Manager, inicie o IBM Cognos Configuration.
2. Na área de janela **Explorer**, clique em **Ambiente**.
3. Especifique valores apropriados para as seguintes configurações:

   URI do gateway
   Padrão: `http://ca_server:port/bi/v1/disp`

   Exemplo: `http://my_ca_server:9300/bi/v1/disp`

   Esse URI sempre deve ser igual à do Cognos Analytics.

   Se a URI contiver **localhost**, substitua **localhost** por um nome completo do host ou endereço IP.

   URI do Dispatcher para Aplicativos Externos
   Padrão: `http://ca_server:port/p2pd/servlet/dispatch`

Exemplo: `http://my_ca_server:9300/p2pd/servlet/dispatch`

Se a URI contiver **localhost**, substitua **localhost** por um nome completo do host ou endereço IP.

4. No menu **Arquivo**, clique em **Salvar**.

Resultados

O Framework Manager é configurado para comunicar-se com o IBM Cognos Analytics.

Configurando o Framework Manager no Firewall de Rede

Use as etapas a seguir para configurar a comunicação entre o Framework Manager e os componentes do IBM Cognos Analytics quando o Framework Manager é instalado dentro de um firewall de rede.

Procedimento

1. No computador no qual você instalou o Framework Manager, inicie o IBM Cognos Configuration.
2. Na janela **Explorer**, clique em **Ambiente**.
3. Na janela **Propriedades**, para o **URI do gateway**, digite o valor apropriado. Use o protocolo HTTPS ou HTTP para selecionar a comunicaçao SSL ou não SMS.
4. Altere a parte do nome do host da **URI do gateway** de localhost para o endereço IP ou o nome do host do computador onde o componente de gateway está instalado.
5. Especifique o valor para o **URI do dispatcher para aplicativos externos** digitando o URI do servidor onde os Application Tier Components estão instalados.

   Esse valor é o mesmo que a propriedade **URI do dispatcher interno** em seu computador com os Componentes da Camada de Aplicativos.
6. Na janela **Explorer**, em **Criptografia**, clique em **Cognos**, o provedor de criptografia padrão.
7. No grupo de propriedades **Configurações da Autoridade de Certificação**, na propriedade **Senha**, digite a mesma senha configurada no computador padrão ativo com Content Manager.
8. No menu **Arquivo**, clique em **Salvar**.

Configurando o Framework Manager Fora do Firewall de Rede

Quando o Framework Manager é instalado fora do firewall de rede, é possível instalar e configurar um gateway que seja dedicado às comunicações com o dispatcher.

Procedimento

1. Configure um gateway dedicado para o Framework Manager.
2. No computador de gateway, abra o IBM Cognos Configuration e mude a propriedade **URIs do dispatcher para o gateway** para o URI que é especificado para o **URI do dispatcher interno** em seu computador de Componentes da camada de aplicativos.
3. No computador do Framework Manager, inicie o IBM Cognos Configuration.
4. Na janela **Explorer**, clique em **Ambiente**.
5. Na janela **Propriedades**, para o **URI do gateway**, digite o valor apropriado para o servidor que você está usando como o gateway dedicado.

- Se seu servidor da web estiver configurado para o gateway ISAPI, substitua `cognos.cgi` por `cognosisapi.dll`.
- Se seu servidor da web estiver configurado para usar os módulos Apache, utilize a seguinte sintaxe:

  `http://host_name:port/ibmcognos/cgi-bin/module_alias`

6. Altere a parte do localhost da **URI do gateway** para o endereço IP ou o nome do host do servidor de gateway dedicado.
7. Para o **URI do dispatcher para aplicativos externos**, digite o URI que é especificado para o **URI do dispatcher interno** no servidor no qual os Componentes da camada de aplicativos estão instalados.
8. Na janela **Explorer**, em **Criptografia**, clique em **Cognos**, o provedor de criptografia padrão.
9. No grupo de propriedades **Configurações da Autoridade de Certificação**, na propriedade **Senha**, digite a mesma senha configurada no computador padrão ativo com Content Manager.
10. No menu **Arquivo**, clique em **Salvar**.

Resultados

O Framework Manager foi configurado para comunicar-se com o IBM Cognos Analytics e com seus componentes.

Configurando variáveis para conexões de origem de dados para o Framework Manager

As ferramentas de modelagem do IBM Cognos Analytics criam e gerenciam metadados. O Framework Manager cria e gerencia metadados para as funções de relatório. Como os metadados são obtidos de origens de dados em ambientes multiplataforma e multilíngue, há vários fatores que devem ser analisados antes de configurar o ambiente de origens de dados para o Framework Manager. Geralmente, isso depende da outra tecnologia utilizada para suas origens de dados ou de importação.

Se você fez upgrade de uma versão anterior do Framework Manager, não será necessário configurar nada no ambiente de origem de dados. É necessário configurar o ambiente de origem de dados somente se o Framework Manager foi instalado em um local diferente da versão anterior.

Usuários que operam em diferentes idiomas podem se conectar a uma origem de dados do MSAS 2005 a partir da mesma instância do IBM Cognos Analytics. Os modeladores devem criar um pacote separado para cada idioma. Os usuários podem executar relatórios em qualquer idioma.

Para obter mais informações sobre conexões de origem de dados, consulte o *Guia de Administração e Segurança* do IBM Cognos.

Certifique-se de que instalou as fontes adequadas para suportar os conjuntos de caracteres e símbolos de moedas que forem utilizados. Para que os símbolos das moedas japonesa e coreana sejam exibidos corretamente, é necessário instalar fontes adicionais do disco Supplementary Languages Documentation.

Execute as seguintes etapas no local em que instalou o Framework Manager.

Procedimento

1. Configure a variável de ambiente para suporte multilíngue:
   - Para Oracle, configure a variável de ambiente **NLS_LANG** (Suporte ao Idioma Nacional) em cada computador no qual o Framework Manager e o servidor IBM Cognos Analytics estão instalados, digitando o seguinte comando:

     ```
     NLS_LANG = language_territory.character_set
     ```

     Os exemplos são:

     ```
     NLS_LANG = AMERICAN_AMERICA.UTF8
     ```

     ```
     NLS_LANG = JAPANESE_JAPAN.UTF8
     ```

     O valor da variável determina o comportamento dependente de código de idioma do IBM Cognos Analytics. Convenções de mensagens de erro, de ordem de classificação, de data, de hora, monetária, numérica e de calendário adaptam-se automaticamente ao idioma e código do idioma nativos.
   - Para o IBM Db2, configure a variável de ambiente **DB2CODEPAGE** para um valor de 1252.

     Para obter mais informações sobre se esta variável de ambiente opcional deve ser usada, consulte a documentação do Db2.

   Nenhuma configuração é necessária para o SAP BW. O SAP suporta apenas uma página de códigos única em sistemas SAP BW que não sejam Unicode.
2. Para Oracle, inclua `$ORACLE_HOME/lib` na sua variável **LD_LIBRARY_PATH**.

   Quando você configurar os caminhos de biblioteca de carregamento, assegure-se de que as bibliotecas Oracle de 32 bits estejam no caminho de procura da biblioteca, que geralmente é o diretório `$ORACLE_HOME/lib` ou o diretório `$ORACLE_HOME/lib32` se você instalou um cliente Oracle de 64 bits.
3. Para SAP BW, configure os seguintes objetos de autorização para que a ferramenta de modelagem possa recuperar metadados.

   Onde os valores padrão são especificados, talvez seja necessário modificar os valores no sistema SAP.
   - **S_RFC**

     Configure o campo **Atividade** para **16**.

     Configure o campo **Nome do RFC a ser protegido** para **SYST, RSOB, SUGU, RFC1, RS_UNIFICATION, RSAB, SDTX, SU_USER**.

     Configure o objeto **Tipo de RFC** para ser campo protegido como **FUGR**.
   - **S_TABU_DIS**

     Configure o campo **Atividade** para **03**.

     Configure o campo **Grupo de Autorização** para **&NC&**.

     Nota: &NC& representa qualquer tabela que não possui um grupo de autorização. Por motivos de segurança, crie um grupo de autorização e designe a tabela **RSHIEDIR** para ele. O novo grupo de autorização restringe o acesso ao usuário apenas para a tabela, que é necessária para a ferramenta de modelagem. Crie o grupo de autorização como uma customização no sistema SAP.
   - **S_USER_GRP**

     Configure o campo **Atividade** para **03, 05**.

     Defina o campo **User group in user master main** com o valor padrão.
   - **S_RS_COMP**

     Defina o campo **Activity** com o valor padrão.

     Configure o campo **Área de Informações** como *Nome Técnico da InfoArea*.

Configure o campo **Cubo de Informações** com o valor: *Nome Técnico do Cubo de Informações*.

Defina o campo **Name (ID) of reporting components** com o valor padrão.

Defina o campo **Type of reporting components** com o valor padrão.

- **S_RS_COMP1**

  Defina o campo **Activity** com o valor padrão.

  Defina o campo **Name (ID) of reporting components** com o valor padrão.

  Defina o campo **Type of reporting components** com o valor padrão.

  Defina o campo **Owner (Person Responsible)** com o valor padrão.

- **S_RS_HIER**

  Configure o campo **Atividade** para **71**.

  Configure o campo **Nome da Hierarquia** como *Nome da Hierarquia*.

  Configure o campo **InfoObject** como *Nome Técnico do InfoObject*.

  Configure o campo **Versão** como *Versão da Hierarquia*.

- **S_RS_ICUBE**

  Configure o campo **Atividade** para **03**.

  Configure o campo **Subobjeto InfoCube** para os valores **DATA** e **DEFINITION**.

  Configure o campo **Área de Informações** como *Nome Técnico da InfoArea*.

  Configure o campo **InfoCube** como *Nome Técnico do InfoCube*.

Para obter mais informações sobre objetos de autorização SAP BW, consulte o Transaction SU03.

Testando a instalação do Framework Manager

É possível testar a configuração iniciando o aplicativo e criando um projeto.

Procedimento

Para iniciar o Framework Manager, no menu **Iniciar**, clique em **Todos os Programas** > **IBM Cognos Framework Manager** > .
No Microsoft Windows 8 ou Windows 2012 Server, dê um clique duplo no ícone **Framework Manager** no painel **Iniciar**.
Pode surgir um aviso para atualização se a versão do esquema do modelo for anterior à versão suportada atualmente.
Se a página **Bem-vindo** do Framework Manager for exibida, a instalação está funcionando.

IBM Cognos Transformer

O IBM Cognos Transformer é a ferramenta de modelagem de metadados para criar PowerCubes para uso com produtos do IBM Cognos.

O Transformer pode ser disponibilizado mais facilmente para especialistas em negócios que querem projetar modelos e construir PowerCubes para uso próprio. Por exemplo, os departamentos de TI podem fornecer a especialistas de negócio ou modeladores do Transformer um programa de instalação baseado na web pode ser transferido de um portal corporativo ou seguro, permitindo a fácil distribuição dos arquivos de instalação.

O Transformer consiste nos componentes a seguir:

- Utilitário do sistema operacional UNIX e Linux para a construção de PowerCubes

- IBM Cognos Transformer Client
  Esse componente deve ser instalado em um computador Windows.

Ambos os componentes devem ser instalados em um local diferente do IBM Cognos Analytics.

Definições padrão são utilizadas para a configuração. Você pode alterar essas configurações padrão se necessário. No entanto, as configurações devem ser iguais às do IBM Cognos Analytics.

Requisitos do sistema para o IBM Cognos Transformer

Antes de instalar o IBM Cognos Transformer, certifique-se de que o computador atenda aos requisitos de software e de hardware. O tamanho dos PowerCubes determina os requisitos de hardware, como espaço em disco.

A tabela a seguir lista os requisito mínimos de hardware e de software para a execução do IBM Cognos Transformer.

Tabela 19. Requisitos do Sistema para Transformer

Exigência	**Especificação**
Sistema operacional	Windows UNIX: Oracle Solaris, IBM AIX Linux
RAM	Mínimo: 512 MB Ideal: 4 GB
Espaço em disco	Mínimo: 500 MB de espaço livre na unidade que contém o diretório temporário
Origem de dados	Software do cliente de banco de dados instalado no mesmo computador do IBM Cognos Transformer Configuração da conectividade do banco de dados
Outro	Microsoft Data Access Component (MDAC) 2.6 ou posterior para uso com amostras de produto

Instalando o IBM Cognos Transformer

Instale o IBM Cognos Transformer se você planeja criar PowerCubes para uso com os produtos do IBM Cognos.

O local de instalação do Transformer deve ser diferente do local de instalação do IBM Cognos Analytics.

Os componentes do servidor do Cognos Analytics devem ser instalados e configurados antes de instalar o Transformer.

O idioma que você seleciona no assistente de instalação determina o idioma da interface com o usuário do assistente de instalação e do IBM Cognos Transformer. Todos os idiomas disponíveis são instalados.

Com um sistema operacional UNIX ou Linux, a instalação do IBM Cognos Transformer não fica completa até você instalar também o IBM Cognos Transformer em um computador com o sistema operacional Microsoft Windows. Todos os componentes são instalados nos dois ambientes e depois é possível usar os recursos e ferramentas adequados a cada ambiente. Por exemplo, o cliente IBM Cognos Transformer fornece uma interface gráfica com o usuário para projetar modelos em computadores Windows. Em seguida, você constrói cubos em seu computador UNIX ou Linux. Os modelos que contêm uma origem de dados IQD não são suportados no Linux.

Instale em um diretório que contenha apenas caracteres ASCII no nome do caminho. Alguns servidores não aceitam caracteres que não sejam ASCII em nomes de diretórios.

Antes de instalar o IBM Cognos Transformer, feche todos os programas que estão atualmente em execução para garantir que o programa de instalação copie todos os arquivos obrigatórios em seu computador.

Se estiver instalando no Windows, certifique-se de ter privilégios de administrador para o computador Windows no qual está instalando. Se você não for um administrador, peça ao administrador de seu sistema para incluí-lo no grupo Administrador de seu computador.

Instalando o IBM Cognos Transformer nos Sistemas Operacionais UNIX ou Linux

Use as seguintes etapas para instalar o IBM Cognos Transformer em sistemas operacionais UNIX ou Linux.

Procedimento

1. Acesse o local em que os arquivos de instalação foram transferidos por download e extraídos.
2. Para iniciar o assistente de instalação, vá para o diretório do sistema operacional e digite

   ```
   ./issetup
   ```
3. Selecione o idioma para utilizar na instalação.

   O idioma que você seleciona no assistente de instalação determina o idioma da interface com o usuário do assistente de instalação e do IBM Cognos Transformer. Todos os idiomas disponíveis são instalados.
4. Siga as instruções do assistente de instalação e copie os arquivos necessários para seu computador.

   Dica: O componente Series 7 IQD Bridge não é suportado em Linux.
5. Na página **Concluir** do assistente de instalação, faça o seguinte:
   - Se desejar ver os arquivos de log, clique em **Visualização** para o arquivo de log adequado.
   - Não inicie o IBM Cognos Configuration agora, porque primeiro você deve assegurar que seu ambiente esteja configurado corretamente.

     Posteriormente, é possível configurar o Transformer usando o IBM Cognos Configuration ao digitar `cogconfig.sh` no diretório *`install_location`*`/bin64`.
   - Clique em **Concluir**.

O que Fazer Depois

Para obter informações sobre a sintaxe para opções da linha de comandos do UNIX que são suportadas pelo IBM Cognos Transformer, consulte o *Guia do IBM Cognos Transformer UNIX Commands* no IBM Cognos Analytics Knowledge Center (www.ibm.com/support/knowledgecenter/SSEP7J_11.0.0/com.ibm.swg.ba.cognos.cbi.doc/welcome.html).

A página do manual do IBM Cognos Transformer está acessível no UNIX digitando `cogtr man` no *`diretório`*`install_location /bin64`.

Instalando o IBM Cognos Transformer em Sistemas Operacionais Windows

Use as seguintes etapas para instalar o IBM Cognos Transformer nos sistemas operacionais Microsoft Windows.

Procedimento

1. Acesse o local em que os arquivos de instalação foram transferidos por download e extraídos e dê um clique duplo em `issetup.ex`.
2. Selecione o idioma para utilizar na instalação.

   O idioma que você seleciona no assistente de instalação determina o idioma da interface com o usuário do assistente de instalação e do IBM Cognos Transformer. Todos os idiomas disponíveis são instalados.
3. Siga as instruções do assistente de instalação e copie os arquivos necessários para seu computador.
4. Na página **Concluir** do assistente de instalação, faça o seguinte:
   - Se desejar ver os arquivos de log, clique em **Visualização** para o arquivo de log adequado.
   - Não inicie o IBM Cognos Configuration agora, porque primeiro você deve assegurar que seu ambiente esteja configurado corretamente.

     É possível iniciar o IBM Cognos Configuration usando o atalho **IBM Cognos Configuration** do menu **Iniciar**.
   - Clique em **Concluir**.

Configurando o IBM Cognos Transformer

Você deve configurar o IBM Cognos Transformer para se comunicar com o IBM Cognos Analytics.

Antes de Iniciar

Instale e configure os componentes do IBM Cognos Analytics antes de configurar o IBM Cognos Transformer. Primeiro você deve instalar e configurar o Content Manager e iniciar o serviço **IBM Cognos** em pelo menos um computador do Content Manager antes de configurar o IBM Cognos Transformer. Isso garante que o serviço de autoridade de certificação emita um certificado para o computador com IBM Cognos Transformer.

Para suportar o uso de origens de dados do IBM Cognos Analytics (incluindo pacotes e relatórios) no Transformer, assegure-se de que o cliente de banco de dados esteja instalado no computador no qual o Transformer está instalado.

Procedimento

1. No computador no qual instalou o IBM Cognos Transformer, inicie o IBM Cognos Configuration.
2. Na área de janela **Explorer**, clique em **Ambiente**.
3. Especifique valores apropriados para as seguintes configurações:

   URI do gateway
   Padrão: `http://ca_server:port/bi/v1/disp`

   Exemplo: `http://my_ca_server:9300/bi/v1/disp`

   Esse URI sempre deve ser igual à do Cognos Analytics.

   Se a URI contiver **localhost**, substitua **localhost** por um nome completo do host ou endereço IP.

   URI do Dispatcher para Aplicativos Externos
   Padrão: `http://ca_server:port/p2pd/servlet/dispatch`

   Exemplo: `http://my_ca_server:9300/p2pd/servlet/dispatch`

   Se a URI contiver **localhost**, substitua **localhost** por um nome completo do host ou endereço IP.
4. No menu **Arquivo**, clique em **Salvar**.

Resultados

O IBM Cognos Transformer é configurado para se comunicar com o IBM Cognos Analytics.

Comunicação entre o Transformer e o Cognos Analytics

Você deve configurar o IBM Cognos Transformer para se comunicar com o IBM Cognos Analytics e seus componentes.

As instruções deste tópico destinam-se ao instalador ou administrador. Se você for o modelador ou especialista de negócios do Transformer que deseja fazer download e utilizar o Transformer, consulte "Implementando IBM Cognos Transformer para Modeladores" na página 145

Se o IBM Cognos Analytics tiver sido instalado em mais de um local, certifique-se de que todos os URIs apontem para a versão correta do IBM Cognos Analytics.

Instalações com um firewall

Quando o Transformer está fora de um firewall de rede que protege os componentes da camada de aplicativos, podem surgir problemas de comunicação com o dispatcher. Para evitar esses problemas, é possível instalar o Transformer na mesma camada de arquitetura que os componentes da camada de aplicativos ou instalar e configurar um gateway que seja dedicado às comunicações do Transformer. Para obter mais informações, consulte "Considerações sobre Firewall" na página 29.

Se você estiver usando um gateway dedicado, o computador de gateway também deverá ser configurado. Para obter mais informações, consulte Capítulo 5, "Instalar e configurar o gateway", na página 95.

Origens de dados e o Transformer

O IBM Cognos Transformer cria e gerencia metadados para PowerCubes. Como metadados são derivados de origens de dados em ambientes multiplataformas ou multilíngues, há várias coisas que você deve considerar ou fazer ao configurar um ambiente de origem de dados para o IBM Cognos Transformer. Geralmente, tudo isso depende da outra tecnologia usada para suas origens de dados ou de importação.

Se os usuários que operam em diferentes idiomas se conectam a uma origem de dados do Microsoft Analysis Services (MSAS) 2000, deve-se criar uma instância separada do IBM Cognos Analytics para cada idioma.

Usuários que operam em diferentes idiomas podem se conectar a uma origem de dados do MSAS 2005 a partir da mesma instância do IBM Cognos Analytics. Os modeladores devem criar um pacote separado para cada idioma. Os usuários podem executar relatórios em qualquer idioma.

Para obter mais informações sobre conexões a origens de dados, consulte o *IBM Cognos AnalyticsGuia de administração e segurança*.

Certifique-se de que instalou as fontes adequadas para suportar os conjuntos de caracteres e símbolos de moedas que forem utilizados. Para que os símbolos das moedas japonesa e coreana sejam exibidos corretamente, é necessário instalar fontes adicionais do disco Supplementary Languages Documentation.

Configurando origens de dados para o Transformer

Use estas etapas para configurar origens de dados do Oracle ou SAP BW para o IBM Cognos Transformer.

Procedimento

1. Configure a variável de ambiente para suporte multilíngue:
   - Para Oracle, configure a variável de ambiente **NLS_LANG** (Suporte ao Idioma Nacional) em cada computador no qual o Framework Manager e o servidor IBM Cognos Analytics estão instalados, digitando o seguinte comando:

     ```
     NLS_LANG = language_territory.character_set
     ```

     Os exemplos são:

     ```
     NLS_LANG = AMERICAN_AMERICA.UTF8
     ```

     ```
     NLS_LANG = JAPANESE_JAPAN.UTF8
     ```

     O valor da variável determina o comportamento dependente de código de idioma do IBM Cognos Analytics. Convenções de mensagens de erro, de ordem de classificação, de data, de hora, monetária, numérica e de calendário adaptam-se automaticamente ao idioma e código do idioma nativos.
   - Para o IBM Db2, configure a variável de ambiente **DB2CODEPAGE** para um valor de 1252.

     Para obter mais informações sobre se esta variável de ambiente opcional deve ser usada, consulte a documentação do Db2.

   Nenhuma configuração é necessária para o SAP BW. O SAP suporta apenas uma página de códigos única em sistemas SAP BW que não sejam Unicode.
2. Para o Oracle, adicione $ORACLE_HOME/lib ao caminho da biblioteca.

   Quando os caminhos de biblioteca de carga forem definidos, certifique-se de que as bibliotecas Oracle de 32 bits estejam no caminho de procura de biblioteca, que geralmente são os diretórios $ORACLE_HOME/lib ou $ORACLE_HOME/lib32, se foi instalado um cliente Oracle de 64 bits.

3. Para SAP BW, configure os seguintes objetos de autorização para que a ferramenta de modelagem possa recuperar metadados.

   Onde os valores padrão são especificados, talvez seja necessário modificar os valores no sistema SAP.

   - **S_RFC**

     Configure o campo **Atividade** para **16**.

     Configure o campo **Nome do RFC a ser protegido** para **SYST, RSOB, SUGU, RFC1, RS_UNIFICATION, RSAB, SDTX, SU_USER**.

     Configure o objeto **Tipo de RFC** para ser campo protegido como **FUGR**.

   - **S_TABU_DIS**

     Configure o campo **Atividade** para **03**.

     Configure o campo **Grupo de Autorização** para **&NC&**.

     Nota: &NC& representa qualquer tabela que não possui um grupo de autorização. Por motivos de segurança, crie um grupo de autorização e designe a tabela **RSHIEDIR** para ele. O novo grupo de autorização restringe o acesso ao usuário apenas para a tabela, que é necessária para a ferramenta de modelagem. Crie o grupo de autorização como uma customização no sistema SAP.

   - **S_USER_GRP**

     Configure o campo **Atividade** para **03, 05**.

     Defina o campo **User group in user master main** com o valor padrão.

   - **S_RS_COMP**

     Defina o campo **Activity** com o valor padrão.

     Configure o campo **Área de Informações** como *Nome Técnico da InfoArea*.

     Configure o campo **Cubo de Informações** com o valor: *Nome Técnico do Cubo de Informações*.

     Defina o campo **Name (ID) of reporting components** com o valor padrão.

     Defina o campo **Type of reporting components** com o valor padrão.

   - **S_RS_COMP1**

     Defina o campo **Activity** com o valor padrão.

     Defina o campo **Name (ID) of reporting components** com o valor padrão.

     Defina o campo **Type of reporting components** com o valor padrão.

     Defina o campo **Owner (Person Responsible)** com o valor padrão.

   - **S_RS_HIER**

     Configure o campo **Atividade** para **71**.

     Configure o campo **Nome da Hierarquia** como *Nome da Hierarquia*.

     Configure o campo **InfoObject** como *Nome Técnico do InfoObject*.

     Configure o campo **Versão** como *Versão da Hierarquia*.

   - **S_RS_ICUBE**

     Configure o campo **Atividade** para **03**.

     Configure o campo **Subobjeto InfoCube** para os valores **DATA** e **DEFINITION**.

     Configure o campo **Área de Informações** como *Nome Técnico da InfoArea*.

     Configure o campo **InfoCube** como *Nome Técnico do InfoCube*.

   Para obter mais informações sobre objetos de autorização SAP BW, consulte o Transaction SU03.

Testando a instalação do Transformer

É possível testar a configuração iniciando o aplicativo e criando um modelo.

Procedimento

Para iniciar o IBM Cognos Transformer, no menu **Iniciar**, acesse os programas e clique em **IBM Cognos Transformer**.
No Microsoft Windows 8 ou Windows 2012 Server, dê um clique duplo no ícone **IBM Cognos Transformer** no painel **Iniciar**.
Para iniciar o IBM Cognos Transformer manualmente, clique duas vezes no arquivo `cogtr.exe` no diretório *install_location*`\bin`.
Se vir a janela **Transformer**, a instalação está funcionando.

Tarefas de Configuração Adicionais para IBM Cognos Transformer

Depois de instalar o Transformer, é possível executar essas tarefas:

- Se quiser usar modelos do Transformer do IBM Cognos Series 7 e quiser continuar usando origens de dados IQD,Inclua origens de dados do IBM Cognos Series 7 no Transformer

Para tornar o Transformer disponível para instalação e uso de modeladores, execute as seguintes tarefas:

- Crie um local de instalação de rede para modeladores do Transformer
- Exporte dados de configuração para modeladores do Transformer
- Implemente IBM Cognos Analytics Transformers para modeladores

Incluindo Origens de Dados do IBM Cognos Series 7 no Transformer

Caso pretenda usar modelos do Transformer e origens de dados do IBM Cognos Series 7, será necessário incluir o local das origens de dados do IBM Cognos Series 7 no arquivo de gateway do Transformer.

As instruções deste tópico destinam-se ao instalador ou administrador. Se você for o modelador ou especialista de negócios do Transformer que deseja fazer download e utilizar o Transformer, consulte "Implementando IBM Cognos Transformer para Modeladores" na página 145

Procedimento

1. Faça logon como administrador.
2. No diretório *install_location*/CS7Gateways/bin, abra o cs7g.ini em um editor de texto.
3. Inclua os locais para as origens de dados do IBM Cognos Series 7 no arquivo.
4. Salve o arquivo.

   As mudanças são aplicadas na próxima vez que abrir o Transformer.

Criação de uma localização de instalação de rede para modeladores do Transformer

Sua empresa pode ter negócios especializados ou usuários de poder que podem criar PowerCubes modelados em uma combinação de origens de dados pessoais e corporativos. Esses usuários podem fazer sua própria análise dos dados para sua linha de negócio ou pequeno grupo de usuários. Um instalador ou administrador

pode fazer o download de um arquivo executável para um local da Web ou LAN no qual modeladores possam executar o arquivo para iniciar o assistente de instalação do IBM Cognos Transformer.

As instruções deste tópico destinam-se ao instalador ou administrador. Se você for o modelador ou especialista de negócios do Transformer que deseja fazer download e utilizar o Transformer, consulte "Implementando IBM Cognos Transformer para Modeladores" na página 145

Antes de Iniciar

Antes de tornar o arquivo de instalação disponível para modeladores do Transformer, outros recursos ou permissões devem ser configurados:

- O software do cliente de banco de dados está instalado, ou disponível para ser instalado pelos modeladores, nos computadores que têm o Transformer e que são usados para acessar origens de dados do IBM Cognos Analytics ou origens de dados IQD do IBM Cognos Series 7.
- Modeladores devem ter privilégios para criar uma origem de dados no IBM Cognos Administration.

  Modeladores não precisam de acesso direto ao IBM Cognos Administration. Eles podem criar e atualizar origens de dados utilizando o ferramentas do Transformer ou de linhas de comandos. É possível fornecer modeladores com uma pasta assegurada no portal no qual publicar pacotes do PowerCube.
- Os modeladores devem ter acesso a uma localização na qual armazenar PowerCubes depois de criá-los.

  Esse local também deve estar acessível para o serviço do IBM Cognos e pode ser um compartilhamento protegido em uma LAN.
- Para criar PowerCubes em um servidor Transformer específico, os modeladores devem ter privilégios de FTP para transferir modelos e executar privilégios para criar cubos nesse servidor.

  Os modeladores podem transferir modelos e executar criações de cubo utilizando scripts. Os modeladores podem também utilizar métodos automatizados para criar PowerCubes. Para obter mais informações, consulte o *Guia de administração e segurança*.

Procedimento

1. Insira o disco para o produto de modelagem do IBM Cognos Transformer.
2. Se a página **Bem-vindo** do assistente de instalação aparecer, saia do assistente.
3. No disco, localize o arquivo C8transformerinstall.exe.
4. Copie o arquivo para uma localização segura na qual os modeladores do Transformer tenham acesso.

Dados de Configuração para Modeladores do Transformer

Se deseja tornar o arquivo de instalação do Transformer disponível para os modeladores do Transformer, os modeladores precisarão das configurações do dispatcher e de criptografia para configurar o Transformer em seu computador local. É possível exportar a configuração de um computador com Transformer para uso com todos os outros computadores com Transformer. Os modeladores podem copiar o arquivo de configuração exportado para seu diretório de instalação do Transformer e, em seguida, executar o comando para configurar o computador do Transformer no modo silencioso.

As instruções deste tópico destinam-se ao instalador ou administrador. Se você for o modelador ou especialista de negócios do Transformer que deseja fazer download e utilizar o Transformer, consulte “Implementando IBM Cognos Transformer para Modeladores” na página 145

Se tiver atualizado o coglocale, cogtr.xml, ou os arquivos cs7g.ini no computador do Transformer, copie esses arquivos para a localização da web ou LAN para que os modeladores do Transformer possam fazer o download deles para seus computadores.

Para exportar a configuração, o computador de origem deve ter os mesmos componentes do IBM Cognos Analytics que os computadores com o modelador do Transformer “Comunicação entre o Transformer e o Cognos Analytics” na página 139.

Exportando a Configuração do Transformer:

Use o IBM Cognos Configuration para exportar a configuração de um computador com o Transformer para usar com todos os outros computadores com o Transformer.

Procedimento

1. No IBM Cognos Configuration, no menu **File**, clique em **Exportar como**.
2. Se desejar exportar a configuração atual para uma pasta diferente, na caixa **Procurar em**, localize e abra a pasta.

   Certifique-se de que a pasta esteja protegida de acesso inadequado ou não autorizado.
3. Na caixa **Nome de arquivo**, digite um nome para o arquivo de configuração.
4. Clique em **Salvar**.
5. Renomeie o arquivo exportado para cogstartup.xml.
6. Copie o arquivo cogstartup.xml exportado do computador de origem para a mesma localização de web e LAN que o arquivo de instalação do Transformer.
7. Se tiver alterado a configuração global no computador de origem, copie o arquivo coglocale.xml do computador de origem para a mesma localização da web ou LAN que o arquivo de instalação do Transformer.

   O local padrão do arquivo coglocale.xml é *install_location*/configuration.

Copiando Arquivos de Configuração Atualizados do Transformer:

Se você atualizou determinados arquivos de configuração, deve-se copiá-los no mesmo local que o arquivo de instalação do Transformer.

Procedimento

1. Se atualizou o cogtr.xml, copie-o do diretório `install_location/configuration` no mesmo local da Web ou da LAN que o arquivo de instalação do Transformer.
2. Se atualizou o arquivo cs7g.ini, copie-o do diretório `install_location/CS7Gateways/bin` no mesmo local da Web ou da LAN do arquivo de instalação do Transformer.

Implementando IBM Cognos Transformer para Modeladores

Se for o especialista em negócio ou modelador do Transformer, implante agora o Transformer para poder criar PowerCubes e publique-os em usuários ou grupos selecionados.

Se não tiver concluído a instalação, siga as etapas para instalar o Transformer. Para configurar o Transformer para que ele possa se comunicar com o dispatcher do IBM Cognos Analytics, siga as etapas para configurar o Transformer.

Para suportar o uso de origens de dados do IBM Cognos Analytics (incluindo pacotes e relatórios) no Transformer, assegure-se de que o cliente de banco de dados esteja instalado no computador do Transformer.

Instalação do Transformer:

Como um especialista em negócios ou modelador do Transformer, use as seguintes etapas para instalar o Transformer a partir de um local da Web ou LAN fornecido pelo administrador.

Procedimento

1. Da localização da web ou LAN que o administrador forneceu, execute o arquivo C8transformerinstall.exe.
2. Siga as instruções do assistente de instalação e copie os arquivos necessários para seu computador.

   Dica: O componente Series 7 IQD Bridge não é suportado em Linux.
3. Na página **Concluir** do assistente, clique em **Concluir**.

O que Fazer Depois

O *Guia de comandos UNIX do IBM Cognos Transformer* fornece a sintaxe para as opções da linha de comandos UNIX que são suportadas pelo Cognos Transformer. É possível acessar esse documento no IBM Cognos Analytics Knowledge Center (www.ibm.com/support/knowledgecenter/SSEP7J_11.0.0).

Configuração do Transformer:

Como um especialista em negócios ou modelador do Transformer, use as seguintes etapas para configurar o Transformer.

Procedimento

1. Vá para a mesma localização da web ou LAN que o arquivo de instalação do Transformer.
2. Se algum arquivo .xml estiver presente, copie-o para o diretório *Transformer_location*\configuration, em que *Transformer_location* é o diretório no qual você instalou o Transformer.
3. Se um arquivo .ini estiver presente, copie-o para o diretório *Transformer_location*\CS7Gateways\bin.
4. Acesse o diretório *Transformer_location*\bin.
5. Digite o comando de configuração:

   ```
   ./cogconfig.bat -s
   ```

O IBM Cognos Configuration aplica as definições de configuração especificadas na cópia local do cogstartup.xml, criptografa credenciais, gera certificados digitais e inicia os serviços do IBM Cognos.

6. Para testar o IBM Cognos Transformer, no menu **Iniciar**, acesse os programas e clique em **IBM Cognos Transformer**.

   Se vir a janela **Transformer**, a instalação está funcionando.

7. Depois que o Transformer estiver instalado e em execução com sucesso, exclua os arquivos de instalação que foram extraídos do arquivo de instalação.

Capítulo 7. Opções de Configuração

Após você instalar e configurar os componentes do IBM Cognos, é possível alterar a configuração do seu ambiente. Inicialmente, as configurações padrão são utilizadas para configurar os componentes. No entanto, é possível alterar as configurações padrão se as condições existentes tornarem as opções padrão inapropriadas, ou para adequar melhor seu ambiente.

Por exemplo, é possível configurar recursos para o IBM Cognos Application Firewall ou especificar a quantidade de recursos usada pelos componentes do IBM Cognos. Além disso, é possível entregar conteúdo do IBM Cognos usando outro portal configurando o Portal Services.

É possível configurar componentes do IBM Cognos para usar outros recursos, como usar um provedor de autenticação e depois ativar a conexão única para a conexão do banco de dados e os usuários.

Se utilizar um esquema de balanceamento de carga no ambiente, será possível alterar as configurações e melhorar o desempenho. Por exemplo, é possível balancear solicitações entre dispatchers alterando sua capacidade de processamento ou definindo um número máximo e mínimo de processos e conexões. Para obter mais informações sobre ajuste de desempenho de servidor, consulte o *Guia de administração e segurança*.

Para todas as instalações de sistema operacional Microsoft Windows e a maioria das instalações do sistema operacional UNIX e Linux, use o IBM Cognos Configuration para fazer suas configurações. Entretanto, se o console anexado ao computador UNIX ou Linux no qual você está instalando os componentes do IBM Cognos não suportar uma interface gráfica com o usuário baseada em Java, será necessário editar manualmente o arquivo `cogstartup.xml` no diretório *`install_location`*`/configuration` e, então, executar o IBM Cognos Configuration no modo silencioso.

Use essas tarefas de configuração opcionais para customizar sua configuração para que os componentes do IBM Cognos se integrem facilmente ao seu ambiente existente.

Alterando a versão do Java usada pelos comonentes do IBM Cognos Analytics

Os componentes do IBM Cognos Analytics precisam de um Java Runtime Environment (JRE) para operar.

É possível alterar a versão do Java em situações nas quais se deseja usar os componentes do IBMCognos Analytics com um servidor de aplicativos que requer uma versão de JRE específica ou quando já se utiliza uma versão de JRE com outros aplicativos. Mude as versões do Java configurando a variável de ambiente JAVA_HOME.

JAVA_HOME

Configure uma variável de ambiente JAVA_HOME se desejar usar o seu próprio Java.

Certifique-se de que a versão do JRE é suportada pelos produtos IBM Cognos.

Em sistemas operacionais Microsoft Windows, se não tiver uma variável JAVA_HOME, os arquivos JRE que são fornecidos com a instalação são usados.

Para verificar se o JRE é suportado, consulte IBM Software Product Compatibility Reports (www.ibm.com/support/docview.wss?uid=swg27047186).

Arquivo de política irrestrita do JCE

Os JREs incluem um arquivo de políticas restrito que limita a determinados algoritmos criptográficos e conjuntos de cifras. Se você precisar de uma gama maior de algoritmos criptográficos e conjuntos de cifras do que a mostrada no IBM Cognos Configuration, é possível fazer o download e instalar o arquivo de políticas irrestritas JCE.

Para o Java que é fornecido pela IBM, o arquivo de políticas JCE irrestrito está disponível no Website da IBM (www14.software.ibm.com/webapp/iwm/web/preLogin.do?source = jcesdk).

Etapas

1. Ativar a configuração do Cognos.
2. Clique em **Arquivo** > **Exportar como...** e exporte a configuração para um arquivo de texto, como `export_cogstartup.xml`, na pasta `configuration`. Sair do Cognos Configuration.
3. Faça backup dos arquivos e pastas a seguir:
   - **Arquivos**
   - *install_location/configuration/cogstartup.xml*
   - *install_location/configuration/caSerial*
   - **Pastas**
   - *install_location/configuration/csk*
   - *install_location/configuration/certs*
4. Remova as pastas e os arquivos de backup, **exceto** a pasta *install_location*`/configuration/certs/mobile`. Remova todos os outros arquivos na pasta *install_location*`/configuration/certs`.
5. Renomeie o arquivo de backup de configuração criado na **etapa 2** para `cogstartup.xml`.
6. Configure a variável de ambiente do sistema JAVA_HOME para o JRE que desejar usar. Certifique-se de que esse JRE tenha bcprov pronto no `jre/lib/ext folder`.
7. Ative o Cognos Configuration, salve a configuração e reinicie o servidor. Como uma alternativa, use a linha de comandos a partir da pasta *install_location*`/bin64` e execute esse comando: `cogconfig.bat -s`.

   Isso gerará novamente as chaves para o novo JRE.

Alteração de definições de configuração padrão

Quando você instala componentes do IBM Cognos, a instalação usa as definições de configuração padrão. Se você tiver alguma razão para não usar esses valores padrão, como uma porta sendo usada por outro processo, use IBM Cognos Configuration para alterar o valor.

Se alterar o valor de uma propriedade, será necessário salvar a configuração e depois reiniciar o serviço do IBM Cognos para aplicar as novas configurações em seu computador.

Para instalações distribuídas, certifique-se de ter configurado todos os computadores nos quais instalou o Content Manager antes de alterar as definições de configuração padrão nos outros computadores com o IBM Cognos. Por exemplo: é possível

- alterar um URI
- gerenciar o grupo de configurações
- gerenciar o servidor de configuração
- definir configurações criptográficas
- configurar componentes do IBM Cognos para usar o IBM Cognos Application Firewall
- configurar propriedades de arquivo temporário
- configurar o gateway para usar um namespace
- ativar e desativar serviços
- configurar fontes
- alterar a fonte padrão para relatórios
- salvar saída de relatório em um sistema de arquivos
- alterar o local dos gráficos de mapa para o Relatórios
- Configuração do banco de dados de notificação.

Depois de mudar o comportamento padrão de componentes do IBM Cognos para melhor se ajustar ao ambiente do IBM Cognos, é possível configurar um provedor de autenticação e instalar e configurar o Framework Manager.

Configurações de porta e de URI

É possível mudar alguns elementos em um URI dependendo de seu ambiente. Um URI do IBM Cognos contém os seguintes elementos:

Informações adicionais sobre portas estão disponíveis no tópico “Revisar as configurações de porta padrão” na página 7

- Para o URI do Content Manager URI, URI do dispatcher para aplicativos externos, ou URI do dispatcher

  ```
  protocol://host_name_or_IP:port/context_root/alias_path
  ```

- Para o URI do gateway ou o URI do conteúdo na web

  ```
  protocol://host_name_or_IP:port/virtual_directory/gateway_application
  ```

  ou

  ```
  protocol://host_name_or_IP:port/context_root/alias_path
  ```

  Importante: Para configurações HTTPS/SSL, certifique-se de usar o nome completo do host para URIs.

Os elementos estão descritos na tabela a seguir:

Tabela 20. Elementos e Descrições da URI do IBM Cognos

Elemento	Descrição
protocolo	Especifica o protocolo usado para solicitar e transmitir informações, Hyper Text Transfer Protocol ou Hyper Text Transfer Protocol (Seguro). **Exemplo:** http ou https
nome ou IP do host	Especifica a identidade do host na rede. É possível usar um endereço IP, um nome de computador ou um nome de domínio totalmente qualificado. Em uma instalação distribuída, é necessário alterar o elemento de localhost de um URI. Em um ambiente misto dos servidores de sistema operacional UNIX e Microsoft Windows, certifique-se de que os nomes de host possam ser resolvidos para os endereços IP por todos os servidores no ambiente. **Exemplo:** localhost ou 192.168.0.1 ou [2001:0db8:0000:0000:0000:148:57ab]:80
porta	Especifica a porta em que o sistema de host ouve pedidos. A porta padrão para os serviços do IBM Cognos Analytics é 9300. A porta padrão para um servidor da web é 80. **Exemplo:** 9300 ou 80
raiz do contexto	Usada pelo servidor de aplicativos para determinar o contexto do aplicativo para que a solicitação possa ser encaminhada para o aplicativo da web correto para processamento. **Exemplo:** p2pd
caminho do alias	Usado pelo servidor de aplicativos para distribuir uma solicitação ao componente padrão em um aplicativo web. O caminho do alias não deve ser modificado ou os componentes do IBM Cognos não funcionarão corretamente. **Exemplo:** servlet/dispatch
diretório virtual	Usado pelo servidor web para mapear um diretório virtual ou alias em um local físico. Por exemplo, no URI do gateway padrão de http://localhost:80/ibmcognos/cgi-bin/cognos.cgi, o diretório virtual é ibmcognos/cgi-bin. **Exemplo:** ibmcognos/
aplicativo do gateway	Especifica o nome do aplicativo gateway do Cognos usado. Por exemplo, se você estiver acessando componentes do IBM Cognos usando uma Interface Gateway Comum (CGI), o aplicativo gateway padrão será cognos.cgi. **Exemplo:** cognos.cgi

Se você estiver usando a colaboração com o IBM Connections, certifique-se de incluir o domínio completo para todas as entradas do nome do host no IBM Cognos Configuration. Por exemplo, se seu computador for nomeado MyComputer e o domínio for **MyCompanyName.com**, para o valor host_name_or_IP, use **MyComputer.MyCompanyName.com**. O domínio deve ser incluído em ordem para o IBM Connections permitir o acesso.

Mudando uma configuração de porta ou de URI

Use o seguinte procedimento para alterar as propriedades de URI no IBM Cognos Configuration.

Procedimento

1. Inicie o IBM Cognos Configuration.
2. Na janela **Explorer**, clique no grupo ou componente apropriado:
   - Para alterar um elemento para o dispatcher, clique em **Ambiente**.
   - Para alterar um elemento do servidor de log local, em **Ambiente**, clique em **Criação de log**.
3. Na janela **Propriedades**, clique na caixa de diálogo **Valor** próxima à propriedade de URI que deseja alterar.
4. Selecione o elemento e digite as novas informações.
   - Para alterar a porta usada pelo dispatcher local, mude o valor da propriedade do URI do dispatcher interno. Você deve alterar os URI de todos os componentes locais devido ao fato da mudança afetar todos os URI baseados no dispatcher local.
   - Se a porta do dispatcher for alterada, verifique se o novo número de porta foi especificado durante a configuração dos computadores remotos que usam este recurso, o Content Manager ou serviços Software Development Kit neste sistema.
   - Para configurações HTTPS/SSL, certifique-se de usar o nome completo do host para URIs.
5. No menu **Arquivo**, clique em **Salvar**.

Mudando a porta de serviço do conjunto de dados no Cognos Analytics 11.0.6 para 11.0.8

A porta de serviço do conjunto de dados do IBM Cognos Analytics é capturada dinamicamente quando o Cognos Analytics é iniciado pela primeira vez.

A porta é armazenada e pode ser referenciada no arquivo *install_location*`/wlp/usr/servers/dataset-service/bootstrap.properties`.

O número da porta é baseado na porta do dispatcher do Cognos Analytics mais 1. Por exemplo, 9300 + 1 = 9301 (padrão).

Após a porta de serviço do conjunto de dados ser designada e armazenada, ela não poderá ser atualizada ou mudada, mesmo se você mudar a porta do dispatcher. No entanto, é possível forçar o serviço do conjunto de dados a capturar novamente a porta ou é possível codificar permanentemente a porta no arquivo `bootstrap.properties` para forçar o serviço de consulta para uma porta específica.

Como a porta de serviço do conjunto de dados é designada quando o Cognos Analytics é iniciado pela primeira vez, é melhor que todos os softwares estejam em execução antes de iniciar o Cognos Analytics. Isso assegura que o serviço do conjunto de dados não selecione uma porta que seja usada por outro produto.

Use as etapas a seguir para forçar o serviço do conjunto de dados a capturar novamente uma porta de modo dinâmico:

1. Pare a instância do Cognos Analytics que deseja atualizar.
2. Abra o arquivo *install_location*/wlp/usr/servers/dataset-service/bootstrap.properties em um editor de texto.
3. Defina a configuração http.port para 0 no caminho a seguir: http.port=0
4. Inicie o Cognos Analytics. O http.port é capturado novamente quando o produto é iniciado.
5. Verifique o arquivo bootstrap.properties para ver o número da porta que foi designado.

Use as etapas a seguir para forçar o serviço do conjunto de dados para uma porta específica:

1. Pare a instância do Cognos Analytics que deseja atualizar.
2. Abra o arquivo *install_location*/wlp/usr/servers/dataset-service/bootstrap.properties em um editor de texto.
3. Defina a configuração http.port para um valor específico. Por exemplo, http.port=9876.
4. Inicie o Cognos Analytics. O http.port é designado quando o produto é iniciado.
5. Verifique o arquivo bootstrap.properties para ver se o número da porta correto foi designado.

Após o Cognos Analytics ser iniciado, verifique se o serviço do conjunto de dados está atendendo no http.port designado usando netstat.

Dica: A partir do Cognos Analytics 11.0.9, a porta de serviço do conjunto de dados pode ser configurada no IBM Cognos Configuration.

Gerenciando o grupo de configurações

11.0.4

O grupo de configurações define um grupo de servidores que compartilham a configuração. Isso é crítico em instalações de multisservidor, de forma que os valores de configuração permaneçam disponíveis e consistentes em todos os nós, mesmo após partições de rede. O host de contato do grupo de configurações é executado na mesma instância que o Content Manager ativo.

Sobre Esta Tarefa

- Em uma instalação **Fácil** e se estiver expandindo a capacidade de um sistema em execução selecionando a opção **Conectar e instalar**, esses valores serão configurados para você.
- Para uma instalação **Customizada Primeiro**, com a máquina configurada como o Content Manager ativo, esses valores serão configurados para você.
- Para uma **Conectar e instalar** Customizada, se você se conectar com êxito ao nó do Content Manager por meio da URL do Cognos Analytics durante a instalação, esses valores serão configurados para você.
- Para uma instalação **Customizada Primeiro**, em que o Content Manager é configurado como uma espera, ou se a validação da URL do gateway falhar durante a instalação mas você escolher continuar, será necessário configurar essas propriedades de acordo com as etapas a seguir.

Procedimento

1. Inicie o Cognos Configuration.
2. Na janela **Explorador**, em **Configuração Local**, clique em **Ambiente**.
3. Clique em **Grupo de configurações**.
4. Para configurar os valores corretos:
   - Se esta for a instalação de servidor do Content Manager ativo, será possível configurar os valores para o servidor local clicando com o botão direito nos nomes da propriedade e, então, clicando em **Reconfigurar no Padrão**.
   - Se esta for a instalação do servidor do Content Manager em espera ou uma instalação da camada do Aplicativo, é necessário configurar os valores.
     a. Clique com o botão direito em **Grupo de configurações**, clique no botão **Recuperar** para ativar a caixa de diálogo **Recuperar servidores de configuração**.

        11.0.6 Se o Content Manager ativo for ativado por SSL, será possível recuperar as propriedades do grupo de configurações **após** a URL do Content Manager e outras propriedades terem sido configuradas e salvas corretamente.

     b. Insira as informações adequadas para acessar o servidor do Content Manager ativo e, então, clique em **OK**.

        ID do Usuário - O ID com privilégios administrativos no servidor.

        Senha - A senha para o ID do Usuário.

        ID de Namespace - O valor pode ser localizado em **Segurança**, no recurso **Autenticação**. Por exemplo, `CognosEx`

        URL do Cognos Analytics - A URL usada para executar o Cognos Analytics. Por exemplo, `http://myserver:9300/bi`
   - Caso não seja possível recuperar os valores usando a opção **Recuperar**, é possível configurar os valores manualmente. Siga a orientação na parte inferior da janela de propriedades para cada uma das propriedades.

     Certifique-se de que as duas portas abaixo de **Configurações do Membro Local** sejam duas portas locais diferentes que não estejam em uso. Se todos os seus aplicativos na máquina estavam em execução durante a instalação, essas portas já deveriam estar configuradas com as portas disponíveis.

     Importante: Essas portas devem ser abertas para o tráfego de entrada e saída.

     – A **Porta de sincronização de membro** é a porta local usada para a comunicação de rede que transfere e sincroniza informações de configuração de um servidor para outro. Todas as instalações precisam ter a capacidade de conversar com o `MutualAuthSSLHttpEndpoint` nas outras instalações. Por exemplo, qualquer firewall entre o aplicativo e a camada de dados precisa estar aberto nessa porta. O httpEndpoint é usado exclusivamente para comunicação interna de uma instância do Cognos Analytics para outra. O padrão é 4300.

     – A **Porta de coordenação de membro** é a porta local usada para a comunicação de rede para coordenação de grupo. Esta porta é usada para descobrir e associar um grupo e para manter uma lista atualizada de membros do grupo de configurações. Na instalação primária do Content Manager, a porta de contato do grupo é a mesma porta. Cada instalação precisa ter a capacidade de conversar com qualquer outra instalação na porta de coordenação do grupo, assim, novamente, qualquer firewall entre camadas da instalação precisa estar aberto para essa porta. O padrão é 5701.

5. Salve a configuração.

Gerenciando o servidor de configuração

11.0.3

O servidor de configuração identifica o servidor que gerencia os valores de configuração. Isso é crítico em instalações de multisservidor, de forma que os valores de configuração permaneçam disponíveis e consistentes em todos os nós, mesmo após partições de rede. O servidor de configuração é executado na mesma instância do Content Manager ativo.

Aplica-se ao 11.0.3 (substituído no 11.0.4 pelo gurpo de configurações).

Sobre Esta Tarefa

Em Instalações Fáceis e, caso você esteja expandindo a capacidade de um sistema em execução selecionando a opção Conectar e Instalar, este valor é configurado para você.

Procedimento

1. Inicie o Cognos Configuration.
2. Na janela **Explorador**, em **Configuração Local**, clique em **Ambiente**.
3. Na janela **Ambiente - Propriedades de Grupo**, role para baixo até a categoria **Outras Configurações de URI** e clique em **Servidor de Configuração**.
4. Para configurar o valor correto:
   - Se esta for a instalação de servidor do Content Manager ativo, será possível configurar o valor para o servidor local clicando com o botão direito e, então, clicando em **Reconfigurar como Padrão**.
   - Se esta for a instalação de servidor do Content Manager em espera, ou uma instalação de camada do Aplicativo, será necessário configurar o valor clicando no ícone de edição  para ativar o diálogo de edição.
     a. No diálogo **Valor - Servidor de Configuração**, clique no botão **Recuperar** para ativar o diálogo **Recuperar Servidores de Configuração**. Insira as informações adequadas para acessar o servidor do Content Manager ativo e, então, clique em **OK**.

        ID do Usuário - O ID com privilégios administrativos no servidor.

        Senha - A senha para o ID do Usuário.

        ID de Namespace - O valor pode ser localizado em **Segurança**, no recurso **Autenticação**. Por exemplo, `CognosEx`

        URL do Cognos Analytics - A URL usada para executar o Cognos Analytics. Por exemplo, `http://myserver:9300/bi`

     b. O valor de **Servidor de Configuração** é recuperado. Clique em **OK** para configurar o valor.
   - Se não for possível recuperar o valor utilizando o botão **Recuperar**, é possível configurar o valor manualmente.
     a. No servidor Content Manager ativo, abra *install_location*`/zookeeper/conf/zoo.cfg`
     b. Localize duas configurações como essa:

```
server.1=Myhost.ibm.com:2888:3888
clientPort=2181
```

c. Concatene os dois valores com um caractere de ponto e vírgula, dessa forma:

   ```
   Myhost.ibm.com:2888:3888;2181
   ```

d. Insira esse valor na propriedade.

5. Salve a configuração.

Configuração de definições criptográficas

Os componentes do IBM Cognos requerem um provedor de criptografia; caso contrário, não serão executados. Se excluiu o provedor de criptografia padrão, é necessário configurar outro provedor para substituí-lo.

É possível configurar as seguintes definições criptográficas:

- definições criptográficas gerais
- definições para o provedor de criptografia padrão
- definições para um provedor de criptografia em uma infraestrutura de segurança Entrust

Definindo configurações criptográficas gerais

Em uma instalação distribuída, os computadores IBM Cognos se comunicam com o Content Manager para estabelecer a confiança e obter algumas chaves criptográficas do Content Manager.

Se alterar as chaves criptográficas no Content Manager, como alterando os servidores de aplicativos ou reinstalando o Content Manager, você deverá excluir as chaves criptográficas nos outros computadores IBM Cognos. Então é necessário salvar as configurações em cada computador para que possam obter as novas chaves criptográficas do Content Manager. Além disso, todos os componentes do IBM Cognos em uma instalação distribuída devem ser configurados com as mesmas definições do provedor de criptografia.

Também, em um ambiente de distribuição, a chave simétrica deve ser armazenada somente nos computadores em que o Content Manager foi instalado.

É possível configurar as seguintes definições criptográficas gerais:

- conformidade de normas

  Especifica qual norma criptográfica será usada, IBM Cognos ou NIST SP 800-131A.
- propriedades de armazenamento de chave simétrica comum (CSK)

  A CSK é usada pelo IBM Cognos para criptografar e decriptografar dados.
- definições do secure sockets layer (SSL)

  Estes incluem autenticação mútua, confidencialidade e configurações de Segurança da Camada de Transporte SSL.

  Nota: A Segurança da Camada de Transporte consiste em um conjunto de regras de criptografia que usa certificados verificados e chaves de criptografia para proteger comunicações pela Internet. TLS é uma atualização do protocolo SSL. Escolha entre 1.1, 1.2 ou a configuração de combinação.
- definições avançadas de algoritmo

  Esses incluem algoritmos de resumo e de logon.

Procedimento

1. Inicie o IBM Cognos Configuration.
2. Na janela **Explorer**, em **Segurança**, clique em**Criptografia**.
3. Na janela **Propriedades**, mude os valores padrão clicando na caixa de diálogo **Valor** e selecionando o valor adequado:
   - As opções para cumprimento de conformidade de normas incluem o IBM Cognos e o NIST SP 800-131A. Este valor pode fazer com que a operação de salvamento falhe se outros parâmetros não forem permitidos no padrão selecionado. Deve-se alterar o algoritmo selecionado ou a conformidade das normas. Talvez seja necessário instalar arquivos de política de jurisdição ilimitada do JRE para permitir todos os algoritmos suportados. Eles estão disponíveis a partir daIBM.
   - Nos computadores que não contêm o Content Manager, se não desejar armazenar as CSKs localmente, altere **Armazenar chave simétrica localmente** para **Falso**, em **Configurações CSK**.

     Quando **Armazenar chave simétrica localmente** for **Falso**, a chave é recuperada do Content Manager quando solicitado. A propriedade **Localização do keystore simétricas comuns** é ignorada.
   - Se deseja que os computadores de ambos os lados de uma transmissão provem sua identidade, mude **Utilizar autenticação mútua** para **Verdadeiro**, em **Configurações SSL**.

     Não altere a configuração **Utilizar confidencialidade**.
   - Se desejar mudar o algoritmo de resumo, selecione outro valor na propriedade **Algoritmo digest**.
4. No menu **Arquivo**, clique em **Salvar**.
5. Teste o provedor de criptografia somente em um computador de gateway. Na janela **Explorer**, clique com o botão direito em **Criptografia** e clique em **Testar**.

   Os componentes do IBM Cognos verificam a disponibilidade da chave simétrica.

Resultados

Depois de ter configurado as definições criptográficas, as senhas em suas configurações e todos os dados criados são criptografados.

Configurando o provedor de criptografia padrão

É possível definir algumas configurações criptográficas para o provedor de criptografia padrão.

As seguintes configurações podem ser definidas:

- Algoritmos e conjuntos de criptografia
- Configurações de nome de identidade
- Configurações de armazenamento de chaves criptográficas

  O par de chaves criptográficas inclui a chave privada que é usada para criptografar dados e a chave pública que é usada para decriptografar dados.
- Configurações da autoridade de certificação

  A autoridade de certificação (CA) é a CA padrão ou uma CA diferente.
- Configurações de nome alternativo de assunto

  O Nome Alternativo de Assunto (SAN) é usado para validar a origem de um certificado SSL.

Procedimento

1. Se estiver usando um JRE diferente do fornecido com o servidor IBM Cognos, acesse *install_location*/jre/lib/ext.
2. Copie bcprov-jdk*version*.jar no *JRE_location*/lib/ext.
3. Se estiver usando um JRE diferente do fornecido pela IBM, você também deve fazer download e instalar o arquivo de políticas irrestrito Java Cryptograph Extension (JCE) para seu JRE para assegurar que todos os algoritmos e conjuntos de códigos disponíveis sejam mostrados em IBM Cognos Configuration.
4. Inicie o IBM Cognos Configuration.
5. Na janela **Explorer**, em **Segurança**, **Criptografia**, clique em **Cognos**.
6. Na janela **Propriedades**, altere as propriedades, conforme necessário.

   Dica: Para obter informações detalhadas sobre cada propriedade, visualize a descrição da propriedade no IBM Cognos Configuration quando clicar na propriedade.

   - Para configurar o algoritmo de confidencialidade, na propriedade adequada, **Algoritmo de confidencialidade** ou **Algoritmo de confidencialidade PDF**, clique na coluna **Valor** e selecione o algoritmo na lista suspensa.

     O valor do algoritmo de confidencialidade determina como os dados são criptografados pelos componentes do IBM Cognos. Por exemplo, senhas do banco de dados inseridas no IBM Cognos Configuration são criptografadas quando você salva a configuração. O algoritmo selecionado quando os dados são criptografados também devem estar disponíveis para os dados para serem criptografados mais tarde.

     A disponibilidade dos algoritmos de confidencialidade podem mudar se houver mudanças em seu ambiente Por exemplo, se seu Java Runtime Environment (JRE) tiver mudado ou se você tiver instalado outro software criptográfico no computador. É necessário verificar se o **Algoritmo de confidencialidade** selecionado quando os dados foram criptografados também está disponível quando desejar acessar os dados.

     Se foram feitas mudanças em um computador, como uma atualização no JRE ou a instalação de um software que atualizou o JRE, isto pode afetar a disponibilidade dos algoritmos de confidencialidade. Para garantir que os conjuntos de códigos e algoritmos disponíveis sejam mostrados no IBM Cognos Configuration, faça o download e instale o arquivo de políticas Java Cryptography Extension (JCE) irrestrito. Para o Java que a IBM fornece, o arquivo de políticas JCE restrito pode ser transferido por download dos Arquivos de Política JCE Irrestritos (https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=jcesdk).
   - Para ajustar os conjuntos de cifras, em **Conjuntos de Cifras Suportados**, clique na coluna **Valor** e, em seguida, clique no ícone de edição  .

     Remova os conjuntos de códigos que não são aplicáveis e mova os conjuntos remanescentes para cima ou para baixo na lista para que aqueles conjuntos de códigos na faixa mais alta estejam na posição mais alta da lista.

     Não misture conjuntos de códigos na faixa de 40 a 56 bits com conjuntos de códigos na faixa de 128 a 168 bits.
   - Para mudar o local das chaves de criptografia, em **Configurações da chave de criptografia**, mude **Local do armazenamento de chaves de criptografia** para um novo local.

- Para usar outra autoridade de certificação, em **Configuração da autoridade de certificação**, altere **Utilizar CA de terceiros** para **Verdadeiro**.

  Para obter mais informações, consulte "Configurando Componentes do IBM Cognos para Usar Outra Autoridade de Certificação" na página 179.
- Ao configurar para HTTPS/SSL, mude o **Nome comum do servidor** de CAMUSER para o nome completo do domínio do servidor.
- Para configurar o **Nome Alternativo de Assunto**, especifique **Nomes DNS**, **Endereços IP** e **Endereços de e-mail** (opcional) que estão associados ao certificado do servidor. Os valores são incluídos nas extensões de Nome Alternativo de Assunto no certificado do servidor. É possível especificar diversos valores para cada propriedade. Separe os valores usando o caractere de espaço.

7. No menu **Arquivo**, clique em **Salvar**.

Resultados

Se você usar outro servidor de autoridade de certificação (CA), configure os componentes do IBM Cognos para usarem a CA. Para obter mais informações, consulte "Configurando Componentes do IBM Cognos para Usar Outra Autoridade de Certificação" na página 179.

Configuração das definições do provedor de criptografia em uma infraestrutura de segurança Entrust

Para configurar a criptografia em uma infraestrutura de segurança Entrust, substitua o provedor de criptografia padrão no IBM Cognos Configuration por um provedor que você configurar para Entrust e atualize os arquivos de segurança no ambiente do IBM Cognos.

Antes de Iniciar

Verifique se as senhas dos bancos de chaves correspondem às do Perfil Entrust (EPF)

Para evitar erros de gateway, assegure-se de que a Conta Guest da Internet tenha permissão de leitura e gravação ao arquivo `.epf` do Entrust e permissão de leitura ao arquivo `.ual` do Entrust.

Procedimento

1. Se estiver usando um JRE diferente do fornecido com o servidor IBM Cognos, acesse *install_location*`/jre/lib/ext`.
2. Copie `bcprov-jdk`*version*`.jar` no *JRE_location*`/lib/ext`.
3. Assegure-se de que os seguintes arquivos do IBM Cognos e Entrust existam no local em que o JRE está instalado:
   - No Entrust Authority Security Toolkit do qual foi feito download a partir do Entrust, copie o arquivo `.jar` file, como `enttoolkit.jar`, no *JRE_location*`/lib/ext`.
4. Para garantir que todos os conjuntos de códigos e algoritmos disponíveis sejam mostrados no IBM Cognos Configuration, faça o download e instale o arquivo de políticas Java Cryptography Extension (JCE) irrestrito. Para o Java que a IBM fornece, o arquivo de políticas JCE restrito pode ser transferido por download dos Arquivos de Política JCE Irrestritos (https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=jcesdk).
5. Inicie o IBM Cognos Configuration.

6. Na janela **Explorer**, no grupo **Segurança**, clique em**Criptografia**.
7. Na janela **Propriedades**, em **Configurações avançadas de algoritmo**, altere o **Algoritmo digest** para o algoritmo digest de mensagem adequado ou para o algoritmo hash seguro para a sua política de segurança.
8. Na janela **Explorer**, no grupo **Segurança** e no componente **Criptografia**, clique com o botão direito no recurso **IBM Cognos** e clique em **Excluir**.
9. No grupo **Segurança**, clique com o botão direito do mouse em **Criptografia** e clique em **Novo Recurso** > **Provedor**.
10. No campo **Nome**, digite um nome para o serviço de criptografia que está criando.
11. No campo **Tipo**, clique na seta e em **Entrust**e, em seguida, clique em **OK**.

    Uma ramificação com o nome designado aparece em **Criptografia**.
12. Clique na ramificação criou.

    As propriedades de recursos aparecerão na janela de propriedades.
13. Na janela **Propriedades do Recurso**, insira os valores apropriados, conforme listados na tabela a seguir:

Tabela 21. Valores e Descrições das Propriedades de Criptografia

Propriedade	Descrição
Localização do arquivo INI	A localização do arquivo de inicialização (.ini) do Entrust.
Nome distinto de arquivo de identidade (DN)	O nome distinto associado ao perfil da identidade do Entrust.
Localização do arquivo de identidade	A localização do arquivo de perfil (.epf) da identidade do Entrust.
Utilizar login do servidor Entrust	O parâmetro que controla se os usuários devem digitar uma senha para fazer logon no Entrust PKI.
Senha do arquivo de identidade	A senha do Entrust Profile, que deve corresponder à senha no Entrust Profile (EPF).
Algoritmo de confidencialidade	O nível de criptografia que é necessário para ficar em conformidade com a política de segurança.
Algoritmo de confidencialidade PDF	O algoritmo de criptografia a ser usado quando criptografar dados PDF.
Ciphersuites com suporte	Os conjuntos de códigos que são suportados em seu ambiente de segurança. Remova os que não se aplicam e reorganize os conjuntos de códigos restantes do mais alto para o mais baixo. Isso garante que o conjunto de códigos mais seguro seja usado primeiro.
Localização do keystore de assinatura	A localização do banco de dados de chaves que contém os pares de chaves de assinatura.
Localização do keystore de criptografia	A localização do keystore que contém os pares de chaves de criptografia.

Importante: Registre as senhas em um local seguro.

14. No menu **Arquivo**, clique em **Salvar**.

15. Atualize para o Entrust Java Toolkit 7.2 SP2 Patch 170072.

IBM Cognos Application Firewall

IBM Cognos Application Firewall analisa e valida solicitações de HTTP e XML antes de elas serem processadas pelos servidores IBM Cognos. IBM Cognos Application Firewall pode modificar essas solicitações de HTTP e XML.

IBM Cognos Application Firewall protege produtos da Web do IBM Cognos contra dados dolosos. As formas mais comuns de dados mal-intencionados são de estouro de buffer e ataques de scripts de cross-site scripting (XSS), através de injeção de scripts em páginas válidas ou redirecionamento para outro Web site.

É possível rastrear atividades de firewall verificando o arquivo de log, que contém solicitações rejeitadas. Por padrão, as mensagens de log são armazenadas no arquivo *install_location*/logs/cogaudit.log.

Se você estiver usando os recursos de colaboração com o IBM Connections, será necessário incluir o nome do host, domínio e número da porta no qual o IBM Connections está sendo executado na propriedade **Domínios e Hosts Válidos** para o Cognos Application Firewall.

Todas as configurações do Cognos Application Firewall devem ser as mesmas para todos os computadores nos quais os Componentes da Camada de Aplicativos do IBM Cognos estão instalados em um ambiente distribuído. Por exemplo, se o Cognos Application Firewall estiver desativado em alguns computadores e ativado em outros, o resultado poderá ser um comportamento inesperado e erros do produto.

Os seguintes tipos de URLs são aceitos pela validação do Cognos Application Firewall:

- URLs totalmente qualificados (absolutos)

  no formato *protocol*://*host*:*port*/*path*, em que o *protocolo* é http ou https e o *host* é validado em relação à lista de domínios válida
- URLs relativos ao diretório de instalação web

  no formato /*raiz_instalação_web*/.* em que *raiz_instalação_web* é o diretório de gateway web, baseado no alias ibmcognos configurado em seu servidor web.

  Por exemplo,

  /ibmcognos/ps/portal/images/action_delete.gif
- URLs específicos permitidos, incluindo o seguinte (nenhum diferencia maiúsculas de minúsculas)

  about:blank

  JavaScript:window.close( )

  JavaScript:parent.close( )

  JavaScript:history.back( )

  parent.cancelErrorPage( )

  doCancel( )

Configurando componentes do IBM Cognos para usar o IBM Cognos Application Firewall

Usando IBM Cognos Configuration, é possível alterar configurações para o suporte de outra ferramenta XSS e incluir nomes de host e domínio na lista do IBM Cognos de nomes válidos.

Procedimento

1. Inicie o IBM Cognos Configuration em cada local em que os Componentes da Camada de Aplicativos estão instalados.
2. Na janela **Explorer**, em **Segurança**, clique em **IBM Cognos Application Firewall**.
3. Na janela **Propriedades**, na propriedade **Habilitar a validação do CAF**, defina os valores adequados.

   Por padrão, o IBM Cognos Application Firewall fica ativado.

   Importante: O IBM Cognos Application Firewall é um componente essencial para a segurança do IBM Cognos, ajudando a fornecer proteção contra vulnerabilidades de invasão. A desativação do IBM Cognos Application Firewall removerá a proteção. Sob circunstâncias normais, não desative o IBM Cognos Application Firewall.
4. Se estiver usando outra ferramenta XSS que verifica caracteres específicos nos parâmetros de solicitação GET, na janela **Propriedades**, para a propriedade **A verificação XSS de terceiros está habilitada**, altere o valor para **Verdadeiro**.

   Os caracteres padrão que são proibidos incluem >, < e '.
5. Inclua nomes de host e domínio na lista do IBM Cognos de nomes válidos:
   - Para a propriedade **Domínios e Hosts Válidos**, clique no valor e, em seguida, clique no ícone de edição  .
   - Na caixa de diálogo **Valor - Domínios ou hosts válidos**, clique em **Adicionar**.

     Deve-se incluir os domínios de todos os hiperlinks incluídos no portal. Para obter mais informações, consulte o tópico sobre como criar uma URL no *Guia de administração e segurança do IBM Cognos Analytics*.

     Dica: Se estiver usando drill through do IBM Cognos Series 7 para relatórios no IBM Cognos Analytics, inclua os nomes de host dos servidores gateway do IBM Cognos Series 7 na lista.
   - Na linha em branco da tabela, clique e digite o nome de host ou de domínio.

     Para permitir um domínio e todos os seus subdomínios, use um caractere curinga no início do nome do domínio.

     Por exemplo, ***.mycompany.com**

     Se estiver usando os recursos de colaboração com o IBM Connections, será necessário incluir o host, domínio e número da porta para o perfil do IBM WebSphere no qual o IBM Connections foi instalado. Por exemplo, se instalasse o IBM Connections em um computador denominado **myserver** e seu domínio fosse **mycompany.com**, você incluiria **myserver.mycompany.com:9080**, em que 9080 é o número da porta do IBM WebSphere em que o IBM Connections está em execução.
   - Repita as duas etapas anteriores marcadas para cada nome a ser adicionado.
   - Clique em **OK**.

   IBM Cognos Application Firewall valida nomes de host e domínio para proteger as URLs que são criadas. Por padrão, o IBM Cognos Application Firewall considera nomes de domínio derivados das propriedades de configuração de ambiente como nomes de domínio seguros. A inclusão de nomes à lista de nomes e hosts válidos é útil quando você precisa redirecionar

solicitações para computadores não IBM Cognos usando as funções Voltar ou Cancelar ou ao usar drill through em instalações de diferentes produtos IBM Cognos.

6. Salve a configuração.
7. Reinicie os serviços.

Criptografia de propriedades de arquivo temporário

Arquivos temporários são usados no IBM Cognos Analytics para armazenar os relatórios visualizados recentemente e para armazenar dados usados pelos serviços durante o processamento. É possível alterar o local dos arquivos temporários e optar por criptografar seu conteúdo.

Por padrão, os componentes do IBM Cognos armazenam arquivos temporários no diretório *install_location*\temp e os arquivos não são criptografados.

Para otimizar a segurança, negue todos os acessos ao diretório temporário, exceto para a conta do serviço usada para iniciar os serviços do IBM Cognos. São necessárias permissões de leitura e gravação para a conta do serviço.

Procedimento

1. Inicie o IBM Cognos Configuration.
2. Na janela **Explorer**, clique em **Ambiente**.
3. Na janela **Propriedades**, na propriedade **Localização dos arquivos temporários**, especifique o novo local.
4. Se solicitar que o conteúdo de arquivos temporários seja criptografado, configure a propriedade **Criptografar arquivos temporários** para **Verdadeiro**.
5. Certifique-se de que a conta do usuário sob a qual os componentes do IBM Cognos Analytics são executados tenha os privilégios adequados para o local dos arquivos temporários. Por exemplo:
   - nos sistemas operacionais Microsoft Windows, privilégios de controle integral
   - nos sistemas operacionais UNIX ou Linux, privilégios de leitura/gravação

Configuração do gateway para usar um namespace

Se os componentes do IBM Cognos usarem diversos namespaces, ou se o acesso anônimo estiver ativado e os componentes do IBM Cognos usarem um namespace, é possível configurar o gateway para se conectar a um namespace. Os usuários logados no servidor web em que o gateway está localizado não são avisados para escolher uma fonte de autenticação. Por exemplo, se tiver dois servidores web, é possível configurar cada servidor web para usar um namespace diferente.

Procedimento

1. No computador no qual gateway está localizado, inicie o IBM Cognos Configuration.
2. Na janela **Explorer**, clique em **Ambiente**.
3. Na janela **Propriedades**, na caixa **Valor** ao lado da propriedade **Namespace do gateway**, digite a ID do namespace que deseja usar.
4. No menu **Arquivo**, clique em **Salvar**.
5. Reinicie seu servidor web.

Ativação e desativação de serviços

Em uma instalação de distribuição, é possível enviar certos tipos de solicitações para computadores específicos ativando ou desativando os serviços instalados.

Por exemplo, para dedicar um computador a executar e distribuir relatórios, é possível desativar os serviços em um computador com Application Tier Components.

Nota: Os valores padrão para o serviço do dispatcher e o serviço de apresentação são "false" em computadores que têm apenas o Content Manager instalado. Em todos os outros tipos de instalação, os valores padrão são verdadeiros.

Se foram instalados todos os componentes em diversos computadores, é possível desativar serviços adequados em cada computador para obter a configuração de distribuição solicitada. Solicitações são enviadas somente para dispatchers em que dado serviço é ativado.

Desativar um serviço impede-o de carregar na memória. Ao serem desativados, os serviços não são iniciados e em consequência não consomem recursos. O serviço virtual não executa até que seja ativado.

Se desativar o serviço do dispatcher, os serviços relacionados ao dispatcher são desativados. Somente os serviços do dispatcher que são ativados podem processar solicitações.

Restrição: Ao reiniciar manualmente os serviços, (se aplicável) o serviço **ApacheDS - cognos** deve ser iniciado antes do serviço **IBM Cognos**.

Ativando e Desativando Serviços

Use o seguinte procedimento para desativar serviços selecionados em componentes em uma instalação distribuída.

Procedimento

1. Inicie o IBM Cognos Configuration.
2. Na janela **Explorer**, em **Ambiente**, clique em **Serviços do IBM Cognos**.
3. Na janela **Propriedades**, clique em **Valor** próximo ao serviço que deseja ativar ou desativar.

   Por padrão, todos os serviços estão ativados.
4. Clique no estado adequado para os serviços:
   - Para desativar o serviço, clique em **Falso**.
   - Para ativar o serviço, clique em **Verdadeiro**.

   Ao reiniciar manualmente os serviços, (se aplicável) o serviço **ApacheDS - cognos** deve ser iniciado antes do serviço **IBM Cognos**.
5. No menu **Arquivo**, clique em **Salvar**.

Configurando Fontes

Os produtos IBM Cognos usam fontes para renderizar relatórios PDF no servidor IBM Cognos. Eles também usam fontes para renderizar gráficos usados em relatórios PDF e HTML.

Para mostrar a saída corretamente, as fontes devem estar disponíveis onde o relatório ou gráfico são processados. Para gráficos e relatórios em PDF, as fontes

devem ser instaladas no servidor IBM Cognos. Se uma fonte solicitada não estiver disponível, os componentes do IBM Cognos substituirão uma fonte diferente.

Como os relatórios HTML são renderizados em um navegador, as fontes necessárias devem ser instaladas no computador de cada usuário do IBM Cognos que visualiza o relatório. Caso uma fonte solicitada não esteja disponível, o navegador a substituirá por uma fonte diferente.

Utilize a seguinte lista de verificação se deseja utilizar uma nova fonte nos relatórios.

__ • Adição da fonte à lista de fontes suportadas.
__ • Especificação do local do arquivo da nova fonte.
__ • Mapeamento da nova fonte para o nome da fonte física, se solicitado.

Considerações para Suportar o Chinês Simplificado

Os produtos IBM Cognos suportam o conjunto de caracteres GB18030-2000, que é usado na codificação de códigos de idioma chinês simplificado.

Se você instalar no Microsoft Windows, o suporte será fornecido para o conjunto de caracteres GB18030-2000 na fonte SimSun-18030, fornecida pela Microsoft.

Em sistemas operacionais diferentes do Windows, você deve instalar uma fonte que suporte GB18030-2000.

Incluindo Fontes no Ambiente do IBM Cognos

É possível incluir fontes na lista de fontes suportadas no ambiente do IBM Cognos se você quiser gerar relatórios que usem fontes que não estão disponíveis atualmente. Também é possível remover fontes. Por padrão, os componentes do IBM Cognos usam um conjunto global de fontes, que estão disponíveis em todos os computadores servidores IBM Cognos.

Procedimento

1. Em cada computador que tiver o Content Manager, inicie o IBM Cognos Configuration.
2. No menu **Ações**, clique em **Editar Configuração Global**.
3. Clique na guia **Fontes**.
4. Clique em **Incluir**.

   Dica: Para remover uma fonte da lista de fontes suportadas, clique na caixa próxima do nome da fonte e clique em **Remover**.
5. Na caixa **Nome da Fonte com Suporte**, digite o nome da fonte e clique em **OK**.
6. No menu **Arquivo**, clique em **Salvar**.

   Todas as fontes globais, incluindo as novas fontes incluídas, devem ser instaladas em todos os computadores do ambiente que tenham o IBM Cognos.

Resultados

Se uma fonte global não estiver instalada em todos os computadores IBM Cognos, será necessário mapear a fonte global para uma fonte física instalada.

Especificando o local das fontes disponíveis

É necessário especificar o local de instalação de todas as fontes, incluindo aquelas que foram adicionadas à lista de fontes suportadas.

Por padrão, a lista de fontes é composta de fontes que são instaladas no diretório *install_location*\bin\fonts do computador do IBM Cognos. Se os componentes do IBM Cognos estiverem instalados em um computador de sistema operacional Microsoft Windows, eles também usarão as fontes que estão instaladas no diretório de fonte do Windows.

Você especifica o local da fonte em todos os computadores em que o Application Tier Components está instalado.

Procedimento

1. Em cada computador com Componentes da Camada de Aplicativos, inicie o IBM Cognos Configuration.
2. Na janela **Explorer**, clique em **Ambiente**.
3. Na janela **Propriedades**, na propriedade **Locais de fontes físicas**, especifique o local das fontes.

   Se houver diversos caminhos de fontes, separe cada caminho por um ponto-e-vírgula (;).

   Se estiver usando um servidor de aplicativos diferente do que é fornecido com o IBM Cognos Analytics, insira o caminho completo para o local da fonte. Por exemplo: *install_location*\bin\fonts.
4. No menu **Arquivo**, clique em **Salvar**.

Mapeamento de fontes suportadas para fontes instaladas

É possível substituir fontes globais, que não estão instaladas no computador, por fontes físicas.

Mapeie as fontes em cada computador onde o Application Tier Components estejam instalados.

Por exemplo, inclua uma fonte na lista de fontes suportadas que não está instalada no computador IBM Cognos. É possível especificar qual fonte usar como substituto.

Se desejar imprimir relatórios mais rápido usando as fontes de PDF integradas, mapeie uma fonte global como Arial para uma das fontes de PDF integradas, como Helvetica-PDF, seguindo as etapas abaixo. Também é possível selecionar uma das fontes de PDF integradas para um objeto de texto no Relatórios ou no Query Studio. Para obter mais informações, consulte o *Guia do usuário do Query Studio* ou o *Guia do usuário do Relatórios*.

Nenhum mapeamento será necessário se você incluir uma fonte na lista de fontes suportadas que não está instalada em computadores IBM Cognos. Entretanto, é preciso especificar a localização das fontes.

Procedimento

1. Em cada computador com Componentes da Camada de Aplicativos, inicie o IBM Cognos Configuration.
2. Na janela **Explorer**, clique em **Ambiente**.
3. Na janela **Propriedades**, clique na caixa **Valor** próxima à propriedade **Mapa de Fontes Físicas** e, em seguida, clique no ícone de edição  .

   A caixa de diálogo **Valor - Mapa de fontes físicas** aparece.
4. Clique em **Incluir**.

Dica: Para remover uma fonte, selecione a caixa de seleção próxima da fonte e clique em **Remover**.

5. Na caixa de diálogo **Nome da Fonte Global**, digite o nome da fonte adicionada à lista de fontes suportada.
6. Clique na caixa **Nome da Fonte Física**.
7. Se souber o nome da fonte física, digite-o. Caso contrário, clique no ícone de edição  .

   Na caixa de diálogo **Nome da Fonte Física**, clique em **Procurar Agora** e clique em um nome de fonte nos resultados.
8. Repita as etapas 4 a 7 para cada fonte global que necessita de mapeamento.
9. Clique em **OK**.
10. No menu **Arquivo**, clique em **Salvar**.

Resultados

Agora, se necessário, especifique a localização de instalação das fontes.

Usando fontes de sistema no IBM Cognos Configuration

É possível configurar o IBM Cognos Configuration para usar suas fontes do sistema em sistemas operacionais Microsoft Windows.

Nota: Se ativar configurações de fonte do sistema, não será possível alterá-las no IBM Cognos Configuration.

Procedimento

1. Acesse o diretório *install_location*/configuration.
2. Abra o arquivo cogconfig.prefs em um editor de texto.
3. Inclua a linha a seguir:

   ```
   UseSystemDisplaySetting=true
   ```
4. Salve e feche o arquivo.
5. Reinicie IBM Cognos Configuration.

Alterar a Fonte Padrão de Relatórios em PDF

É possível alterar a fonte padrão usada pelos componentes do IBM Cognos Analytics para os relatórios em PDF. A seguinte fonte padrão é exibida ao abrir um relatório.

Altera-se a fonte padrão no computador em que o Content Manager está instalado. Em seguida, a fonte torna-se o padrão para todos os computadores em sua instalação. Altere a fonte usada para relatórios em PDF usando o IBM Cognos Configuration.

Certifique-se de que a fonte padrão esteja instalada em todos os computadores em sua instalação do IBM Cognos.

Para garantir que os caracteres GB18030 sejam exibidos corretamente em relatórios em PDF, configure a fonte padrão como SimSun-GB18030.

Procedimento

1. Em cada computador que tiver o Content Manager, inicie o IBM Cognos Configuration.

2. No menu **Ações**, clique em **Editar Configuração Global**.
3. Clique na guia **Geral**.
4. Na caixa de diálogo **Valor**, em **Fonte padrão**, digite a fonte que deseja utilizar como o padrão para relatórios.
5. Clique em **OK**.
6. No menu **Arquivo**, clique em **Salvar**.
7. Em todos os computadores com Componentes da Camada de Aplicativos, certifique-se de que o local de instalação da fonte padrão esteja especificado na propriedade **Locais de fontes físicas** (em **Ambiente** na janela **Explorer**) ou de que a fonte esteja em um diretório de fonte do Windows.

Configuração de fontes integradas a relatórios em PDF

Quando um relatório em PDF é aberto no Adobe Reader, todas as fontes usadas nesse relatório devem estar disponíveis. As fontes devem estar integradas no relatório ou instaladas no computador do usuário. Se uma fonte não estiver disponível em nenhum desses locais, o Adobe Reader tentará substituir uma fonte apropriada. Essa substituição pode causar mudanças na apresentação do relatório ou alguns caracteres podem não ser exibidos.

Para garantir que os relatórios em PDF apareçam corretamente no Adobe Reader, o IBM Cognos Analytics integra as fontes necessárias nos relatórios por padrão. Para minimizar o tamanho do arquivo, o IBM Cognos Analytics integra apenas os caracteres (também chamados de glifos) utilizados no relatório, em vez de todos os caracteres do conjunto de fontes. O IBM Cognos Analytics somente integra as fontes se elas estiverem licenciadas para integração. As informações sobre licença são armazenadas na própria fonte e são lidas pelo IBM Cognos Analytics.

Se tiver certeza de que as fontes usadas nos relatórios estão disponíveis nos computadores dos usuários, é possível limitar ou eliminar fontes integradas para reduzir o tamanho dos relatórios PDF. Ao limitar fontes, você especifica se uma fonte sempre é ou nunca é integrada usando uma lista de fontes integradas no IBM Cognos Configuration.

Procedimento

1. No computador com Content Manager, inicie o IBM Cognos Configuration.
2. Na janela **Explorer**, clique em **Ambiente**.
3. Na janela **Propriedades**, em **Configurações de Fonte**, clique no valor de **Fontes a Serem Integradas (serviço de relatório em lotes)** ou em **Fontes a Serem Integradas (serviço de relatório)** e, em seguida, clique no ícone de edição  .
4. Se não estiver usando o diretório de fontes padrão ou se desejar adicionar um caminho para um diretório adicional, na caixa de diálogo **Fontes a Serem Incorporadas nos Relatórios no Formato PDF**, especifique o novo caminho na caixa de diálogo de caminhos de fontes.

   Dica: clique em **Buscar Agora** para obter uma lista de fontes disponíveis no caminho especificado.
5. Para uma fonte que sempre estará disponível nos computadores dos usuários, role até o nome da fonte e clique na caixa de seleção **Nunca**.

   O IBM Cognos Analytics não integra a fonte a nenhum relatório. O Adobe Reader seleciona a fonte do computador do usuário quando o relatório é aberto.

6. Para uma fonte que pode nem sempre estar disponível nos computadores dos usuários, role até o nome da fonte e clique na caixa de seleção **Sempre**.

   O IBM Cognos Analytics integra a fonte a todos os relatórios que a utilizam. Adobe Reader usa a fonte integrada quando o relatório é aberto.
7. Clique em **OK**.

Saída de relatório salvo

Por padrão, os arquivos de saída de relatório são salvos no armazenamento de conteúdo. Existe a opção de salvar uma cópia da saída de relatório em outro local de arquivo, fora ou dentro do IBM Cognos Analytics. Se usar esta opção, um arquivo descritor com a extensão an _descr também é salvo. Os arquivos salvos não são gerenciados pelo IBM Cognos Analytics.

Salvar a saída de relatório fora do IBM Cognos Analytics

Se você configurar um local de sistema de arquivos fora do IBM Cognos Analytics, poderá compartilhar a saída de relatório com aplicativos externos ou pessoas que não têm o IBM Cognos Analytics. É assim que se salva a maioria dos arquivos de saída de relatório.

Para usar esse recurso, primeiro você deve configurar um diretório-raiz no IBM Cognos Configuration. Um administrador deve configurar o local do arquivo no IBM Cognos Administration. Para obter mais informações, consulte o tópico sobre como configurar um local de arquivo para a saída de relatório salva fora do IBM Cognos Analytics, no *Guia de administração e segurança do IBM Cognos Analytics*.

As saídas do relatório sempre serão gravadas no diretório configurado para cada instância do Serviço de entrega. A fim de evitar ter saídas de relatório gravadas em diversos locais, assegure-se de estar executando apenas uma instância do Serviço de entrega ou configurar todas as instâncias para usar um local de arquivo de rede compartilhada. Qualquer despachante executando o Serviço de entrega deve ter acesso ao sistema de arquivos ou estar desativado em todos os sistemas não destinados a salvar saída de relatório.

Procedimento

1. Crie um diretório para o sistema de arquivos.

   Dica: Certifique-se de que o diretório esteja acessível para os usuários e separado do diretório de instalação. Por exemplo, em uma instalação distribuída no Microsoft Windows, uma pasta de archive como *\\servername\directory* poderia ser usada.
2. No computador com Content Manager, inicie o IBM Cognos Configuration.
3. No menu **Ações**, clique em **Editar Configuração Global**.
4. Na janela **Configuração global**, clique na guia **Geral**.
5. Para **Raiz do sistema de arquivos da localização de archive**, digite um URI usando o formato

   `file://directory`

   em que *diretório* é o diretório criado na etapa 1.

   A parte arquivo:// do URI é necessária. Nomes UNC do Windows como *\\servername\directory* podem ser usados. Se for o caso, o URI deve ser formatado como segue:

   `file://\\servername\directory`

   Dica: Assegure-se de não usar uma unidade mapeada ao executar o Cognos como um serviço do Microsoft Windows.

6. Para confirmar que o local correto será usado, clique em **Testar**.
7. Clique em **OK**.
8. No menu **Arquivo**, clique em **Salvar**.

Resultados

O administrador agora deve configurar o local do arquivo. Para obter informações, consulte o tópico sobre como configurar um local de arquivo para a saída de relatório salva fora do IBM Cognos Analytics, no *Guia de administração e segurança do IBM Cognos Analytics*.

Salvar saída de relatório dentro do IBM Cognos Analytics

Se você configurar um local de sistema de arquivos dentro do IBM Cognos Analytics, poderá usar a saída de relatório novamente. Isso também pode ser útil para propósitos de archive, pois os arquivos salvos no armazenamento de conteúdo podem ser excluídos regularmente devido a regras de retenção.

Para usar esse recurso, primeiro você deve ativar a propriedade **Salvar saídas de relatório em um sistema de arquivos** no IBM Cognos Configuration. Um administrador deve configurar o local do arquivo usando o parâmetro CM.OutPutLocation no IBM Cognos Administration. Para obter mais informações, consulte o tópico sobre como configurar um local de arquivo para a saída de relatório salva dentro do IBM Cognos Analytics, no *Guia de administração e segurança do IBM Cognos Analytics*.

As saídas do relatório sempre serão gravadas no diretório configurado para cada instância do Serviço de entrega. A fim de evitar ter saídas de relatório gravadas em diversos locais, assegure-se de estar executando apenas uma instância do Serviço de entrega ou configurar todas as instâncias para usar um local de arquivo de rede compartilhada. Qualquer despachante executando o Serviço de entrega deve ter acesso ao sistema de arquivos ou estar desativado em todos os sistemas não destinados a salvar saída de relatório.

Para proteger a segurança da saída de relatório quando usar esse recurso, o sistema de arquivos deve ter criptografia de terceiros.

Procedimento

1. Crie um diretório para o sistema de arquivos.

   Dica: Certifique-se de que o diretório esteja acessível somente para usuários autorizados.
2. No computador com Content Manager, inicie o IBM Cognos Configuration.
3. Na janela **Explorer**, clique em **Acesso a Dados** > **Content Manager**.
4. Na propriedade **Salvar saídas de relatórios em um sistema de arquivos**, clique em **Verdadeiro**.
5. Para testar a conexão com o diretório de saída de relatório, no menu **Ações**, clique em **Testar**.
6. No menu **Arquivo**, clique em **Salvar**.

Resultados

O administrador agora deve configurar o local do arquivo usando o parâmetro CM.OutPutLocation. Para obter informações, consulte o tópico sobre como configurar um local de arquivo para a saída de relatório salva dentro do IBM

Cognos Analytics, no *Guia de administração e segurança do IBM Cognos Analytics*.

Mudando o local da saída de relatório temporária

Quando os usuários executam relatórios interativos, a saída do relatório será armazenada no Content Manager ou em um cache de sessão temporária no sistema local do arquivo de relatórios. É possível alterar o local do cache de sessão temporário para um computador remoto, como um diretório compartilhado em um sistema baseado em Microsoft Windows ou um diretório montado comum em um sistema baseado em UNIX ou Linux.

Por padrão, o local do cache de sessão temporário no sistema de arquivos de relatório é `install_location/temp/session`. O diretório `session` é criado pelo servidor de relatório quando a primeira solicitação de uma sessão do usuário é recebida.

Procedimento

1. Inicie o IBM Cognos Configuration nos computadores em que os Componentes da Camada de Aplicativos estão instalados.
2. Na janela **Explorer**, clique em **Ambiente**.
3. Na janela **Propriedades**, clique no valor do **Local de Arquivos Temporários** e, em seguida, clique no ícone de edição  .
4. Na caixa de diálogo **Selecionar pasta**, use a caixa **Salvar em** para localizar o computador e o diretório e, em seguida, clique em **Selecionar**.
5. No menu **Arquivo**, clique em **Salvar**.

   Quando um usuário executa uma sessão de relatório interativa, a saída de relatórios temporários será armazenada no novo local.

Mudando o local dos mapas anteriores do Gerenciador de mapas para o Relatórios

O IBM Cognos Analytics é fornecido com um conjunto de gráficos de mapa de amostra que podem ser usados no Relatórios. É possível alterar o local dos gráficos de mapa usando o IBM Cognos Configuration.

Nota: Essas informações são aplicadas somente aos mapas anteriores do Gerenciador de mapas que você pode usar em relatórios.

Por padrão, os gráficos de mapa são armazenados no diretório `install_location/maps` no computador dos Componentes da Camada de Aplicativos.

Para obter mais informações sobre como usar gráficos de mapas, consulte o *Guia do Usuário* do Relatórios.

Para obter informações sobre o uso de mapas customizados de outras fontes, consulte o Map Manager *Installation and User Guide*.

Procedimento

1. No computador com Componentes da Camada de Aplicativos, inicie o IBM Cognos Configuration.
2. Na janela **Explorer**, clique em **Ambiente**.

3. Na janela **Propriedades**, clique no valor para **Localização de arquivos de mapeamento**.
4. Clique no botão de edição  .
5. Na janela **Selecionar pasta**, navegue para o diretório que deseja e clique em **Selecionar**.
6. No menu **Arquivo**, clique em **Salvar**.

Ajustando o WebSphere Liberty Profile

Em ambientes de produção, ajuste o WebSphere Liberty Profile para permitir o número máximo de usuários simultâneos esperado, ajustando os valores de **coreThreads** e **maxThreads** nas propriedades Avançadas dos recursos. Estes valores configuram as contagens principais e máximas de encadeamentos do executor.

Procedimento

1. Inicie o IBM Cognos Configuration.
2. Na janela **Explorer**, em **Ambiente**, em **Serviços do IBM Cognos**, clique no nome dos Recursos (o padrão é **IBM Cognos**).
3. Na janela **Propriedades**, próximo a **Propriedades Avançadas**, clique na caixa **Valor** e, em seguida, clique no ícone de edição  .
4. Ajuste os valores de parâmetro conforme necessário.

Tabela 22. Nomes e valores do parâmetro Recurso de Serviço

Nome do parâmetro	Valor
coreThreads	O número principal de encadeamentos com os quais o servidor do WebSphere Liberty Profile é iniciado. Se este valor for menor que 0, um valor padrão será usado. Este valor padrão é calculado com base no número de encadeamentos de hardware presentes no sistema.
maxThreads	O número máximo de encadeamentos que podem ser associados ao servidor do WebSphere Liberty Profile.

   Para obter mais informações, consulte o WebSphere Liberty Profile Knowledge Center, Ajustando o perfil Liberdade (http://www.ibm.com/support/knowledgecenter/?lang=en#!/SSEQTP_8.5.5/com.ibm.websphere.wlp.doc/ae/twlp_tun.html?cp=SSEQTP_8.5.5%2F1-3-11-0-7).
5. No menu **Arquivo**, clique em **Salvar**.

Ativando replicação de sessão para serviços do Content Manager em espera

O recurso de replicação de sessão permite o failover direto do IBM Cognos Content Manager entre um serviço do Content Manager ativo e um serviço do Content Manager em espera.

Com a replicação de sessão ativada, os dados da sessão do usuário são replicados entre todas as instâncias do Content Manager. Se o Content Manager ativo falhar, os dados da sessão do usuário serão preservados e os usuários continuarão usando o aplicativo sem interrupção.

A replicação de sessão usa duas portas para se comunicar com segurança com diferentes IBM Cognos Content Managers configurados dentro de um único ambiente.

Procedimento

1. Em um computador no qual o IBM Cognos Content Manager está instalado, inicie o IBM Cognos Configuration.
2. Na área de janela **Explorer**, em **Segurança**, clique em **Replicação**.
3. Especifique as propriedades a seguir:
   a. Configure **Ativar replicação** para **Verdadeiro**.
   b. Na caixa de valor **Número da porta do listener peer**, insira um número de porta.

      Um valor de 0 seleciona a primeira porta dinâmica disponível durante a inicialização do serviço do IBM Cognos.
   c. Na caixa de valor **Número da porta de replicação de RMI**, insira um número de porta.

   Nota: A **Propriedades avançadas** deve ser usada apenas sob orientação do Suporte Técnico IBM.
4. Salve a configuração e reinicie o serviço do IBM Cognos.
5. Repita as etapas para cada instância do Content Manager em seu ambiente.

   Os números de porta especificados não precisam ser idênticos para cada instância do Content Manager.

Usar um armazenamento de objeto externo para a saída de relatório e conjuntos de dados

É possível configurar o Content Manager para armazenar a saída de relatório e os conjuntos de dados em uma unidade local ou um compartilhamento de rede definindo um armazenamento de objeto externo. A saída de relatório está disponível por meio do portal e do IBM Cognos SDK, mas a saída de relatório não está armazenada no banco de dados de armazenamento de conteúdo.

Utilizar um armazenamento de objeto externo para saída de relatório reduz o tamanho do armazenamento de conteúdo e fornece aprimoramentos de desempenho para o Content Manager.

Antes de Iniciar

Certifique-se de fazer o seguinte antes de criar uma conexão de armazenamento de objeto externo.

- Forneça aos computadores do Content Manager acesso ao local do arquivo do armazenamento de objeto externo.
- Forneça a conta de usuário que executa o serviço do IBM Cognos com acesso de leitura e gravação para o local do arquivo.
- Crie o armazenamento de conteúdo.

Procedimento

1. Inicie o IBM Cognos Configuration.
2. Na janela **Explorer**, em **Acesso a Dados** > **Content Manager**, clique com o botão direito no nome do seu **Content Store**, e depois clique em **Novo recurso** > **Armazenamento de Objeto Externo**.

3. Na janela **Novo Recurso - Armazenamento de Objeto Externo**, digite um nome exclusivo para o seu repositório do sistema de arquivos e clique em **OK**.

   É possível ter apenas um armazenamento de objeto externo.
4. Clique no nome para o repositório.
5. Na janela **Armazenamento de Objeto Externo - Propriedades do Recurso**, clique dentro do campo de valor, clique em Editar e quando a janela **Valores de URI** se abrir, digite o caminho para o local do seu sistema de arquivos, em que file-system-path é o caminho completo para um local de arquivo existente.

Tabela 23. Exemplos de Valores de URI

Sistema de Arquivos	Valor da URI

Windows	`file:///c:/file-system-path`
	
	`file://host/share/file-system-path`

UNIX ou Linux	`file:///file-system-path`

Nota: Caminhos relativos, como `file:///../file-system-path` e mapeamentos de unidade não são suportados.

Em uma instalação distribuída, todos os Content Managers devem ter acesso de leitura e gravação para o local do sistema de arquivos. Para melhorar o desempenho ao ler saídas, os Componentes da Camada de Aplicativo, essencialmente o serviço de repositório, deve ter acesso de leitura ao local do sistema de arquivos. Se eles não tiverem acesso de leitura, os pedidos são roteados para o Content Manager ativo.

6. Reinicie o serviço do IBM Cognos.

Verifique o Acesso ao Objeto de Armazenamento Externo

Use o IBM Cognos Configuration para verificar se os componentes do IBM Cognos podem se conectar ao armazenamento de objeto externo.

Procedimento

1. Inicie o IBM Cognos Configuration.
2. No **Explorer** > **Acesso a Dados**, dê um clique direito no nome da sua conexão de armazenamento de objeto externo.
3. Clique em **Teste**.

   O IBM Cognos Configuration verifica o acesso ao local do arquivo de armazenamento de objeto externo.

   Você também pode testar essa conexão clicando com o botão direito em **Configuração Local** e selecionando **Testar**.

Customizando a Impressão no Lado do Servidor para Plataformas UNIX e Linux

A forma na qual o portal do IBM Cognos Analytics manipula a impressão do servidor pode diferir dependendo da plataforma.

Por esse motivo, é possível customizar a forma na qual o portal manipula a impressão de relatórios em formato PDF para plataformas UNIX e Linux configurando o arquivo *rsprintpdf.sh*.

O arquivo *rsprintpdf.sh* não deve ser configurado para servidores de impressão do sistema operacional Microsoft Windows.

Quando um usuário seleciona **Executar com Opções**, altera o **Formato** para PDF, seleciona **Imprimir o Relatório** na seção **Entrega** e, em seguida, especifica formatos adicionais por meio de **opções avançadas**, como orientação Paisagem, tamanho de papel A4 ou um **Hora e Modo** para executar o relatório, podem ocorrer problemas ao imprimir em um servidor de impressão UNIX ou Linux. A saída pode não ser criada ou pode aparecer truncada ou com a orientação incorreta.

Procedimento

1. Abra o arquivo *rsprintpdf.sh* localizado no diretório *install_location/bin directory*.
2. Em um editor de texto, customize a seção específica para a sua plataforma do servidor de impressão, por exemplo, AIX ou Linux.
3. Use a informações a seguir para a customização. A informações é transmitida ao script *rsprintpdf.sh* pelo processo do servidor como as opções da linha de comandos.

Tabela 24. Opções de customização para a impressão de relatórios em formato PDF

Opção	Nome	Descrição
-p	impressora	Especifica a fila de impressão. Se nenhuma fila de impressão for especificada, a fila padrão será usada.
-o	orientação	Especifica a orientação da página de um arquivo, como retrato ou paisagem. Se nenhuma orientação for especificada, a orientação retrato será usada.
-m	Mídia	Especifica o tamanho da mídia de saída, como tamanho carta ou A4. Se a mídia, a altura e a largura não forem especificadas, a bandeja de papel padrão será usada.
-h	Altura	Para tamanhos de página customizados. Especifica a altura da página, em pontos. Só será válida se especificada com a opção -w, sem a opção -m.
-w	largura	Para tamanhos de página customizados. Especifica a largura da página, em pontos. Só será válida se especificada com a opção -h, sem a opção -m.
-L	Arquivo de log	Especifica um caminho para um arquivo especificado pelo usuário para a criação de log das mensagens de erro. O nome de arquivo padrão para o arquivo de log é *rsprintpdf.errors.log*.

4. **Dica**: mantenha uma cópia do arquivo *rsprintpdf.sh* para o caso de substituição em uma atualização de software futura.

Alterar o Banco de Dados de Notificação

Por padrão, o servidor de notificações usa o mesmo banco de dados que o Content Manager usa para o armazenamento de conteúdo. É possível usar um banco de dados separado para notificações em situações em que se executa um grande volume de relatórios em lote e e-mails.

Usar um banco de dados separado para notificações compreende as seguintes tarefas:

- Criando um banco de dados de notificação.

Para IBM Db2, Oracle e Microsoft SQL Server, use o mesmo procedimento usado ao criar o banco de dados de armazenamento de conteúdo. Utilize as instruções em "Diretrizes para Criar o Armazenamento de Conteúdo" na página 8.

Nota: Se estiver usando o Db2, não será possível gerar um script para criar o banco de dados de notificação da mesma maneira que o armazenamento de conteúdo.

Para o Db2 on z/OS, use as instruções em "Configurações sugeridas para criar um banco de dados de notificação no IBM Db2 on z/OS".

- Configurando a conectividade do banco de dados.

  É possível usar o mesmo procedimento usado para configurar a conectividade do banco de dados do armazenamento de conteúdo, "Configure a conectividade do banco de dados para o banco de dados de armazenamento de conteúdo." na página 66.
- Alterando as propriedades da conexão para o banco de dados de notificação.

  Utilize as instruções em "Alterar as propriedades de conexão para o banco de dados de notificação" na página 176.

Configurações sugeridas para criar um banco de dados de notificação no IBM Db2 on z/OS

O banco de dados criado para o banco de dados de notificação deve conter as definições de configuração especificadas.

Para garantir uma instalação com sucesso, siga as seguintes diretrizes ao criar o banco de dados de notificação.

Use a lista de verificação a seguir para ajudá-lo a configurar o banco de dados de notificação no Db2 on z/OS.

__ • Crie uma instância do banco de dados, um grupo de armazenamento e uma conta de usuário para o banco de dados de notificação.

  O usuário deve ter permissões para criar e excluir tabelas no banco de dados.

  O IBM Cognos Analytics usa as credenciais da conta do usuário para se comunicar com o servidor de banco de dados.

__ • Certifique-se de reservar um pool de buffer com um tamanho de página de 32 k e um segundo com um tamanho de página de 4 k para a instância do banco de dados.

__ • Os administradores devem executar um script para criar tablespaces para manter objetos grandes e outros dados para o banco de dados de notificação a fim de usar esses tablespaces.

  Para obter mais informações sobre como executar o script, consulte "Criando espaços de tabela para um banco de dados de notificação no IBM Db2 for z/OS" na página 176.

__ • O administrador do banco de dados deve fazer backup regularmente dos bancos de dados do IBM Cognos Analytics regularmente, porque eles contêm os dados do IBM Cognos.

  Para garantir a segurança e integridade dos bancos de dados, proteja-os de acesso não autorizado ou inadequado.

Criando espaços de tabela para um banco de dados de notificação no IBM Db2 for z/OS

Se você estiver usando o Db2 for z/OS, um administrador de banco de dados deverá executar scripts para criar um conjunto de espaços de tabelas necessário para o banco de dados de notificação. Os scripts devem ser alterados para substituir os parâmetros de espaço reservado com os adequados a seu ambiente.

Certifique-se de que você usa as convenções de nomenclatura para o Db2 for z/OS. Por exemplo, todos os nomes de parâmetros devem iniciar com uma letra e o comprimento não deve exceder 6 caracteres. Para obter mais informações, consulte o Db2 Knowledge Center.

Procedimento

1. Conecte-se ao banco de dados como um usuário com privilégios para criar e arrastar tablespaces e para permitir a execução de instruções SQL.
2. Para criar os espaços de tabela de notificação, acesse o diretório *install_location*/configuration/schemas/delivery/zosdb2.
   a. Faça uma cópia de backup do arquivo de script NC_TABLESPACES.sql e salve o arquivo em outro local.
   b. Abra o arquivo de script NC_TABLESPACES.sql original e use a tabela a seguir para ajudá-lo a substituir os parâmetros de marcador pelos parâmetros apropriados para seu ambiente.

Tabela 25. Nomes e descrições de parâmetros de espaços de tabela para o banco de dados de notificação do Db2 on z/OS

Nome do parâmetro	Descrição
NCCOG	Especifica o nome do banco de dados de notificação.
DSN8G810	Especifica o nome do grupo de armazenamento.
BP32K	Especifica o nome do pool de buffer.

   Nem todos os parâmetros listados estão no script, mas alguns podem ser incluídos no futuro.
   c. Salve e execute o script.
   Por exemplo,
   ```
   db2 -tvf NC_TABLESPACES.sql
   ```
   d. Abra o arquivo de script NC_CREATE_DB2.sql e substitua o parâmetro de marcador NCCOG pelo nome do banco de dados de notificação.
   e. Salve o script.
   Os serviços de tarefa e monitor de programação executarão o script automaticamente. No entanto, você mesmo pode executá-lo.

Alterar as propriedades de conexão para o banco de dados de notificação

Após criar uma banco de dados separado para notificação, você deve configurar componentes do IBM Cognos para usar o novo banco de dados.

É necessário configurar todos os Content Managers e Application Tier Components para utilizar o mesmo banco de dados de notificação.

Procedimento

1. Em cada local em que o Content Manager ou Componentes da Camada de Aplicativos estão instalados, inicie o IBM Cognos Configuration.
2. Na janela **Explorer**, em **Acesso a dados**, clique em **Notificação**.
3. Identifique o banco de dados usado para notificação:
   - Na janela Explorer, clique com o botão direito do mouse em **Notificação** e selecione **Novo Recurso** > **Banco de Dados**.
   - Digite um nome para o recurso do banco de dados.
   - Selecione o tipo de banco de dados do menu suspenso.
   - Clique em **OK**.
4. Na janela **Propriedades**, insira os valores para o recurso de banco de dados de notificação.
5. No menu **Arquivo**, clique em **Salvar**.
6. Teste a notificação. Na janela **Explorer**, clique com o botão direito em **Notificação** e clique em **Testar**.

   Esse procedimento testa a conexão com o banco de dados e do servidor de correio.

   Se o banco de dados de armazenamento de conteúdo estava sendo usado para notificação, as programações serão replicadas nas tabelas do novo banco de dados de notificação.

Resultados

Verifique se os valores usados para identificar o recurso do banco de dados de notificação são os mesmos em todos os computadores com Content Manager e Application Tier Components. Para usar o banco de dados de notificação padrão, não é necessário editar os valores na janela **Propriedades**.

Mude a Conformidade Padrão de Segurança para os Armazenamentos Confiáveis do IBM Cognos

Por padrão, os armazenamentos confiáveis do IBM Cognos usados para comunicações de SSL incluem somente certificados que são qualificados para o padrão NIST SP800-131a. Você pode alterar os certificados disponíveis para você utilizando o ThirdPartyCertificateTool.

Você pode incluir padrões não NIST SP800-131a e também pode remover os padrões não NIST SP800-131a que tiver incluído.

Restaure Certificados Padrão Não NIST SP800-131a para Armazenamentos Confiáveis do IBM Cognos

Por padrão, os armazenamentos confiáveis do IBM Cognos incluem somente certificados de autoridade de certificação (CA) qualificados para o padrão NIST SP800-131a. Se utilizar outros certificados, como os certificados de CA SHA1 ou 1024-bit, você deve incluir esses certificados no armazenamento confiável individualmente. Ou, você inclui esses certificados do armazenamento confiável do JRE que estiver utilizando com o comando de restauração ThirdPartyCertificateTool.

Dica: Os exemplos neste tópico usam a senha padrão, **NoPassWordSet**. Se você mudar a **Senha do keystore** e a senha **Configurações da autoridade de certificação** no IBM Cognos Configuration, certifique-se de usar a senha que você configurou.

Antes de Iniciar

Nos sistemas operacionais UNIX ou Linux, certifique-se de configurar uma variável de ambiente JAVA_HOME antes de usar o `ThirdPartyCertificateTool`.

Em instalações do Microsoft Windows, é possível executar a ferramenta com o `-java:local` para usar o JRE que é fornecido com a instalação. Por exemplo,

```
ThirdPartyCertificateTool.bat -java:local -R
```

Procedimento

1. Acesse o diretório `install_location/bin`.
2. Restaure os certificados padrão não NIST SP800-131a digitando o seguinte comando:

   Nos sistemas operacionais UNIX ou Linux, digite

   ```
   ThirdPartyCertificateTool.sh -R -p NoPassWordSet
   ```

   Nos sistemas operacionais Windows, digite

   ```
   ThirdPartyCertificateTool.bat -R -p NoPassWordSet
   ```

Remova Certificados Padrão Não NIST SP800-131a dos Armazenamentos Confiáveis do IBM Cognos

Se você tiver incluído certificados não NIST SP800-131a nos armazenamentos confiáveis do IBM Cognos, como certificados CA SHA1 ou 1024-bit, é possível remover esses certificados com o ThirdPartyCertificateTool.

Dica: Os exemplos neste tópico usam a senha padrão, **NoPassWordSet**. Se você mudar a **Senha do keystore** e a senha **Configurações da autoridade de certificação** no IBM Cognos Configuration, certifique-se de usar a senha que você configurou.

Antes de Iniciar

Nos sistemas operacionais UNIX ou Linux, certifique-se de configurar uma variável de ambiente JAVA_HOME antes de usar o `ThirdPartyCertificateTool`.

Em instalações do Microsoft Windows, é possível executar a ferramenta com o `-java:local` para usar o JRE que é fornecido com a instalação. Por exemplo,

```
ThirdPartyCertificateTool.bat -java:local -N
```

Procedimento

1. Acesse o diretório `install_location/bin`.
2. Digite o seguinte comando:

   Nos sistemas operacionais UNIX ou Linux, digite

   ```
   ThirdPartyCertificateTool.sh -N -p NoPassWordSet
   ```

   Nos sistemas operacionais Windows, digite

   ```
   ThirdPartyCertificateTool.bat -N -p NoPassWordSet
   ```

Configurando Componentes do IBM Cognos para Usar Outra Autoridade de Certificação

Por padrão, os componentes do IBM Cognos Analytics usam seu próprio serviço de autoridade de certificação (CA) para estabelecer a raiz de confiança na infraestrutura de segurança do IBM Cognos. No entanto, é possível configurar os componentes do IBM Cognos para usar um certificado de outra autoridade de certificação, como iPlanet ou Microsoft.

Para usar outro certificado CA, você deve usar o processo a seguir:

1. "Criar Arquivos Certificate Signing Request (CSR)" na página 181.

   Parte dessa tarefa requer que você submeta os CSRs para a autoridade de certificação e gere os certificados. Para obter mais informações sobre esse processo, consulte a documentação do CA.
2. "Importar os Certificados CA nos Componentes do IBM Cognos" na página 182
3. "Configurar componentes do IBM Cognos para usar certificados gerados por sua CA" na página 183.

Comandos e exemplos de ThirdPartyCertificateTool

Algumas tarefas usam uma ferramenta de linha de comandos nomeada `ThirdPartyCertificateTool`. As tabelas a seguir listam as opções para essa ferramenta de linha de comandos.

Comandos ThirdPartyCertificateTool

Tabela 26. Modo principal de operação

Comando	Descrição
-c	Cria uma certificate signing request (CSR).
-i	Importa um certificado.
-E	Exporta um certificado.

Tabela 27. Modificadores de operação

Comando	Descrição
-e	Trabalhe com a identidade de criptografia.
-T	Trabalhe com o armazenamento confiável (usado apenas com **-i** e **-E**).

Tabela 28. Sinalizadores de Informações

Comando	Descrição
-d	Nome distinto (DN) a ser usado para o certificado.
-r	Local do arquivo de certificado ou CSR (depende do modo).
-t	Arquivo de cadeia da autoridade de certificação. Pode ser PEM, cadeia de certificado de autoridade de certificação PKCS#7 ou certificado de autoridade de certificação de formato DER único.
-p	Senha do keystore. Se **-p** não for incluído, **NoPassWordSet** será usado como uma senha padrão.
-a	Algoritmo de par de chaves: **RSA**. **RSA** é o valor padrão.

Tabela 28. Sinalizadores de Informações (continuação)

Comando	Descrição
-P	Cria um keystore de CA que inclui as autoridades de certificação confiáveis pelo atual JRE.
-N	Configura o armazenamento confiável da CA para usar a norma NIST SP800-131a.
-R	Restaura os certificados não NIST SP800-131a de volta para o armazenamento confiável.

Os valores de amostra da tabela a seguir são usados:

Tabela 29. Valores de Amostra

Propriedade	Valor
DN de certificado de criptografia	Um valor exclusivo, formatado como: `CN=EncryptCert,O=MyCompany,C=CA`
Senha do keystore	A senha padrão: NoPassWordSet Esse valor deve corresponder às senhas no IBM Cognos Configuration em **Segurança** > **Criptografia** > **Cognos**. Se você alterar os valores padrão para **Senha de armazenamento de chaves de assinatura**, **Senha de armazenamento de chaves de criptografia** e **Senha de armazenamento de chaves de Autoridade de Certificação**, certifique-se de usar as senhas que você configurou.

Exemplos de ThirdPartyCertificateTool

Tabela 30. Exemplos de ThirdPartyCertificateTool

Exemplo	Comando
Para criar um novo par de chaves de criptografia e CSR PKCS#10:	`ThirdPartyCertificateTool.bat -c -e -d cn=Me,o=MyCompany,c=CA -r crypto.csr -a RSA -p password`
Para importar o certificado de criptografia gerado pela CA de terceiro e a cadeia de certificados de autoridade de certificação PKCS#7:	`ThirdPartyCertificateTool.bat -i -e -r crypto.cer -p password -t cacert.p7b`
Para importar o certificado de criptografia gerado pela CA de terceiro e a cadeia de certificados de autoridade de certificação PEM:	`ThirdPartyCertificateTool.bat -i -e -r crypto.cer -p password -t cacert.pem`
Para incluir o `ca.cer` como um certificado confiável:	`ThirdPartyCertificateTool.bat -i -T -r ca.cer -p password -t cacert.cer`
Para exportar o certificado de criptografia para o `crypto.cer`:	`ThirdPartyCertificateTool.bat -E -e -r crypto.cer -p password`
Para exportar o certificado de autoridade de certificação do IBM Cognos para o `ca.cer` (quando NÃO estiver usando uma CA de terceiro):	`ThirdPartyCertificateTool.bat -E -T -r ca.cer -p password`

Tabela 30. Exemplos de ThirdPartyCertificateTool (continuação)

Exemplo	Comando
Para remover todos os certificados de autoridade de certificação não NIST SP800-131a e configurar o armazenamento confiável da CA no padrão NIST SP800-131a:	`ThirdPartyCertificateTool.bat -N -p password`
Para restaurar os certificados SP800-131a não NIST de JRE no armazenamento confiável da CA:	`ThirdPartyCertificateTool.bat -R -p password`

Criar Arquivos Certificate Signing Request (CSR)

Para obter um certificado de uma autoridade de certificação (CA), deve-se primeiramente gerar arquivos de solicitação de assinatura de certificado (CSR) para a chave de criptografia do keystore do IBM Cognos. A CA usa esse arquivo para produzir um certificado de criptografia e um certificado de CA que você importa no seu keystore.

Dica: Os exemplos neste tópico usam a senha padrão, **NoPassWordSet**. Se você mudar a **Senha do keystore** e a senha **Configurações da autoridade de certificação** no IBM Cognos Configuration, certifique-se de usar a senha que você configurou.

Antes de Iniciar

Nos sistemas operacionais UNIX ou Linux, certifique-se de que você configurou uma variável de ambiente JAVA_HOME antes de utilizar o `ThirdPartyCertificateTool`.

Em instalações do Microsoft Windows, é possível executar a ferramenta com o `-java:local` para usar o JRE que é fornecido com a instalação. Por exemplo,

```
ThirdPartyCertificateTool.bat -java:local -c -d ...
```

Procedimento

1. Faça backup de seus dados de chave:
   a. Acesse o diretório *install_location*\configuration.
   b. Faça backup do arquivo `cogstartup.xml` em um local seguro.
   c. Faça backup dos conteúdos do seguinte diretório para um local seguro: *install_location*\configuration\certs
2. Acesse o diretório *install_location*\bin.
3. Crie o certificado assinando a solicitação para a chave de criptografia digitando o seguinte comando:

   No UNIX ou Linux, digite

   ```
   ThirdPartyCertificateTool.sh -c -e -d "CN=EncryptCert,O=MyCompany,C=CA"
   -r encryptRequest.csr -p NoPassWordSet
   ```

   No Windows, digite

   ```
   ThirdPartyCertificateTool.bat -c -e -d "CN=EncryptCert,O=MyCompany,C=CA"
   -r encryptRequest.csr -p NoPassWordSet
   ```

   O valor do nome distinto (DN) no comando (`"CN=SignCert,O=MyCompany,C=CA"`) identifica exclusivamente a instalação do IBM Cognos. Os atributos usados refletem uma estrutura hierárquica em sua organização.

A senha que você insere para essa chave deve ser usada novamente ao importar o certificado e novamente no IBM Cognos Configuration.

É possível ignorar com segurança todos os avisos sobre criação de log.

O comando cria o arquivo `CAMKeystore` no diretório `certs`, configura a senha especificada, cria um par de chaves, armazena-o no keystore e exporta o arquivo `encryptRequest.csr` no diretório *`install_location`*`\bin`.

4. Copie o arquivo `encryptRequest.csr` para um diretório que seja acessível à autoridade de certificação.
5. Insira o arquivo `encryptRequest.csr` na autoridade de certificação e gere o certificado.

   A autoridade de certificação produz um certificado-chave de criptografia e um certificado de autoridade de certificação.

   Importante: Os certificados gerados pelo seu CA devem estar no formato PEM (ASCII com odificação Base-64).

Resultados

Agora é possível importar os certificados gerados nos componentes do IBM Cognos.

Importar os Certificados CA nos Componentes do IBM Cognos

Após ter obtido os certificados do CA, será necessário importá-los para os componentes do seu IBM Cognos.

Você deve importar os certificados em cada computador em que existam componentes do IBM Cognos instalados; incluindo o Content Manager, os Componentes da Camada de Aplicativo, o gateway e os componentes de modelagem.

Dica: Os exemplos neste tópico usam a senha padrão, **`NoPassWordSet`**. Se você mudar a **Senha do keystore** e a senha **Configurações da autoridade de certificação** no IBM Cognos Configuration, certifique-se de usar a senha que você configurou.

Antes de Iniciar

Nos sistemas operacionais UNIX ou Linux, certifique-se de que você configurou uma variável de ambiente JAVA_HOME antes de utilizar o `ThirdPartyCertificateTool`.

Em instalações do Microsoft Windows, é possível executar a ferramenta com o `-java:local` para usar o JRE que é fornecido com a instalação. Por exemplo,

```
ThirdPartyCertificateTool.bat -java:local -c -d ...
```

Procedimento

1. Crie uma cópia do certificado de criptografia e nomeie-o `encryptCertificate.cer`.
2. Crie uma cópia do certificado CA raiz e nomeie-o como `ca.cer`.
3. Copie os arquivos `encryptCertificate.cer` e `ca.cer` no diretório *`install_location`*`/bin`.

4. Importe o certificado de criptografia no armazenamento de chaves de criptografia do IBM Cognos digitando o seguinte comando:

   Nos sistemas operacionais UNIX ou Linux, digite

   ```
   ThirdPartyCertificateTool.sh -i -e -r encryptCertificate.cer -p
   NoPassWordSet -t ca.cer
   ```

   Nos sistemas operacionais Windows, digite

   ```
   ThirdPartyCertificateTool.bat -i -e -r encryptCertificate.cer -p
   NoPassWordSet -t ca.cer
   ```

   Importante: Assegure-se de usar a senha inserida quando exportou a chave de criptografia na tarefa anterior.

   É possível ignorar com segurança todos os avisos sobre criação de log.

   O comando lê os arquivos `encryptCertificate.cer` e `ca.cer` no diretório *`install_location`*`\bin` e importa os certificados de ambos os arquivos no arquivo `CAMKeystore` no diretório `certs` usando a senha especificada.
5. Importe o certificado CA no armazenamento confiável do IBM Cognos digitando o seguinte comando:

   Nos sistemas operacionais UNIX ou Linux, digite

   ```
   ThirdPartyCertificateTool.sh -i -T -r ca.cer -p NoPassWordSet
   ```

   Nos sistemas operacionais Windows, digite

   ```
   ThirdPartyCertificateTool.bat -i -T -r ca.cer -p NoPassWordSet
   ```

   O comando lê o arquivo `ca.cer` e importa o conteúdo no arquivo `CAMKeystore` no diretório `certs` usando a senha especificada.

Resultados

Agora é possível configurar os componentes do IBM Cognos para usar os certificados CA.

Configurar componentes do IBM Cognos para usar certificados gerados por sua CA

Após ter importado os certificados CA, use o IBM Cognos Configuration para configurar cada computador em que um componente do IBM Cognos esteja instalado para usar o certificado.

Nota: Certifique-se de que os locais e senhas de armazenamento de chaves no IBM Cognos Configuration correspondam aos digitados na ferramenta de linha de comandos. Por exemplo, se mudar a **Senha do armazenamento de chaves de criptografia** e a **Senha do armazenamento de chaves de Autoridade de Certificação** na Configuração do IBM Cognos, certifique-se de usar a senha que configurou.

Procedimento

1. Inicie o IBM Cognos Configuration.
2. Na janela **Explorer**, em **Segurança** > **Criptografia**, clique em **Cognos**.
3. Clique na caixa **Valor** próxima a **Usar CA de Terceiro** e selecione **True**.

   Quando você configura essa propriedade como verdadeira, todas as propriedades para a autoridade de certificação e nome de identidade são ignoradas.
4. Insira a senha usada para a chave de criptografia na **Senha do armazenamento de chaves de criptografia** e insira o caminho para o **Local do armazenamento**

de chaves de criptografia. Se os mesmos valores foram usados nos exemplos, nas tarefas anteriores, não será necessário alterar o caminho.

5. Insira a **Senha do Armazenamento de Chaves da Autoridade de Certificação**.
6. Clique em **Arquivo** > **Salvar**.
7. Reinicie os serviços do IBM Cognos.

Configurando o Protocolo SSL para Componentes do IBM Cognos

É possível usar o protocolo Secure Sockets Layer (SSL) para a comunicação entre os componentes do IBM Cognos em instalações distribuídas e de único servidor.

Conectores do IBM WebSphere Liberty Profile

Se o URI do dispatcher interno for prefixado com http, mas o URI do dispatcher externo for prefixado com https, ou vice-versa, os conectores não SSL Liberty HTTP/1.1 e SSL Liberty HTTP/1.1 serão ativados no arquivo `server.xml`.

Se as URIs do dispatcher interno e externo usarem protocolos e portas diferentes, a porta do dispatcher interno será acessível apenas para os componentes no computador local. O URI do dispatcher interno também deve especificar o localhost.

Instalações de Computador Único

Em uma instalação de computador único, se você não estiver usando SSL, deverá parar o serviço antes de alterar o protocolo para https. Após salvar a configuração com as definições de SSL, você poderá reiniciar os serviços.

Instalações Distribuídas

Na instalação distribuída, você deve configurar primeiro o computador do Content Manager ativo padrão para usar o protocolo SSL e iniciar os serviços nesse computador antes de configurar os componentes da Camada do Aplicativo e o gateway para usar o SSL.

Incluir um Computador em uma Instalação

Se adicionar um computador a um ambiente com o SSL ativado, aparecerá um aviso para aceitar temporariamente a confiança para um certificado ao salvar as configurações. Aceitar o certificado temporário permitirá que a confiança permanente seja estabelecida com os componentes existentes.

Incluir um Componente em um Computador

Se incluir um componente em uma instalação já configurada no SSL, a confiança serSSL, a confiança para os certificados SSL será herdada a partir dos componentes existentes. Se você incluir o componente em um local diferente no mesmo computador, mas em um ambiente já configurado para SSL, será solicitado que aceite temporariamente a confiança para um certificado ao salvar a configuração. Aceitar o certificado temporário permitirá que a confiança permanente seja estabelecida com os componentes existentes.

Configurando SSL para componentes do IBM Cognos

Para componentes do IBM Cognos, é possível usar SSL para conexões internas, conexões externas ou as duas.

Se você configurar SSL apenas para conexões internas, os componentes do IBM Cognos no computador local se comunicarão usando esse protocolo. O dispatcher recebe conexões seguras em uma porta diferente das solicitações de HTTP remotas. Desta forma, é necessário configurar dois URIs de dispatcher.

Se você configurar SSL apenas para conexões externas, as comunicações de componentes IBM Cognos remotos com o computador local usarão o protocolo SSL. É necessário configurar o dispatcher para procurar por solicitações seguras e remotas em uma porta diferente em relação a solicitações locais, HTTP. Também é necessário configurar os URIs do Content Manager e do dispatcher para aplicativos externos usarem o mesmo protocolo e porta que o dispatcher local.

Se configurar o SSL para todas as conexões, o dispatcher pode usar a mesma porta para conexões internas e externas. Da mesma forma, se não usar o SSL para a comunicação local ou remota, o dispatcher pode usar a mesma porta para todas as comunicações.

Por padrão, os componentes do IBM Cognos Analytics usam uma autoridade de certificação (CA) interna para estabelecer a raiz de confiança na infraestrutura de segurança do IBM Cognos. Isso se aplica às duas conexões, SSL e não SSL. Se desejar usar certificados gerenciados por outro serviço, consulte "Configurando Componentes do IBM Cognos para Usar Outra Autoridade de Certificação" na página 179.

Na instalação distribuída, você deve configurar primeiro o computador do Content Manager ativo padrão para usar o protocolo SSL e iniciar os serviços nesse computador antes de configurar o computador de Componentes da camada de aplicativos.

Procedimento

1. Inicie o IBM Cognos Configuration.
2. Na janela **Explorer**, clique em **Ambiente**.
3. Na janela **Propriedades**, digite os valores apropriados para os valores da URI.

   Importante: Para configurações HTTPS/SSL, certifique-se de usar um nome completo do host para URIs. Além disso, na janela do Explorer, em **Segurança** > **Criptografia** > **Cognos** > **Nome da identidade**, mude o **Nome comum do servidor** de CAMUSER para o nome completo do domínio do servidor.

   - Para configurar o SSL apenas para conexões internas, insira `https` e um número da porta para a comunicação SSL na propriedade **URI do Dispatcher Interno**.

     Para as propriedades **URI do Dispatcher Externo** e **URI do Dispatcher para Aplicativos Externos**, deixe `http` como o protocolo e use o número da porta padrão ou outro número da porta disponível.

     Se você usar o servidor de aplicativos que é fornecido com o IBM Cognos Analytics, a propriedade **URI do dispatcher interno** deverá especificar `localhost`.

     O número da porta nas duas URIs do dispatcher deve ser diferente.
   - Para configurar o SSL apenas para conexões externas, insira `https` e um número da porta para a comunicação SSL nas propriedades **URI do Dispatcher Externo** e **URI do Dispatcher para Aplicativos Externos**.

     Para a propriedade **URI do Dispatcher Interno**, deixe `http` como o protocolo e use o número da porta padrão ou outro número da porta disponível.

Se você usar o servidor de aplicativos que é fornecido com o IBM Cognos Analytics, a propriedade **URI do dispatcher interno** deverá especificar `localhost`.

O número da porta nas duas URIs do dispatcher deve ser diferente.

- Para configurar o SSL para todas as conexões, insira a mesma URI para as propriedades **URI do Dispatcher Interno**, **URI do Dispatcher Externo** e **URI do Dispatcher para Aplicativos Externos**. Insira `https` e um número da porta para a comunicação SSL.
- Adicionalmente, é possível inserir `https` e um número da porta para a comunicação SSL na propriedade **URI do Content Manager**.
- Se você instalou o gateway em um computador separado e estiver usando SSL para conexões externas, no IBM Cognos Configuration no computador de gateway, insira `https` e o número da porta para comunicação SSL na propriedade **URIs de dispatcher para gateway**.

4. No menu **Arquivo**, clique em **Salvar**.
5. Reinicie os serviços.

   Em ambiente distribuído, inicie os serviços no computador com Content Manager primeiro, seguido pelos serviços nos computadores dos Componentes da camada de Aplicativos.

Configure a Confiança Compartilhada entre Servidores IBM Cognos e Outros Servidores

Se quiser usar a autoridade de certificação do IBM Cognos e quiser usar SSL para conexões de outros servidores com servidores IBM Cognos, será necessário incluir o certificado do IBM Cognos no armazenamento confiável nos outros servidores.

Nota: Se usar navegadores para se conectar aos componentes do IBM Cognos, os navegadores solicitarão automaticamente que os usuários atualizem seus armazenamentos confiáveis.

Se quiser que a conexão entre os servidores IBM Cognos e o outro servidor sejam mutuamente autenticada, você também deverá copiar o certificado da autoridade de certificação no armazenamento confiável para os servidores IBM Cognos.

Se tiver configurado componentes do IBM Cognos para usar outra autoridade de certificação (CA), você não precisará configurar a confiança compartilhada entre o servidor IBM Cognos e os outros servidores.

Copiando o Certificado do IBM Cognos em outro Servidor

A primeira tarefa de inclusão do certificado do IBM Cognos no armazenamento confiável em outros servidores é copiar o certificado no servidor.

Procedimento

1. Acesse o diretório *install_location*/bin.
2. Extraia o certificado do IBM Cognos digitando o seguinte comando:
   - Em sistemas operacionais UNIX ou Linux, digite

     `ThirdPartyCertificateTool.sh -E -T -r` *destination_file* `-p` **`NoPassWordSet`**
   - Nos sistemas operacionais Microsoft Windows, digite

     `ThirdPartyCertificateTool.bat -E -T -r` *destination_file* `-p` **`NoPassWordSet`**
3. Importe o certificado para o armazenamento confiável em seu servidor.

Para obter informações em como atualizar o armazenamento confiável, consulte a documentação de seu servidor.

Copiando o Certificado CA em Servidores IBM Cognos

Após copiar o certificado do IBM Cognos em outros servidores, copie o certificado da autoridade de certificação no servidor IBM Cognos.

Procedimento

1. Copie o certificado da autoridade de certificação em um local seguro no servidor IBM Cognos.

   Verifique se a autoridade de certificação CA está no formato X.509 codificado na base 64.
2. Importe a autoridade de certificação CA digitando o seguinte comando:
   - Em sistemas operacionais UNIX ou Linux, digite o seguinte:

     `ThirdPartyCertificateTool.sh -T -i -r` *`CA_certificate_file`* `-p` **`NoPassWordSet`**
   - Nos sistemas operacionais Microsoft Windows, digite

     `ThirdPartyCertificateTool.bat -T -i -r` *`CA_certificate_file`* `-p` **`NoPassWordSet`**

Selecionar e Classificar Conjuntos de Cifras para Secure Socket Layer

Uma conexão SSL começa com uma negociação onde o cliente e o servidor apresentam uma lista de conjuntos de códigos suportados em uma sequência prioritária. O conjunto de códigos fornece a qualidade de proteção para a conexão. Ele contém algoritmos criptográficos, de autenticação, hash e de troca de chaves. O protocolo SSL seleciona o conjunto de prioridade mais alta que o cliente e o servidor suportam.

Uma lista de conjuntos de códigos para SSL é fornecida. É possível eliminar conjuntos de códigos que não correspondem a exigências e então atribuir uma prioridade, ou preferência, aos conjuntos de códigos restantes. Os conjuntos de códigos selecionados são apresentados por ordem de prioridade para as partes do cliente e servidor da negociação. No mínimo um dos conjuntos de códigos selecionados entre as plataformas do cliente e servidor devem corresponder.

A lista de conjuntos de códigos suportados é gerada dinamicamente em cada computador e depende do Java Runtime Environment (JRE) ou se você tem outro software criptográfico instalado no computador. Se foram feitas mudanças em um computador, como atualização no JRE ou a instalação de um software que atualizou o JRE, isto pode afetar os conjuntos de códigos suportados nesse computador. Se não possuir mais um conjunto de códigos suportado que corresponda a outros computadores em seu ambiente, pode ser necessário alterar o JRE no computador para corresponder aos outros computadores em seu ambiente.

Procedimento

1. Inicie o IBM Cognos Configuration.
2. Na janela **Explorer**, clique em **Criptografia** > **Cognos**.
3. Na janela **Propriedades**, clique na coluna **Valor** na propriedade **Conjuntos de códigos com suporte**.
4. Clique no ícone de edição  .

- Para mover um conjunto de códigos para a lista **Valores atuais**, clique na caixa de seleção na lista **Valores disponíveis** e em **Adicionar**.
- Para mover um conjunto de códigos para cima ou para baixo na lista **Valores atuais**, clique na caixa de seleção e depois nas setas para cima ou para baixo.
- Para remover um conjunto de códigos da lista **Valores atuais**, clique na caixa de seleção e em **Remover**.

5. Clique em **OK**.
6. No menu **Arquivo**, clique em **Salvar**.

Usar o protocolo secure sockets layer (SSL) para conexões com o banco de dados no IBM Cognos Configuration

É possível configurar o IBM Cognos Analytics para usar o protocolo SSL (Secure Sockets Layer) para a comunicação com os bancos de dados usados pelo IBM Cognos Analytics, incluindo os bancos de dados de armazenamento de conteúdo, de notificação e de criação de log.

O SSL deve ser ativado no servidor de banco de dados e os clientes do banco de dados devem ser configurados para usar conexões SSL com o servidor de banco de dados antes de ativá-lo no IBM Cognos Configuration.

O suporte do SSL está disponível para todos os bancos de dados suportados, exceto para o IBM Db2 for z/OS.

Db2

É possível usar o SSL para o Fix Pack 2 do Db2 versão 9.1 e versões mais recentes.

Para obter informações sobre como configurar o Db2 para conexões SSL, consulte a documentação para sua versão do Db2.

Por exemplo, para a versão 10.5, consulte a Documentação do IBM Db2 versão 10.5 (pic.dhe.ibm.com/infocenter/db2luw/v10r5/index.jsp?topic=%2Fcom.ibm.db2.luw.admin.sec.doc%2Fdoc%2Fc0053514.html).

IBM Informix

Para obter informações sobre configurar conexões do IBM Informix for SSL, consulte a documentação para sua versão do IBM Informix.

Por exemplo, para a versão 12.10, consulte a documentação do IBM Informix versão 12.10 (pic.dhe.ibm.com/infocenter/informix/v121/index.jsp?topic=%2Fcom.ibm.sec.doc%2Fids_ssl_001.htm).

Oracle

Para obter informações sobre configurar conexões do Oracle for SSL, consulte a documentação para sua versão do Oracle.

O White Paper SSL com Oracle JDBC Thin Driver (www.oracle.com/technetwork/database/enterprise-edition/wp-oracle-jdbc-thin-ssl-130128.pdf) publicado pela Oracle fornece informações para configurar a SSL para o servidor de banco de dados e o cliente.

Microsoft SQL Server

Para obter informações sobre configurar conexões do Microsoft SQL Server for SSL, consulte a documentação para sua versão do Microsoft SQL Server.

Por exemplo, para a versão 2012, consulte a documentação do Microsoft SQL Server versão 2012 (technet.microsoft.com/en-us/library/bb879949.aspx).

Nota: Após ativar a SSL no servidor de banco de dados, é possível configurar **Criptografia SSL Ativada** para **True** no IBM Cognos Configuration.

Usando SSL para conexões com o banco de dados no IBM Cognos Configuration para o Microsoft SQL Server

11.0.5

Para usar secure sockets layer (SSL) para conexões com o banco de dados no IBM Cognos Configuration, você deve importar o certificado SSL para o keystore Java e modificar alguns arquivos de configuração do IBM Cognos. Para obter informações sobre a configuração do Microsoft SQL Server para conexões SSL, consulte a documentação para sua versão do Microsoft SQL Server.

É possível usar SSL para conexões com o banco de dados no IBM Cognos Configuration, incluindo armazenamento de conteúdo, notificação, bancos de dados de criação de log, Tarefa Manual e Serviços de Anotação e Cognos Mobile.

O driver JDBC da Microsoft **substitui** o driver JSQLConnect para o SQL Server. Da versão 11.0.5 em diante, deve-se fazer o download, na Microsoft, e colocar o novo driver tipo 4 na pasta *install_location*/drivers.

Nota: Há diferentes nomes de arquivo JAR do driver, como sqljdbc4.jar, sqljdbc41.jar e sqljdbc42.jar. Oficialmente, o sqljdbc42.jar suporta JRE8, que é a versão enviada com o Cognos Analytics.

Antes de Iniciar

Assegure-se de ativar a SSL em seu servidor de banco de dados antes de configurar o IBM Cognos para usar a SSL para conexões com o banco de dados.

Assegure-se de exportar o certificado SSL do seu servidor de banco de dados e o tenha disponível no computador em que estiver configurando a conexão com o banco de dados no IBM Cognos Configuration.

Procedimento

1. Se você estiver usando um servidor SQL que está configurado para SSL como o seu banco de dados de armazenamento de conteúdo, siga estas etapas:
   a. Obtenha o certificado da Autoridade de Certificação raiz que emitiu o certificado do seu SQL Server (ou o certificado de servidor autoassinado, se ele não foi emitido por uma Autoridade de Certificação) e copie para o computador no qual o Cognos Analytics está instalado. Por exemplo, copie o arquivo sqlcert.cer para o diretório-raiz c:\sqlcert.cer
   b. Digite cd C:\Program Files\ibm\cognos\analytics\jre\lib\security
   c. Digite, por exemplo, C:\Progra~1\ibm\cognos\analytics\jre\bin\keytool -import -trustcacerts -file "c:\sqlcert.cer" -keystore cacerts -alias SQLCert

2. Edite *install_location*\bin64\startwlp.bat (Windows) ou *install_location*\bin64\startwlp.sh (Linux, UNIX) para incluir as linhas a seguir após a linha `set JVM_ARGS=-Xmx4096m -XX:MaxNewSize=2048m -XX:NewSize=1024m %DEBUG_OPTS%`:

   Windows:

   ```
   set JVM_ARGS="-Dcom.ibm.jsse2.overrideDefaultTLS=true" %JVM_ARGS%
   set JVM_ARGS="-Dcom.ibm.jsse2.sp800-131=strict" %JVM_ARGS%
   ```

   Linux, UNIX:

   ```
   JVM_ARGS=-Dcom.ibm.jsse2.overrideDefaultTLS=true $JVM_ARGS
   JVM_ARGS=-Dcom.ibm.jsse2.sp800-131=strict $JVM_ARGS
   ```

3. Edite *install_location*\bin64\bootstrap_wlp_*os_version*.xml para incluir as linhas a seguir após a linha `<param condName="${java_vendor}" condValue="IBM">-Xscmaxaot4m</param>`:

   Windows:

   ```
   <param>"-Dcom.ibm.jsse2.overrideDefaultTLS=true"</param>
   <param>"-Dcom.ibm.jsse2.sp800-131=strict"</param>
   ```

   Linux, UNIX:

   ```
   <param>-Dcom.ibm.jsse2.overrideDefaultTLS=true</param>
   <param>-Dcom.ibm.jsse2.sp800-131=strict</param>
   ```

4. Edite *install_location*\bin64\cogconfig.bat (Windows) ou *install_location*\bin64\cogconfig.sh (Linux, UNIX) para que inclua as seguintes linhas após a linha `set J_OPTS=%DD_OPTS% %J_OPTS%`:

   Windows:

   ```
   set J_OPTS="-Dcom.ibm.jsse2.overrideDefaultTLS=true" %J_OPTS%
   set J_OPTS="-Dcom.ibm.jsse2.sp800-131=strict" %J_OPTS%
   ```

   Linux, UNIX:

   ```
   JAVA_OPTS=$JAVA_OPTS -Dcom.ibm.jsse2.overrideDefaultTLS=true
   JAVA_OPTS=$JAVA_OPTS -Dcom.ibm.jsse2.sp800-131=strict
   ```

5. Inicie o Cognos Configuration usando o `cogconfig.bat` ou o `cogconfig.sh` modificado na etapa anterior.

   Importante: Deve-se iniciar o IBM Cognos Configuration usando o `cogconfig.bat` (modificado para incluir o keystore e a senha) e não o executável usual (cogconfigw.exe) ou o atalho do menu iniciar.

6. Em **Acesso a Dados**, sob o tipo de conexão com o banco de dados, selecione a conexão com o banco de dados.
7. Selecione **True** para **Criptografia SSL Ativada**.
8. Teste a conexão e salve a configuração.
9. Inicie o Cognos Analytics. Você terá de corresponder o nome do servidor completo no SQL Server Configuration Manager àquele no certificado (por exemplo, `mymachine.canlab.ibm.com` em vez de `localhost`).

Resultados

Importante: Para conexão única (SSO) e autenticação do Windows, é necessário colocar o `sqljdbc_auth.dll` no diretório `bin64`. A autenticação do Windows é uma configuração de conexão única. A seleção no Configuration Manager para o Content Manager é denominada **Banco de dados Microsoft SQL Server (Autenticação do Windows)**.

Usando SSL para conexões com o banco de dados no IBM Cognos Configuration para um banco de dados do IBM Db2, Informix

Para usar secure sockets layer (SSL) para conexões com o banco de dados no IBM Cognos Configuration, você deve importar o certificado SSL para o keystore Java e modificar alguns arquivos de configuração do IBM Cognos.

É possível usar a SSL para conexões com o banco de dados no IBM Cognos Configuration, incluindo o armazenamento de conteúdo, notificação e bancos de dados de criação de log.

Antes de Iniciar

Assegure-se de ativar a SSL em seu servidor de banco de dados antes de configurar o IBM Cognos para usar a SSL para conexões com o banco de dados.

Assegure-se de exportar o certificado SSL do seu servidor de banco de dados e o tenha disponível no computador em que estiver configurando a conexão com o banco de dados no IBM Cognos Configuration.

Procedimento

1. Siga a documentação para sua versão do banco de dados a fim de ativar a SSL para o servidor de banco de dados e exporte o certificado SSL.
2. Faça o download de arquivos jar de política de intensidade ilimitada.

   Para IBM JRE, acesse https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=jcesdk (https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=jcesdk) e faça download de `unrestrictedpolicyfiles.zip`. Descompacte os arquivos de políticas em *`install_location`*`/jre/lib/security`.
3. No computador no qual você está configurando a conexão com o banco de dados, importe o certificado SSL com a keytool para o JRE utilizado para o IBM Cognos Analytics. Por exemplo, se estiver usando o JRE fornecido com as instalações do IBM Cognos Analytics em sistemas operacionais Microsoft Windows, execute as seguintes etapas:
   a. Acesse o diretório *`install_location`*`/jre/bin`.
   b. Execute o seguinte comando.

      `keytool -import -file` *`path/filename`* `-keystore` *`keystorename`* `-alias` *`aliasname`*

      Em que *`keystorename`* é um nome para um novo keystore e *`aliasname`* é um alias escolhido para o certificado.
   c. Insira uma senha para sua keystore. Se estiver incluindo o certificado em um keystore existente, insira a senha do keystore. Se estiver criando um novo keystore, insira uma senha para o novo keystore.

   Importante: O certificado SSL deve ser importado para o keystore do JRE utilizado para o IBM Cognos Analytics.
4. Edite o arquivo `java.security` para incluir o provedor de SSL.
   a. Se estiver usando o JRE fornecido com as instalações do IBM Cognos Analytics em sistemas operacionais Microsoft Windows, acesse o diretório *`install_location`*`/jre/lib/security`. Caso contrário, acesse o diretório `lib/security` do JRE utilizado para o IBM Cognos Analytics.
   b. Abra `java.security` em um editor de texto.
   c. Localize as linhas a seguir no arquivo.

```
ssl.KeyManagerFactory.algorithm=IbmX509
ssl.TrustManagerFactory.algorithm=PKIX
```

d. Inclua as linhas a seguir após as linhas anteriores.

```
ssl.SocketFactory.provider=com.ibm.jsse2.SSLSocketFactoryImpl
ssl.ServerSocketFactory.provider=com.ibm.jsse2.SSLServerSocketFactoryImpl
```

e. Salve e feche o arquivo.

5. Edite o arquivo IBM Cognos `startwlp`. Esse arquivo é usado ao iniciar o IBM Cognos Analytics.
   a. Acesse o diretório *install_location*/bin64.
   b. Abra o arquivo `startwlp.bat` em um editor de texto. Em sistemas operacionais UNIX ou Linux, abra o arquivo `startwlp.sh`.
   c. Localize a linha a seguir no arquivo.

      Windows:

      ```
      set JVM_ARGS=-Dcom.ibm.cognos.disp.useDaemonThreads=true %JVM_ARGS%
      ```

      Linux, UNIX:

      ```
      DISP_OPTS="-Dcom.ibm.cognos.disp.useDaemonThreads=true"
      ```

   d. Inclua as linhas a seguir após as linhas anteriores.

      Windows:

      ```
      set JVM_ARGS=-Dcom.ibm.jsse2.usefipsprovider=true %JVM_ARGS%
      set JVM_ARGS=-Djavax.net.ssl.trustStore=path/keystorename %JVM_ARGS%
      ```

      Linux, UNIX:

      ```
      DISP_OPTS="-Dcom.ibm.jsse2.usefipsprovider=true %DISP_OPTS%"
      DISP_OPTS="-Djavax.net.ssl.trustStore=path/keystorename"
      ```

      Em que *path* é o caminho para o keystore, e *keystorename* é o nome do keystore.

   e. Salve e feche o arquivo.
6. Edite o arquivo `bootstrap_wlp_`*os_version*`.xml`. Esse arquivo é usado ao iniciar o IBM Cognos Analytics como um serviço do IBM Cognos Configuration.
   a. Acesse o diretório *install_location*/bin64.
   b. Abra o arquivo `bootstrap_wlp_`*os_version*`.xml` em um editor de texto.
   c. Inclua as seguintes linhas no arquivo.

      ```
      <param>"-Dcom.ibm.jsse2.usefipsprovider=true"</param>
      <param>"-Djavax.net.ssl.trustStore=path/keystorename"</param>
      ```

      Em que *path* é o caminho para o keystore, e *keystorename* é o nome do keystore.

   d. Salve e feche o arquivo.
7. Edite o arquivo `cogconfig` do IBM Cognos.
   a. Acesse o diretório *install_location*/bin64.
   b. Abra o arquivo `cogconfig.bat` em um editor de texto. Em sistemas operacionais UNIX ou Linux, abra o arquivo `cogconfig.sh`.
   c. Localize a linha a seguir no arquivo.

      Windows:

      ```
      J_OPTS=%DD_OPTS% %J_OPTS% %DEBUG_OPTS%
      ```

      Linux, UNIX:

      ```
      $JAVA_CMD $JAVA_OPTS CRConfig $*
      ```

   d. Inclua as linhas a seguir após as linhas anteriores.

      Windows:

```
set J_OPTS=-Dcom.ibm.jsse2.usefipsprovider=true %J_OPTS%
set J_OPTS=-Djavax.net.ssl.trustStore=path/keystorename %J_OPTS%
```

Linux, UNIX:

```
JAVA_OPTS="$JAVA_OPTS -Dcom.ibm.jsse2.usefipsprovider=true %JAVA_OPTS%"
JAVA_OPTS="$JAVA_OPTS -Djavax.net.ssl.trustStore=path/keystorename"
```

Em que *path* é o caminho para o keystore, e *keystorename* é o nome do keystore.

e. Salve e feche o arquivo.

8. Inicie o IBM Cognos Configuration usando o arquivo `cogconfig` que você modificou.
   - Em sistemas operacionais Microsoft Windows, clique duas vezes no arquivo `cogconfig.bat` que você modificou.
   - Em sistemas operacionais UNIX ou Linux, execute o arquivo `cogconfig.sh` que você modificou.
9. Em **Acesso a Dados**, sob o tipo de conexão com o banco de dados, selecione a conexão com o banco de dados.

   É possível usar a SSL para conexões com o banco de dados de armazenamento de conteúdo, banco de dados de notificação, banco de dados de criação de log, tarefa manual e bancos de dados de anotação.
10. Selecione **True** para **Criptografia SSL Ativada**.
11. Teste a conexão.
12. Salve sua configuração e reinicie os serviços.

Usando SSL para conexões com o banco de dados no IBM Cognos Configuration para um banco de dados Oracle

Para usar secure sockets layer (SSL) para conexões com o banco de dados no IBM Cognos Configuration, você deve importar o certificado SSL para o keystore Java e modificar alguns arquivos de configuração do IBM Cognos.

É possível usar a SSL para conexões com o banco de dados no IBM Cognos Configuration, incluindo o armazenamento de conteúdo, notificação e bancos de dados de criação de log.

Antes de Iniciar

Assegure-se de ativar a SSL em seu servidor de banco de dados antes de configurar o IBM Cognos para usar a SSL para conexões com o banco de dados.

Procedimento

1. Edite o arquivo IBM Cognos `startwlp`.
   a. Acesse o diretório *install_location*`/bin64`.
   b. Abra o arquivo `startwlp.bat` em um editor de texto. Em sistemas operacionais UNIX ou Linux, abra o arquivo `startwlp.sh`.
   c. Inclua as seguintes linhas no arquivo.

      ```
      set JVM_ARGS=-Doracle.net.ssl_version=3 %JVM_ARGS%
      set JVM_ARGS=-Doracle.net.ssl_client_authentication=false %JVM_ARGS%
      set JVM_ARGS=-Doracle.net.wallet_location=(SOURCE=(METHOD=file)
      (METHOD_DATA=(DIRECTORY=path/client_wallet))) %JVM_ARGS%
      ```

      O parâmetro *path* é o caminho para o diretório de carteira eletrônica do Oracle para o cliente, e o parâmetro *client_wallet* é o nome do diretório de carteira eletrônica para o cliente.

d. Salve e feche o arquivo.

2. Edite o arquivo bootstrap_wlp_*os_version*.xml.

   Esse arquivo é usado ao iniciar o IBM Cognos Analytics como um serviço do IBM Cognos Configuration.

   a. Acesse o diretório *install_location*/bin64.

   b. Abra o arquivo bootstrap_wlp_*os_version*.xml em um editor de texto.

   c. Inclua as seguintes linhas no arquivo.

   ```
   <param>-Doracle.net.ssl_version=3</param>
   <param>-Doracle.net.ssl_client_authentication=false</param>
   <param>-Doracle.net.wallet_location=(SOURCE=(METHOD=file)
   (METHOD_DATA=(DIRECTORY=path/client_wallet)))</param>
   ```

   Os parâmetros Java neste arquivo devem ser iguais aos da etapa 1.

   Dica: O uso de aspas duplas no arquivo bootstrap_wlp_linux38664.xml evita o início do IBM Java e resulta na interrupção e na falha da inicialização do Cognos.

   d. Salve e feche o arquivo.

3. Edite o arquivo cogconfig do IBM Cognos.

   a. Acesse o diretório *install_location*/bin64.

   b. Abra o arquivo cogconfig.bat em um editor de texto. Em sistemas operacionais UNIX ou Linux, abra o arquivo cogconfig.sh.

   c. Inclua as seguintes linhas no arquivo.

   ```
   set J_OPTS=-Doracle.net.ssl_version=3 %J_OPTS%
   set J_OPTS=-Doracle.net.wallet_location=(SOURCE=(METHOD=file)
   (METHOD_DATA=(DIRECTORY=path/client_wallet))) %J_OPTS%
   set J_OPTS=-Doracle.net.ssl_client_authentication=false %J_OPTS%
   ```

   d. Salve e feche o arquivo.

4. Copie os arquivos do driver Oracle a seguir no diretório *install_location*/drivers.

   - jssl-1_1.jar
   - oraclepki.jar
   - osdt_cert.jar
   - osdt_core.jar

5. Inicie o IBM Cognos Configuration.

6. Em **Acesso a dados**, para o tipo de conexão com o banco de dados, selecione a conexão com o banco de dados.

   É possível usar a SSL para conexões com o banco de dados de armazenamento de conteúdo, banco de dados de notificação, banco de dados de criação de log, tarefa manual e bancos de dados de anotação.

   Dica: Assegure-se de que a conexão use o tipo **Banco de dados Oracle (Avançado)**. Se você não selecionar o tipo **Banco de dados Oracle (Avançado)**, exclua a conexão com o banco de dados e crie uma nova que use **Banco de dados Oracle (Avançado)**.

7. Selecione **True** para **Criptografia SSL Ativada**.

8. Teste a conexão.

9. Salve sua configuração e reinicie os serviços.

Protegendo origens de dados JDBC com SSL

Protegendo origens de dados JDBC com SSL

Procedimento

1. Assegure-se de que o Data Server esteja configurado para SSL - fora do ambiente do IBM Cognos Analytics.
2. No Cognos Analytics, assegure-se de que as propriedades URL do JDBC e/ou Conexão da conexão do servidor de dados tenham sido atualizadas para incluir todos os parâmetros necessários conforme a documentação do provedor para ativar o SSL via JDBC. Aqui está um exemplo do parâmetro JDBC URL necessário para quando o Db2 é o servidor de dados: Amostra de conexão do DB2 Data Server
3. Importe os certificados SSL para o armazenamento confiável JRE do IBM Cognos conforme a documentação a seguir (os certificados precisam ser importados para `jre/lib/security/cacerts` e a senha padrão para isso é `changeit`): Importar certificados de CA para componentes do IBM Cognos

Configure conexões da origem de dados JDBC para conexão única usando Kerberos

É possível configurar uma conexão única usando o protocolo Kerberos para conexões de origens de dados JDBC que são usadas para o modo de consulta dinâmica (DQM).

Exceto para Microsoft SQL Server, a autenticação de origem de dados de conexão única é suportada apenas para modo de consulta dinâmica.

11.0.6 O suporte para delegação restrita (uma extensão da Microsoft para Kerberos), permite que um serviço obtenha um chamado para outro serviço em nome do usuário, apresentando o tíquete de serviço do usuário a si próprio. O ticket de serviço é delegado do usuário (Serviço do usuário para Proxy - S4U2Proxy), ou gerado pelo próprio serviço quando o usuário é autenticado por diferentes meios.

Para configurar uma origem de dados para autenticação de conexão única usando Kerberos, deve-se

- Criar um arquivo de inicialização Kerberos.
- Configurar um service principal name (SPN) para a origem de dados do modo de consulta dinâmica.
- Criar um arquivo keytab.
- Configurar um módulo de login Kerberos. Há um novo procedimento alternativo para 11.0.6
- Configure as conexões de origem de dados.

Antes de iniciar, deve-se assegurar que as condições a seguir sejam atendidas:

1. O serviço do IBM Cognos é configurado para conexão única usando um namespace do Microsoft Active Directory.
2. O banco de dados é configurado para usar o protocolo do Kerberos.
3. Os usuários do Active Directory também são configurados no servidor de base de dados.
4. 11.0.6 Se a conexão única for configurada com delegação restrita, verifique a documentação do driver para assegurar que o driver suporte a delegação restrita. Nem todos os drivers que suportam a autenticação Kerberos também suportam delegação restrita.

A consulta dinâmica suporta a delegação restrita Kerberos com os drivers JDBC para Netezza e Cloudera Impala. Essa capacidade requer drivers JDBC das versões a seguir ou mais recentes, as quais foram aprimoradas para receber credenciais GSS.: Netezza 7.2.0.9-P3 e 7.2.1.3-P3 (consulte http://www-01.ibm.com/support/docview.wss?uid=swg21997658 para obter mais informações) e Cloudera Impala 2.5.36

O IBM Cognos Analytics pode ser usado com um ORACLE ou IBM JRE. As solicitações de versões IBM estão localizadas na página ambientes suportados. As pessoas que tentam usar o Cognos Analytics com um IBM JRE e Cloudera Impala JDBC terão que usar o IBM JRE 8.0.3.12 ou mais recente. Consulte https://developer.ibm.com/javasdk/downloads/sdk8/.

Usando autenticação do Kerberos sem conexão única

Se você não configurar o namespace do Active Directory, ainda será possível configurar sua origem de dados para a autenticação do Kerberos. O serviço de consulta do modo de consulta dinâmica interpreta as credenciais fornecidas (nome do usuário e senha) como as credenciais para obter um chamado de concessão de chamado (TGT) a partir do centro de distribuição do Kerberos (Active Directory ou outra implementação do Kerberos). Essas credenciais podem ser fornecidas por meio de uma conexão ou inseridas pelo usuário ao ser solicitado pelas credenciais do banco de dados. Nesse caso, as etapas da configuração são alteradas conforme a seguir:

- Não é necessário registrar um SPN.
- Não é necessário criar um arquivo keytab.
- 11.0.6 **Não** é necessário configurar o Módulo de login Kerberos.

  11.0.0 - 11.0.5 É necessário configurar o Módulo de login Kerberos, mas não é necessário especificar o SPN e a especificação de arquivo keytab.
- É necessário fornecer um arquivo de inicialização Kerberos.

Criando arquivos de inicialização do Kerberos

Deve-se criar um arquivo de inicialização do Kerberos e colocá-lo em um local específico em todos os computadores com os Componentes da Camada de Aplicativos instalados. O arquivo de inicialização do Kerberos `krb5.conf` é usado pela implementação do protocolo do JRE Kerberos.

Para obter mais informações sobre arquivos de inicialização do Kerberos, consulte a Documentação do MIT Kerberos (web.mit.edu/kerberos/krb5-devel/doc/admin/conf_files/krb5_conf.html).

Procedimento

Em todos os computadores em que você possui os Componentes da Camada de Aplicativos instalados, copie o diretório `krb5.conf` file to the `JAVA_HOME/lib/security`.
Em computadores executando UNIX, copie o arquivo `krb5.conf` no diretório `/etc/krb5`.
Em computadores executando Linux, copie o arquivo `krb5.conf` no diretório `/etc`.
Em computadores executando Microsoft Windows, copie o arquivo `krb5.conf` no diretório `C:\winnt` e renomeie o para `krb5.ini`

Criando um SPN para o serviço de consulta

Deve-se criar um service principal name (SPN) para o serviço de consulta usar. O SPN deve ser configurado com um usuário do domínio do Active Directory confiável para delegação.

O SPN deve ser formatado como `spn@REALM`. O valor `spn` é formatado como *`service name/fully qualified domain name`*. E `REALM` é o nome da região configurado no arquivo de inicialização do Kerberos. Por exemplo, se dqm for o nome do serviço, `dqm/myserver.mydomain.com@MYWINDOWSDOMAIN.COM`.

Se o usuário do domínio do Active Directory for denominado dqmuser, o SPN seria registrado usando o comando a seguir:

```
setspn -s dqm/myserver.mydomain.com mywindowsdomain\dqmuser
```

É possível usar os parâmetros **`-L`** e **`-Q`** para verificar se o SPN foi criado corretamente. Por exemplo:

```
setspn -L mywindowsdomain\dqmuser

setspn -Q dqm/myserver.mydomain.com
```

Criando um arquivo keytab

Após a criação do SPN, deve-se criar um arquivo keytab para o serviço. O arquivo keytab permite que o serviço efetue login sem uma senha. O arquivo keytab deverá ser recriado se a senha da conta do serviço mudar.

Procedimento

Use o comando a seguir para criar um arquivo keytab:
`ktpass -out krb5.keytab -princ` *`SPN`* `-mapUser` *`username`* `-mapOp set -pass` *`password`* `-pType KRB5_NT_PRINCIPAL -crypto RC4-HMAC-NT`
Por exemplo,
`ktpass -out krb5.keytab -princ` *`dqm/myserver.mydomain.com@mywindowsdomain.com`* `-mapUser` *`dqmuser@mywindowsdomain`* `-mapOp set -pass` *`password`* `-pType KRB5_NT_PRINCIPAL -crypto RC4-HMAC-NT`

Configurando o módulo de login do Kerberos

Deve-se configurar o módulo de login do Kerberos para permitir que o serviço de consulta do IBM Cognos efetue login no domínio do Active Directory. Para permitir o login no Java Authentication and Authorization Service (JAAS), o pacote requer um arquivo de configuração.

Há dois possíveis procedimentos, dependendo de sua versão do Cognos Analytics.

11.0.6+

Para configurar o módulo de login para Kerberos com conexão única (Active Directory):

1. No Cognos Configuration, selecione o namespace Active Directory em **Segurança** > **Authenticação**.
2. Na propriedade **Nome do principal do serviço DQM**, insira o valor exatamente como está listado no keytab.

   Use o comando **`klist -k <keytab file>`** para localizar o nome do principal.

3. Renomeie o arquivo keytab para `ibmcognosba.keytab` e coloque-e na pasta *install_location*`/configuration`.

O Cognos Analytics criará dinamicamente a configuração de login necessária.

11.0.0+ 11.0.5 Este procedimento ainda pode ser usado em 11.0.6+

Um arquivo de configuração deve ser incluído no arquivo `java.security` no diretório *JRE_HOME*`/lib/security`. Deve-se incluir uma linha como a seguinte no arquivo `java.security`.

```
login.config.url.1=file:///${java.home}/lib/security/jaas.conf
```

Exemplos de configuração do JAAS são fornecidos na instalação do IBM Cognos. Os arquivos de exemplo são nomeados `jaas-ibm.config` e `jaas-oracle.config` e os arquivos estão no diretório *install_location*`\configuration`.

Nos arquivos de exemplo, deve-se substituir os valores a seguir:

- *<principal name>* é o SPN que você criou.
- *<keytab file specification>* é o caminho e o nome do arquivo keytab que você criou.

Se você não estiver usando uma conexão ao banco de dados configurada para autenticação do Kerberos para modelagem, em vez de modificar o arquivo `java.security`, é possível especificar o arquivo de configuração de login do JAAS como um parâmetro de inicialização adicional para o serviço de consulta no IBM Cognos Administration. No IBM Cognos Administration, sob o **Sistema**, expanda seu servidor, selecione **Serviço de Consulta** > **Configurar Propriedades** > **Configurações** e insira o valor nos **Argumentos de JVM Adicional para o serviço de consulta** na forma `-Djava.security.auth.login.config=`*<configuration file>*

Verificando a configuração do Kerberos

Para verificar a configuração do Java Authentication and Authorization Service (JAAS) e o arquivo keytab, é possível executar um comando usando o comando **java** a partir do JRE que o Cognos Analytics estiver usando.

Procedimento

Execute o comando a seguir a partir de *install_location*`/webapps/p2pd/WEB-INF/lib` **java -cp xqeService.jar -Dcom.ibm.security.krb5.Krb5Debug=all -Dcom.ibm.security.jgss.debug=all com.cognos.xqe.util.KerberosSSOLoginHelper**
O utilitário tentará um login usando o arquivo keytab e, no processo, exibirá o resultado da depuração do Kerberos. Ao final, exibirá `Login auxiliar bem-sucedido` ou `Login auxiliar com falha <mensagem de erro>`.

Verificando os recursos do driver JDBC

Independentemente de se a conexão única estiver configurada ou não, o DQM requer que o driver de banco de dados possa criar conexões usando um assunto pré-autorizado. Há um recurso que vem junto à instalação do IBM Cognos Analytics que pode ajudar a testar o driver.

Antes de Iniciar

O utilitário aceita **url**, **uid** e **password** como parâmetros. O driver deve ser instalado na pasta *install_location*/webapps/p2pd/WEB-INF/lib.

Procedimento

Na pasta *install_location*/webapps/p2pd/WEB-INF/lib, usando o comando Java do qual o jre Cognos estiver usando, execute o comando a seguir: **java -cp xqeService.jar;<driver.jar> com.cognos.xqe.util.KerberosConnectionHelper <driver class name> <jdbc url> <user> <password>**
onde:

- O <*driver.jar*> é o arquivo JAR que contém o driver. Se o driver tiver muitos arquivos JAR, será possível especificar "*" para o parâmetro de caminho de classe.
- O <*driver class name*> é o nome de classe usado para carregar o driver.
- O <*jdbc url*> é a URL de conexão JDBC para a origem de banco de dados, incluindo as propriedades específicas do driver para autenticação do Kerberos.
- O <*user*> é o Kerberos principal.
- O <*password*> é a senha do Kerberos principal.

O utilitário tenta se conectar ao banco de dados usando os parâmetros fornecidos e resulta no rastreio de depuração do Kerberos.

Configurando conexões de origem de dados usando o Kerberos

Use as diretrizes neste tópico ao configurar as sequências de conexões para conexões de origem de dados usando conexão única do Kerberos.

Procedimento

1. Na seção Efetuar sign on, selecione **namespace externo** e selecione o namespace Active Directory a partir da lista. Para sequências de conexões de guias dual (Nativa e JDBC), a seção Efetuar sign on está na guia Nativa.
2. No campo **Propriedades de conexão**, especifique `ibmcognos.authentication=java_krb5` e, em seguida, inclua as propriedades requeridas pelo driver JDBC para autenticação do Kerberos, se houver. Para conexões de origem de dados com guias dual (Nativa e JDBC), este campo está na guia **JDBC** e é chamada de **Parâmetros de Conexão JDBC**.

   Se o IBM Cognos Analytics estiver instalado em um computador que está executando sistemas operacionais Microsoft Windows, não será necessário especificar `ibmcognos.authentication=java_krb5` para origens de dados do Microsoft SQL Server e Teradata.
3. Teste a conexão de origem de dados.

Exemplo

A seguir estão exemplos de propriedades de conexão de origem de dados para algumas origens de dados:

- Para conexões de origem de dados do Teradata:

  ```
  ibmcognos.authentication=java_krb5;LOGMECH=KRB5;
  ```
- Para conexões de origem de dados do SAP-HANA:

  ```
  ibmcognos.authentication=java_krb5;
  ```

- Para conexões de origem de dados do Microsoft SQL Server:
  `ibmcognos.authentication=java_krb5;authenticationScheme=JavaKerberos;`

Configurando um Repositório para Mensagens de Log

O protocolo BI Bus inclui o processamento de mensagens de log, uma importante ferramenta de diagnóstico para investigar o comportamento do IBM Cognos Analytics.

Além das mensagens de erro, as mensagens de log oferecem informações sobre o status dos componentes e uma visão de alto nível de eventos importantes. Por exemplo: as mensagens de log podem fornecer informações sobre tentativas de inicializar e encerrar serviços, finalização de solicitações de processamento e indicadores de erros fatais. Os logs de auditoria, que estão disponíveis em um banco de dados de criação de log, fornecem informações sobre a atividade do usuário e do relatório.

Os serviços do IBM Cognos em cada computador enviam informações sobre erros e eventos para um servidor de log local. Um servidor de log local é instalado na pasta *install_location*/logs em cada computador IBM Cognos Analytics que contém o Content Manager ou od Componentes da Camada de Aplicativos. Como o servidor de log usa uma porta diferente de outros componentes do IBM Cognos Analytics, ele continua a processar os eventos mesmo se outros serviços no computador local, como o dispatcher, estiverem desativados.

O fluxo de trabalho a seguir exibe as tarefas necessárias para preparar-se para a criação de log.

- Durante o planejamento, determine a configuração de criação de log adequada para seu ambiente. Por exemplo, avalie diversos repositórios de mensagens de log, como servidores de log remotos e arquivos de log, como o syslog do UNIX ou do Linux ou o log de eventos do Windows NT, além do arquivo de log local. Também é possível enviar somente informações de criação de log de auditoria para um banco de dados. Considere a segurança, tal como os métodos disponíveis para proteção dos arquivos de log contra as falhas do sistema e a adulteração do usuário.
- Durante a configuração, defina as propriedades de inicialização para criação de log, como configurações de conexão para bancos de dados. Você também deve criar um banco de dados de criação de log se houver planos de coletar os logs de auditoria. Se a comunicação entre um servidor de log local e um servidor de log remoto precisar ser assegurada, faça as mudanças apropriadas nas configurações em ambos os computadores do IBM Cognos Analytics. Também é possível habilitar certos recursos de criação de log, como a criação de log específica para um usuário.
- Ao configurar a criação de log, especifique o nível de detalhe para concentrar as mensagens nas informações relevantes em sua organização. O relatórios de auditoria também podem ser configurados para controlar as atividades de usuário e relatório.

  Para obter mais informações sobre a configuração de logs, consulte o *Guia de Administração e Segurança do IBM Cognos Analytics*.

Para obter mais informações sobre como usar mensagens de log para resolver problemas e como resolver problemas relacionados a logs, consulte o *Guia de Resolução de Problemas do IBM Cognos Analytics*.

Diretrizes para Criar um Banco de Dados de Criação de Log

É possível criar um banco de dados para armazenar mensagens de log. A criação de um banco de dados de criação de log envolve as seguintes tarefas:

- Crie um banco de dados de criação de log.

  Para IBM Db2, Oracle e Microsoft SQL Server, use o mesmo procedimento usado ao criar o banco de dados de armazenamento de conteúdo. Utilize as instruções em "Diretrizes para Criar o Armazenamento de Conteúdo" na página 8.

  Nota: Se estiver usando o Db2, não será possível gerar um script para criar o banco de dados de notificação da mesma maneira que o armazenamento de conteúdo.

  Para o Db2 on z/OS, use as instruções em "Configurações sugeridas para criar um banco de dados de criação de log no Db2 on z/OS".
- Configure a conectividade do banco de dados.

  Utilize as instruções em "Conectividade do Banco de Dados para o Banco de Dados de Criação de Log" na página 202.
- Especifique o repositório das mensagens de log.

  Utilize as instruções em "Repositório de Mensagens de Log" na página 204.

Configurações sugeridas para criar um banco de dados de criação de log no Db2 on z/OS

O banco de dados criado deve conter as definições de configuração especificadas.

Use a lista de verificação a seguir para ajudá-lo a configurar o banco de dados de criação de log no Db2 on z/OS.

__ • Efetue logon no sistema z/OS como um usuário com privilégios de administrador no Db2 on z/OS.

__ • Crie uma instância do banco de dados, um grupo de armazenamento e uma conta de usuário para o armazenamento de conteúdo. O IBM Cognos usa as credenciais de uma conta do usuário para se comunicar com o servidor de banco de dados.

__ • Verifique se alocou um pool de buffer com tamanho de página de 8 KB para a instância do banco de dados.

__ • Para um banco de dados de criação de log no Db2 on z/OS, os administradores devem executar um script de espaço de tabela para criar espaços de tabela para conter objetos grandes e outros dados para o banco de dados de criação de log e, em seguida, conceder direitos de usuário à tabela. Para obter mais informações sobre como executar o script do espaço de tabela, consulte "Criar espaços de tabela para um banco de dados de criação de log no Db2 on z/OS".

Criar espaços de tabela para um banco de dados de criação de log no Db2 on z/OS

Se você estiver usando o IBM Db2 on z/OS, um administrador de banco de dados deverá executar um script para criar um conjunto de espaços de tabelas necessáriopara o banco de dados de criação de log. O script deve ser modificado para substituir os parâmetros de espaço reservado com os adequados a seu ambiente.

Certifique-se de usar a convenção de nome para o Db2 on z/OS. Por exemplo, todos os nomes de parâmetros devem iniciar com uma letra e o comprimento não deve exceder 6 caracteres. Para obter mais informações, consulte o Db2 Knowledge Center.

Procedimento

1. Conecte-se ao banco de dados como um usuário com privilégios para criar e arrastar tablespaces e para permitir a execução de instruções SQL.
2. Acesse o diretório *install_location*/configuration/schemas/logging/db2zos.
3. Abra o arquivo de script LS_tablespace_db2zOS.sql e use a tabela a seguir para ajudá-lo a substituir os parâmetros genéricos pelos apropriados para o seu ambiente.

Tabela 31. Nomes e descrições de parâmetros de espaços de tabela para um banco de dados de criação de log no Db2 on z/OS

Nome do parâmetro	Descrição
IPFSCRIPT_DATABASE	O nome do banco de dados de criação de log.
IPFSCRIPT_STOGROUP	O nome do grupo de armazenamento.
IPFSCRIPT_TABLESPACE	O nome do espaço de tabela que contém as tabelas base no banco de dados de criação de log. Este tablespace não é para tabelas auxiliares.
IPFSCRIPT_LS_ID	O identificador de instância para o banco de dados de auditoria. Esse valor não deve ser mais longo do que dois caracteres.
IPFSCRIPT_BP	O nome do buffer pool de 8 k alocado para objetos regulares.
IPFSCRIPT_USERNAME	A conta do usuário que acessa o banco de dados de criação de log.

   Nem todos os parâmetros listados estão no script, mas podem ser adicionados no futuro.
4. Salve e execute o script.
5. Conceda os direitos de usuário do IBM Cognos aos espaços de tabela criados ao executar o arquivo de script:
   - Abra o arquivo de script LS_rightsGrant_db2zOS.sql.
   - Substitua os valores de parâmetros com os adequados a seu ambiente.

     Dica: Certifique-se de que os mesmos valores usados ao criar pools de buffer e a conta de usuário estejam sendo usados.
   - Salve e execute o script LS_rightsGrant_db2zOS.sql.

Resultados

O banco de dados de criação de log foi criado.

Conectividade do Banco de Dados para o Banco de Dados de Criação de Log

Depois de criar um banco de dados para logs de auditoria, etapas adicionais serão necessárias para configurar o cliente de banco de dados se você usar Oracle, o IBM Db2 ou o Informix Dynamic Server como o servidor de banco de dados.

Em um ambiente distribuído, o servidor de log local em um computador Componentes da Camada de Aplicativos pode enviar mensagens de log para um servidor de log remoto, que então envia as mensagens para o banco de dados de criação de log. Para o Oracle e o Db2, o driver JDBC e/ou o software do cliente de banco de dados apropriados são necessários somente no computador de Componentes da Camada de Aplicativos com o servidor de log remoto que se conecta ao banco de dados de criação de log.

Microsoft SQL Server

Se você usar um banco de dados Microsoft SQL Server, o arquivo `JSQLConnect.jar` será instalado no local apropriado, por padrão. A única etapa adicional será garantir que o Microsoft SQL Server use conectividade TCP/IP.

Configurar a conectividade do banco de dados para um banco de dados de criação de log do IBM Db2

Você deve configurar o software do cliente de banco de dados e o driver JDBC em todos os computadores de Componentes da Camada de Aplicativos com uma conexão com o banco de dados de criação de log. Você deve configurar o driver JDBC no computador com Content Manager, a menos que você esteja usando o mesmo tipo de banco de dados para as mensagens de log que usa para o armazenamento de conteúdo.

A versão do driver deve ser pelo menos JCC 3.7 para um sistema operacional Linux ou UNIX, ou para um sistema operacional Microsoft Windows versão 9.1 fix pack, ou JCC 3.42 para um sistema operacional Linux, UNIX, ou para um sistema operacional Microsoft Windows versão 9.5 fix pack 2.

Procedimento

Copie os arquivos a seguir do diretório *DB2_installation*`\sqllib\java` para o diretório *install_location*`\drivers`:

- O arquivo do driver universal, `db2jcc4.jar`
- O arquivo de licença:

  Para o Db2 em sistemas operacionais Linux, UNIX ou Windows, use `db2jcc_license_cu.jar`.

  Para o Db2 on z/OS, use `db2jcc_license_cisuz.jar`.

  Se você estiver conectando-se ao Db2 on z/OS, use a versão do driver do fix pack 5 da versão 9.1 ou do fix pack 2 da versão 9.5 no Linux, UNIX ou Windows.

  Dica: Para verificar a versão do driver, execute o seguinte comando:

  ```
  java -cp path\db2jcc4.jar com.ibm.db2.jcc.DB2Jcc -version
  ```

Configurar a Conectividade para o Banco de Dados de Criação de Log Oracle

Você deve configurar o driver JDBC em todos os computadores de Componentes da Camada de Aplicativos com uma conexão com o banco de dados de criação de log. Também é preciso configurar o driver JDBC no computador com o Content Manager, a menos que esteja utilizando o mesmo tipo de banco de dados para as mensagens de log que utiliza para o armazenamento de conteúdo.

Procedimento

1. No computador onde está instalado o cliente Oracle, acesse o diretório *ORACLE_HOME*/jdbc/lib.
2. Copie o arquivo de biblioteca correto para a sua versão do cliente Oracle no diretório *install_location*\drivers no computador em que o Content Manager estiver instalado e onde a notificação é enviada para um banco de dados Oracle.

   Se estiver usando o Oracle 12c, você deve ter ojdbc7.jar.

   Se estiver usando o Oracle 11g, você deve ter ojdbc5.jar.

   Os arquivos estão disponíveis de uma instalação do cliente ou servidor Oracle e também podem ser transferidos por download do Web site de tecnologia Oracle.

Configurar a Conectividade do Banco de Dados para um Banco de Dados de Criação de Log Informix

Você deve configurar o driver JDBC em todos os computadores de Componentes da Camada de Aplicativos com uma conexão com o banco de dados de criação de log. Também é preciso configurar o driver JDBC no computador com o Content Manager, a menos que esteja utilizando o mesmo tipo de banco de dados para as mensagens de log que utiliza para o armazenamento de conteúdo.

Procedimento

1. No computador onde o Informix está instalado, acesso o diretório *Informix_location*/sqllib/java.
2. Copie os arquivos a seguir no diretório *install_location*\drivers em cada computador em que o Content Manager estiver instalado.
   - o arquivo do driver universal, db2jcc4.jar
   - o arquivo de licença, db2jcc4_license_cisuz.jar

Repositório de Mensagens de Log

Um servidor de log é automaticamente instalado junto com o Content Manager ou o Application Tier Components. É possível especificar um ou mais repositórios em que o servidor de log local envia mensagens de log.

Enviando Mensagens de Log a um Servidor de Log Remoto

Em uma instalação distribuída, é possível configurar o servidor de log em cada computador com IBM Cognos para enviar mensagens de log para um único servidor de log remoto, que age como um servidor de log comum. Em seguida pode-se configurar o servidor de log comum para enviar as mensagens de log a um arquivo ou banco de dados comum, no mesmo ou em outro computador.

Se o servidor de log remoto se tornar indisponível, as mensagens de log serão redirecionadas para os arquivos de recuperação no computador local no diretório *install_location*/logs/recovery/remote. Esses arquivos de recuperação possuem informações de registro de data e hora em seus nomes de arquivo, e não são lidos como arquivos de log comuns. Quando o servidor de log remoto fica disponível, um processo de recuperação automática move todas as informações de log para o servidor de log remoto e exclui os arquivos de log locais.

Salvando Mensagens de Log em um Arquivo

O servidor de log é configurado por padrão para enviar mensagens de log para o arquivo *install_location*/logs/cogaudit.log. Se o arquivo de log padrão não existir quando o serviço do IBM Cognos for iniciado, ele será criado automaticamente.

É possível configurar o servidor de log para enviar mensagens de log para um arquivo diferente. Se você configurar um arquivo de log diferente, o IBM Cognos tentará criar automaticamente esse arquivo na inicialização, além do arquivo de log padrão. Se o local do arquivo de log configurado for diferente daquele do diretório *install_location*/logs, será necessário garantir que o arquivo de log exista antes de iniciar o serviço IBM Cognos. Por exemplo, se você configurar o servidor de log para enviar mensagens para o arquivo /usr/lpp/logfiles/cognos.log, o IBM Cognos tenta criar automaticamente o arquivo cognos.log na pasta /usr/lpp/logfiles. Se essa pasta não existir, o IBM Cognos não cria o arquivo cognos.log e nenhuma mensagem de log pode ser registrada no mesmo. Observe que essas mensagens de log não são registradas no arquivo de log padrão. Embora o IBM Cognos crie automaticamente o arquivo de log padrão mesmo quando outro arquivo de log está configurado, o arquivo de log padrão não é usado como um backup.

Salvando Mensagens de Log em um Banco de Dados

O servidor de log também pode enviar logs de auditoria a um banco de dados no mesmo ou em outro computador. Os logs de auditoria fornecem informações sobre atividade do usuário e de relatório.

O banco de dados de criação de log possui a mesma configuração e requisitos de conta de usuário que o banco de dados de armazenamento de conteúdo. Após você configurar os componentes do IBM Cognos para enviar mensagens para um banco de dados de criação de log, e reiniciar o serviço do IBM Cognos, os componentes do IBM Cognos criam as tabelas e os campos de tabelas obrigatórios. É possível testar a conexão com o banco de dados de criação de log antes de você reiniciar o serviço do IBM Cognos.

Especifique o repositório de mensagens de log para o IBM Db2 no UNIX, Linux ou Windows

É possível configurar um tipo de repositório para as mensagens de log, e depois configurar propriedades para o repositório específico. Também é possível configurar mais de um repositório de mensagens de log.

Antes de Iniciar

Antes de especificar um banco de dados como um repositório, verifique se

__ • criou o banco de dados de criação de log

__ • tenha configurado o cliente de banco de dados

Procedimento

1. No computador onde você instalou o Content Manager ou Componentes da Camada de Aplicativos, inicie o IBM Cognos Configuration.
2. Na janela **Explorer**, em **Ambiente**, clique em**Criação de log**.
3. Na janela **Propriedades**, use a tabela a seguir para ajudar a configurar as propriedades do servidor de log.

Tabela 32. Propriedades do Servidor de Log

Tarefa	Ação
Use TCP entre componentes do IBM Cognos em um computador e seu servidor de log local	Configure a propriedade **Habilitar TCP** como **Verdadeiro**. O UDP fornece uma comunicação mais rápida com um risco menor de conexões perdidas que o TCP. Entretanto, o risco de perder uma conexão local de TCP é baixo. O TCP sempre é usado na comunicação entre um servidor de log local e um remoto.
Altere o número de threads disponíveis para o servidor de log local.	Digite o valor na propriedade **Segmentos de trabalho do servidor de log local**. Mantenha o valor padrão de 10. O intervalo vai de 1 a 20. Entretanto, se tiver um número alto de mensagens de log, é possível alocar mais threads para melhorar o desempenho.

4. Na janela **Explorer**, em **Ambiente**, clique com o botão direito do mouse em **Criação de Log** e clique em **Novo Recurso** > **Destino**.
5. ??Na caixa **Nome**, digite o nome do repositório.
6. Na lista **Tipo**, clique no tipo do repositório e depois em **OK**.
7. Se o repositório for um arquivo, digite os valores adequados para as propriedades obrigatória e opcional na janela **Propriedades**.
8. Se o repositório for um servidor de log remoto, digite os valores adequados para as propriedades obrigatória e opcional na janela **Propriedades**.

   Se a **URI do dispatcher interno** do computador do repositório de destino estiver configurada para usar SSL, na janela **Propriedades**, defina a propriedade **Ativação do SSL** como **Verdadeira**.

   Mais tarde á necessário especificar o repositório das mensagens de log ao configurar o servidor de log remoto.
9. Se o repositório for um banco de dados, na janela **Explorer**, em **Criação de log**, especifique o tipo de banco de dados e suas propriedades da seguinte forma:
   - Clique com o botão direito do mouse no nome do banco de dados e clique em **Novo Recurso** > **Banco de Dados**.
   - ??Na caixa **Nome**, digite o nome do repositório.
   - Na lista **Tipo**, clique no tipo de banco de dados e depois clique em **OK**.
   - Na janela **Propriedades**, digite os valores apropriados para as propriedades obrigatórias e opcionais.

     Para um banco de dados Microsoft SQL Server, é possível escolher usar um número da porta, como 1433, uma instância denominada como valor para a propriedade **Servidor de banco de dados com número da porta ou nome da instância**. Inclua o número da porta se portas que não são padrão forem utilizadas. Inclua o nome da instância se houver várias instâncias do Microsoft SQL Server.

     Para se conectar a uma instância denominada, você deve especificar o nome da instância como uma propriedade URL JDBC ou de origem de dados. Por

exemplo, é possível digitar **localhost\instance1**. Se não forem especificadas propriedades de nome de instância, é criada uma conexão com a instância padrão.

Observe que as propriedades especificadas para a instância denominada, junto com a ID e senha de usuário e nome do banco de dados, são usados para criar um URL JDBC. Eis um exemplo:

jdbc:JSQLConnect://localhost\\instance1/user=sa/*mais propriedades conforme necessário*

- Teste a conexão ao novo banco de dados. Na janela **Explorer**, em **Ambiente**, clique com o botão direito em **Criação de log** e clique em **Teste**.

  Os componentes do IBM Cognos se conectam ao banco de dados. Se você configurou mais de um banco de dados para mensagens de criação de log, os componentes do IBM Cognos testarão todos os bancos de dados.

10. Repita as etapas de 5 a 10 para cada repositório para o qual deseja que o servidor de log envie mensagens.
11. No menu **Arquivo**, clique em **Salvar**.
12. Na janela **Explorer**, clique em **Serviços do IBM Cognos** > **IBM Cognos**.
13. No menu **Arquivo**, clique em **Reiniciar**.

    Se você selecionou um banco de dados como repositório, os componentes do IBM Cognos criarão as tabelas e os campos obrigatórios no banco de dados criado.

Resultados

Se o repositório era um servidor de log remoto, configure e inicie esse servidor. Em seguida, reinicie o serviço do IBM Cognos no computador local.

Se o repositório era um banco de dados, é possível usar componentes do IBM Cognos para executar relatórios de log a partir do banco de dados.

Também é possível definir o nível de criação de log, que controla a quantidade e o tipo de mensagens que são enviadas para um arquivo ou banco de dados de log. Para obter instruções, consulte o *Guia de administração e segurança do IBM Cognos Analytics*.

Especifique o repositório de mensagens de log para o IBM Db2 on z/OS

É possível configurar um tipo de repositório para as mensagens de log, e depois configurar propriedades para o repositório específico. Também é possível configurar mais de um repositório de mensagens de log.

Procedimento

1. No computador onde você instalou o Content Manager ou Componentes da Camada de Aplicativos, inicie o IBM Cognos Configuration.
2. Na janela **Explorer**, em **Ambiente**, clique em**Criação de log**.
3. Na janela **Propriedades**, use a tabela a seguir para ajudar a configurar as propriedades do servidor de log.

Tabela 33. Propriedades do Servidor de Log

Tarefa	Ação
Use TCP entre componentes do IBM Cognos em um computador e seu servidor de log local	Configure a propriedade **Habilitar TCP** como **Verdadeiro**. O UDP fornece uma comunicação mais rápida com um risco menor de conexões perdidas que o TCP. O TCP é usado na comunicação entre um servidor de log local e um remoto.
Altere o número de threads disponíveis para o servidor de log local.	Digite o valor na propriedade **Segmentos de trabalho do servidor de log local**. Mantenha o valor padrão de 10. O intervalo vai de 1 a 20. Entretanto, se tiver um número alto de mensagens de log, é possível alocar mais threads para melhorar o desempenho.

4. Na janela **Explorer**, em **Ambiente**, clique com o botão direito do mouse em **Criação de Log** e clique em **Novo Recurso** > **Destino**.
5. ??Na caixa **Nome**, digite o nome do repositório.
6. Na lista **Tipo**, clique em **Banco de dados** e depois em **OK**.
7. Na janela **Explorer**, em **Criação de Log**, clique com o botão direito do mouse no nome do banco de dados e clique em **Novo Recurso** > **Banco de Dados**.
8. ??Na caixa **Nome**, digite o nome do repositório.
9. Na lista **Tipo**, clique em **Banco de dados DB2** e depois em **OK**.
10. Na janela **Propriedades**, digite **Servidor de banco de dados e número da porta**, **ID do usuário e senha** e **Nome do banco de dados** z/OS.

    Verifique se a ID do usuário é igual ao valor especificado no parâmetro IPFSCRIPT_USERNAME no arquivo de script LS_tablespace_db2zOS.sql "Criar espaços de tabela para um banco de dados de criação de log no Db2 on z/OS" na página 201.
11. Na janela **Explorer**, clique em **Configuração Local**.
12. Na janela **Propriedades**, próxima de **Propriedades Avançadas**, clique na caixa **Valor** e, em seguida, clique no ícone de edição  .
13. Clique em **Adicionar** e adicione os seguintes nomes e valores de parâmetros de configuração:

Tabela 34. Nomes e Valores dos Parâmetros de Configuração

Nome do parâmetro	Valor
IPFSCRIPT_CREATE_IN	O local das tabelas de base Por exemplo: NomeBancodedados.baseNomeTablespace.
IPFSCRIPT_STOGROUP	O nome do grupo de armazenamento.
IPFSCRIPT_DATABASE	O nome do banco de dados de criação de log.
IPFSCRIPT_LS_ID	O identificador de instância para o banco de dados de auditoria. Esse valor não deve ser mais longo do que dois caracteres.

14. No menu **Arquivo**, clique em **Salvar**.
15. Teste a conexão ao novo banco de dados. Na janela **Explorer**, em **Ambiente**, clique com o botão direito em **Criação de log** e clique em **Teste**.

    Os componentes do IBM Cognos se conectam ao banco de dados. Se você configurou mais de um banco de dados para mensagens de criação de log, os componentes do IBM Cognos testarão todos os bancos de dados.

Especifique o Repositório de Mensagens de Log para o Informix

É possível configurar um tipo de repositório para as mensagens de log, e depois configurar propriedades para o repositório específico. Também é possível configurar mais de um repositório de mensagens de log.

Procedimento

1. Na janela **Explorer**, em **Ambiente**, clique em**Criação de log**.
2. Na janela **Propriedades**, use a tabela a seguir para ajudar a configurar as propriedades do servidor de log.

Tabela 35. Propriedades do Servidor de Log

Tarefa	Ação
Use TCP entre componentes do IBM Cognos em um computador e seu servidor de log local	Configure a propriedade **Habilitar TCP** como **Verdadeiro**. O UDP fornece uma comunicação mais rápida com um risco menor de conexões perdidas que o TCP. O TCP é usado na comunicação entre um servidor de log local e um remoto.
Altere o número de threads disponíveis para o servidor de log local.	Digite o valor na propriedade **Segmentos de trabalho do servidor de log local**. Mantenha o valor padrão de 10. O intervalo vai de 1 a 20. Entretanto, se tiver um número alto de mensagens de log, é possível alocar mais threads para melhorar o desempenho.

3. Na janela **Explorer**, em **Ambiente**, clique com o botão direito do mouse em **Criação de Log** e clique em **Novo Recurso** > **Destino**.
4. ??Na caixa **Nome**, digite o nome do repositório.
5. Na lista **Tipo**, clique em **Banco de dados** e depois em **OK**.
6. Na janela **Explorer**, em **Criação de Log**, clique com o botão direito do mouse no nome do banco de dados e clique em **Novo Recurso** > **Banco de Dados**.
7. ??Na caixa **Nome**, digite o nome do repositório.
8. Na lista **Tipo**, clique em **Banco de dados do Informix Dynamic Server** e, em seguida, clique em **OK**.
9. Na janela **Propriedades**, digite os valores para **Servidor de banco de dados e número da porta**, **ID do usuário e senha** e o **Nome do banco de dados**.
10. Se você tiver diversas instâncias de um banco de dados de criação de log do Informix, crie a propriedade avançada IPFSCRIPTIDX e especifique a conta sob a qual a instância é executada:

- Na janela **Explorer**, clique em **Configuração Local**.
- Na janela **Propriedades**, clique na coluna **Valor** de **Propriedades Avançadas** e, em seguida, clique no ícone de edição  .
- Na caixa de diálogo **Valor - Propriedades avançadas**, clique em **Adicionar**.
- Na coluna **Nome**, digite **IPFSCRIPTIDX**
- Na coluna **Valor**, digite a ID do usuário da conta na qual a instância do banco de dados de criação de log é executada.

  Use uma conta do usuário diferente para cada instância do banco de dados de criação de log do Informix.
- Repita cada instância do IBM Cognos Configuration que usa uma instância de um banco de dados de criação de log do Informix.

11. No menu **Arquivo**, clique em **Salvar**.
12. Teste a conexão ao novo banco de dados. Na janela **Explorer**, em **Ambiente**, clique com o botão direito em **Criação de log** e clique em **Teste**.

    Os componentes do IBM Cognos se conectam ao banco de dados. Se você configurou mais de um banco de dados para mensagens de criação de log, os componentes do IBM Cognos testarão todos os bancos de dados.

Ativação de conexão específica do usuário

Ao diagnosticar problemas, é possível definir temporariamente criação de log para monitorar um ou mais usuários específicos em vez de todos os usuários de uma só vez. Após concluir o diagnóstico, retome a criação de log normal. Para ativar a criação de log específica do usuário, use o IBM Cognos Configuration para configurar informações de conexão para Java Management Extensions (JMX), uma tecnologia que fornece ferramentas para gerenciar e monitorar aplicativos e redes orientadas a serviços. Depois configure as informações de conexão JMX em um arquivo de propriedades de implantação.

Após ativar a criação de log específica do usuário para os componentes do IBM Cognos, ative a criação de log para um usuário específico usando o serviço Processo Remoto para JMX. Para obter informações, consulte o tópico sobre como usar a criação de log para diagnosticar um problema para um usuário específico no *Guia de administração e segurança do IBM Cognos Analytics*.

Você deve instalar o Oracle Java SE Development Kit ou o Java Software Development Kit for IBM antes de poder ativar a criação de log específica do usuário.

Configurando Informações de Conexão de JMX Usando o IBM Cognos Configuration

As informações de conexão de Java Management Extensions (JMX) são configuradas no IBM Cognos Configuration especificando um valor de cookie e, em seguida, configurando a porta e as credenciais JMX.

Procedimento

1. No computador em que o Content Manager está instalado, inicie o IBM Cognos Configuration.
2. Na janela **Explorer**, clique em **Ambiente**.
3. Na janela **Propriedades**, configure as propriedade JMX em **Configurações de dispatcher**:
   - Para **Porta JMX externa**, digite um número de porta disponível.

- Para a **Credencial JMX Externa**, clique no ícone de edição  na coluna de **Valor**, digite um ID do usuário e senha e, em seguida, clique em **OK**.

  O ID do usuário e a senha garantem que apenas um usuário autorizado possa se conectar ao ambiente Java para especificar o usuário ou usuários a efetuarem login usando a porta especificada em **Porta JMX externa**.

4. Salve a configuração.

Configure as informações de conexão JMX de um arquivo de propriedades de implantação

Para que o servidor de aplicativos suporte as configurações de Java Management Extensions (JMX), especifique a porta JMX no arquivo de propriedades de implantação p2pd.

Procedimento

1. Em um editor de texto, abra o arquivo `p2pd.deploy_defaults.properties` localizado em *`install_location`*`/webapps/p2pd/WEB-INF`.
2. Remova o comentário da linha `rmiregistryport` e configure o valor para a **Porta JMX externa** que você definiu no IBM Cognos Configuration.
3. Salve o arquivo `p2pd.deploy_defaults.properties`.
4. Reinicie os serviços para o IBM Cognos.

Resultados

Agora o IBM Cognos suporta criação de logs para um ou mais usuários específicos. Para obter mais informações, consulte o tópico sobre como usar a criação de log para diagnosticar um problema para um usuário específico no *Guia de administração e segurança do IBM Cognos Analytics*.

Alteração de definições globais

Por padrão, os componentes do IBM Cognos garantem que todos os códigos do idioma, que podem vir de diferentes fontes e em vários formatos, usem uma forma normalizada. Isto significa que todos os códigos do idioma expandidos se adaptam às configurações de idioma e código da região. Cada computador possui um código do idioma de sistema padrão e um código do idioma de usuário por usuário. Os códigos do idioma de usuário podem ser diferentes do código do idioma de sistema padrão. Caso as configurações globais sejam alteradas em um computador com Content Manager, é necessário fazer as mesmas mudanças nos outros computadores com Content Manager.

As configurações globais são alteradas para os seguintes propósitos

- customizar o suporte ao idioma para a interface com o usuário
- customizar o suporte à moeda
- customizar o suporte ao código do idioma do conteúdo
- mapear o idioma usado na interface com o usuário do produto
- mapear códigos do idioma do conteúdo
- incluir fontes no ambiente do IBM Cognos
- customizar o fuso horário padrão
- alterar a codificação dos e-mails
- Personalização de configurações de cookie.

Personalização do suporte ao idioma na interface com o usuário

Use a tabela Códigos do Idioma do Produto para adicionar ou remover o suporte ao idioma da interface com o usuário. Por exemplo, se não solicitar uma interface com o usuário em alemão, é possível remover o idioma da lista.

Se o idioma da interface com o usuário do produto for alterada, os dados não são atingidos.

Antes de Iniciar

Certifique-se de que instalou as fontes adequadas para suportar os conjuntos de caracteres e símbolos de moedas que forem utilizados. Para que os símbolos das moedas japonesa e coreana sejam exibidos corretamente, é necessário instalar fontes adicionais do disco Supplementary Languages Documentation.

Procedimento

1. Em cada computador que tiver o Content Manager, inicie o IBM Cognos Configuration.
2. No menu **Ações**, clique em **Editar Configuração Global**.
3. Clique na guia **Códigos do idioma do produto**.
   Todos os códigos do idioma suportados são exibidos.
4. Clique em **Incluir**.

   Dica: Para remover o suporte, selecione a caixa de seleção próxima de **Código do Idioma Suportado** e clique em **Remover**.
5. Na segunda coluna, digite a porção do idioma de um código do idioma.
6. Repita as etapas 3 a 5 em outros idiomas suportados que deseja adicionar.
7. Clique em **OK**.
8. No menu **Arquivo**, clique em **Salvar**.

Personalização do suporte de moeda

Se forem necessárias moedas adicionais ou se desejar remover algumas da interface com o usuário, é possível atualizar a lista de moedas suportadas na tabela Moedas. Se usar as moedas japonesa ou coreana, é necessário configurar o suporte para que os caracteres do Iene japonês e do Won coreano sejam exibidos corretamente..

Por padrão, os componentes do IBM Cognos mostram apenas um subconjunto de moedas suportadas na interface com o usuário. As moedas são identificadas pelo código de unidade monetária ISO 4217. A lista completa de moedas suportadas que podem ser incluídas é relacionada no arquivo i18n_res.xml no diretório *install_location*/bin.

A inclusão de moedas no ambiente do IBM Cognos não garante que seu computador tenha uma fonte com os caracteres necessários para exibir a moeda. Certifique-se de ter instalado as fontes adequadas para suportar os símbolos de moedas utilizados. Por exemplo, para exibir o símbolo de moeda indiana (rúpia) corretamente, é necessário instalar uma fonte que contenha aquele caractere. Além disso, para que os símbolos das moedas japonesa e coreana sejam exibidos corretamente, é necessário instalar fontes adicionais do disco Supplementary Languages Documentation.

Adição de moedas à interface com o usuário

É possível adicionar moedas suportadas ou não na interface com o usuário. Inclua as moedas suportadas no IBM Cognos Configuration. Inclua moedas não suportadas no arquivo i18n_res.xml que é fornecido no IBM Cognos.

Se incluir um código de moeda não suportado pelo IBM Cognos, será necessário incluí-lo manualmente no arquivo i18n_res.xml no diretório *install_location*/bin. Copie esse arquivo em cada computador IBM Cognos em sua instalação.

Procedimento

1. Em cada computador que tiver o Content Manager, inicie o IBM Cognos Configuration.
2. No menu **Ações**, clique em **Editar Configuração Global**.
3. Clique na guia **Moedas**.
4. Clique em **Incluir**.

   Dica: Para remover o suporte, selecione a caixa de seleção próxima do item suportado e clique em **Remover**.
5. Na segunda coluna, digite o valor apropriado.

   O valor adicionado deve corresponder aos códigos ISO 4217 para a representação de moedas e formatos. Em geral, o valor adicionado é um código alfabético de três letras. Os dois primeiros caracteres são letras representando o código do país ou região ISO 3166 para o país ou região de onde a moeda é. A letra adicional representa a primeira letra da moeda.
6. Repita as etapas 3 a 5 para os outros tipos de suporte que deseja adicionar.
7. No menu **Arquivo**, clique em **Salvar**.

Customizar Suporte do Código de Idioma do Conteúdo

Para garantir que os usuários visualizem relatórios, dados ou metadados no idioma preferido ou específico da região, adicione códigos do idioma parciais (idioma) ou códigos do idioma completos (idioma - região) à tabela Códigos do Idioma do Conteúdo. Desta forma, se o conteúdo estiver disponível em idiomas ou códigos do idioma diferentes será processado para os usuários com base no código do idioma do usuário. Por padrão, o código do idioma do conteúdo substitui o código do idioma do produto no portal por algum conteúdo.

Se visualizar relatórios no idioma tailandês, os dígitos não são suportados.

Antes de Iniciar

Se um código do idioma não for solicitado, é possível removê-lo da lista. Deixe pelo menos um código do idioma do conteúdo na lista para Application Tier Components operar.

A inclusão de códigos do idioma incompletos (idiomas) no ambiente do IBM Cognos não garante que seu computador tenha uma fonte que possa exibir páginas da Web em seus idiomas preferenciais. Certifique-se de que instalou as fontes adequadas para suportar os conjuntos de caracteres e símbolos de moedas que forem utilizados. Para que os símbolos das moedas japonesa e coreana sejam exibidos corretamente, é necessário instalar fontes adicionais do disco Supplementary Languages Documentation.

Procedimento

1. Em cada computador que tiver o Content Manager, inicie o IBM Cognos Configuration.
2. No menu **Ações**, clique em **Editar Configuração Global**.
3. Clique na guia **Códigos do idioma do conteúdo**.

   Todos os códigos do idioma suportados são exibidos.
4. Clique em **Incluir**.

   Dica: Para remover o suporte, selecione a caixa de seleção próxima do item suportado e clique em **Remover**.
5. Na segunda coluna, digite o valor apropriado.
   - Para adicionar um suporte ao idioma para dados e metadados de relatório, digite uma definição de localidade parcial (idioma).
   - Para adicionar suporte específico de uma região, digite uma definição de código do idioma completo (idioma - região).
6. Repita as etapas 3 a 5 para cada código do idioma adicional de que deseja o suporte.
7. No menu **Arquivo**, clique em **Salvar**.

Códigos do idioma do conteúdo

Use a tabela Mapeamentos de Localidade do Conteúdo para mapear código do idioma do usuário em um código do idioma completo (idioma - região) ou parcial (idioma). Também é possível mapear o idioma preferencial do usuário para outro idioma se o conteúdo não estiver disponível no idioma preferencial do usuário.

Por exemplo, se um relatório ou scorecard não estiver disponível em um idioma preferido, por exemplo vietnamita, mas estiver disponível em francês ou alemão, use a tabela de mapeamento de conteúdo para mapear o idioma preferido (vietnamita) em outro idioma (francês ou alemão). Desta forma, vê-se o relatório ou scorecard no idioma mapeado.

Por padrão, a tabela Mapeamentos de Localidade do Conteúdo inclui os códigos do idioma que não contêm a região. Isto permite usar somente a porção do idioma do código do idioma ao especificar as configurações do código de idioma, e garante que sejam vistas sempre as informações corretas. Por exemplo, em um banco de dados multilíngue, os dados geralmente estão disponíveis em idiomas diferentes, como francês (fr), espanhol (es) e inglês (en), ao invés de estarem disponíveis em diferentes códigos do idioma, como inglês do Canadá (en-ca), inglês dos Estados Unidos (en-us) ou francês da França (fr-fr).

Os exemplos a seguir mostram o método que os componentes do IBM Cognos usam para determinar qual relatório ou scorecard o usuário verá se houver diversas versões de idioma disponíveis.

Exemplo 1

Um relatório está disponível no Content Manager em dois códigos do idioma, como com en-us (inglês dos Estados Unidos) e fr-fr (francês da França), mas o código do idioma do usuário está definido para fr-ca (francês do Canadá). O IBM Cognos usa o mapeamento de código do idioma para determinar qual relatório o usuário vê.

Primeiro, o IBM Cognos verifica se o relatório está disponível no Content Manager no código do idioma do usuário. Se ele não estiver disponível no código do idioma do usuário, o IBM Cognos mapeará o código do idioma do usuário para um código do idioma normalizado na guia Mapeamento de Código do Idioma do Conteúdo. Como o código do idioma do usuário é fr-ca, ele será mapeado para fr. O IBM Cognos usa o valor mapeado para ver se o relatório está disponível em fr. Nesse caso, o relatório estará disponível em en-us e fr-fr, e não em fr.

Em seguida, o IBM Cognos mapeia cada um dos relatórios disponíveis para um código do idioma normalizado. Desta forma, en-us se torna en e fr-fr se torna fr.

Já que o relatório e o código do idioma do usuário mapeiam para fr, o usuário com o código do idioma do usuário fr-ca verá o relatório salvo com o código do idioma fr-fr.

Exemplo 2

O código do idioma do usuário e os códigos do idioma do relatório são todos mapeados para o mesmo código do idioma. O IBM Cognos escolhe qual código do idioma usar. Por exemplo, se o código do idioma do usuário for en-ca (inglês do Canadá) e os relatórios estiverem disponíveis em en-us (inglês dos Estados Unidos) e en-gb (inglês do Reino Unido), o IBM Cognos mapeará cada código do idioma para en. O usuário verá o relatório na configuração do código de idioma escolhida pelo IBM Cognos.

Exemplo 3

Os códigos do idioma do relatório e do usuário não mapeiam para um idioma comum. O IBM Cognos escolhe o idioma. Neste caso, pode ser necessário configurar um mapeamento. Por exemplo, se um relatório estiver disponível em en-us (inglês dos Estados Unidos) e fr-fr (francês da França), mas o código do idioma do usuário for es-es (espanhol da Espanha), o IBM Cognos escolherá o idioma.

Mapeamento de código do idioma do conteúdo

Use a tabela Mapeamentos de Localidade do Conteúdo para mapear código do idioma do usuário em um código do idioma completo (idioma - região) ou parcial (idioma). Também é possível mapear o idioma preferencial do usuário para outro idioma se o conteúdo não estiver disponível no idioma preferencial do usuário.

Procedimento

1. Em cada computador que tiver o Content Manager, inicie o IBM Cognos Configuration.
2. No menu **Ações**, clique em **Editar Configuração Global**.
3. Clique na guia **Mapeamentos de Localidade do Conteúdo**.
4. Clique em **Incluir**.
5. Na caixa **Chave**, digite o código do idioma do usuário:
   - Para se certificar de que todas as regiões de um código do idioma de usuário vejam o conteúdo em um idioma específico, digite a porção do idioma do código do idioma, seguida de um travessão e (-) um asterisco (*).

     Por exemplo, digite **fr-***
   - Para se certificar de que um código do idioma de usuário (idioma - região) veja o conteúdo em um idioma específico, digite o código do idioma completo.

Por exemplo, digite **fr-ch**

- Para mapear um idioma preferido a outro idioma, digite a porção do idioma preferido do código do idioma.

  Por exemplo, digite **zh**

Dica: Para especificar o código do idioma para usar para um intervalo de chaves, use o caractere curinga (*) com o valor **Chave** e, em seguida, na caixa **Mapeamento de Código do Idioma**, digite o código do idioma. Por exemplo, se desejar que todas as chaves alemãs usem código do idioma alemão, digite **de*** na caixa **Chave** e digite na caixa **Mapeamento de Localidade**.

6. Na caixa **Mapeamento de Localidade**, digite a porção do idioma do código do idioma.

   Os usuários locais especificados na caixa **Chave** visualizarão o conteúdo no referido idioma.
7. Repita as etapas 3 a 5 em outros mapeamentos que deseja fazer.
8. Clique em **OK**.
9. No menu **Arquivo**, clique em **Salvar**.

Mapeamento de códigos do idioma do produto

Use a tabela Mapeamentos de Código de Idioma do Produto para especificar o idioma usado na interface com o usuário quando o idioma especificado no código do idioma do usuário não estiver disponível.

Certifique-se de que todas as regiões de um código do idioma usam o mesmo idioma, ou que um código do idioma específico e completo (idioma - região) use um idioma em particular.

Por padrão, o usuário vê a interface do produto no idioma que corresponde à configuração de idioma do código do idioma do usuário.

Procedimento

1. Em cada computador que tiver o Content Manager, inicie o IBM Cognos Configuration.
2. No menu **Ações**, clique em **Editar Configuração Global**.
3. Clique na guia **Mapeamentos de Código de idioma do produto**.
4. Clique em **Incluir**.
5. Na caixa **Chave**, digite o código do idioma do usuário:
   - Para se certificar de que todas as regiões de um código do idioma de usuário vejam a interface com o usuário em um idioma específico, digite a porção do idioma do código do idioma, seguida de um travessão e (-) um asterisco (*).

     Por exemplo, digite **es-***
   - Para se certificar de que um código do idioma completo (idioma - região) veja a interface com o usuário em um idioma específico, digite o código do idioma completo.

     Por exemplo, digite **es-es**
   - Para mapear um idioma preferido a outro idioma, digite a porção do idioma preferido do código do idioma.

     Por exemplo, digite **zh**

Dica: Para especificar qual código do idioma usar como padrão, use o caractere curinga (*) para o valor **Chave** e, em seguida, na caixa **Mapeamento de Código do Idioma**, digite o código do idioma.

6. Na caixa **Mapeamento de Localidade**, digite a porção do idioma do código do idioma.

   Os usuários locais especificados na caixa **Chave** visualizarão o conteúdo no referido idioma.
7. Repita as etapas 3 a 5 em outros mapeamentos que deseja fazer.
8. Clique em **OK**.
9. No menu **Arquivo**, clique em **Salvar**.

Personalização do fuso horário do servidor

É possível customizar o fuso horário usado pelo Content Manager selecionando um fuso horário do servidor diferente no IBM Cognos Configuration.

Para instalações em UNIX que não suportam uma interface gráfica de usuário baseada em Java, é possível visualizar a lista de fusos horários aceitáveis abrindo o IBM Cognos Configuration no computador Windows onde o Framework Manager está instalado.

O Content Manager está configurado para usar o fuso horário de seu sistema operacional por padrão. Todas as atividades planejadas no IBM Cognos são configuradas com o uso desse fuso horário. Além disso, os usuários no portal usarão esse fuso horário se configurarem suas preferências para o fuso horário padrão. Para obter mais informações sobre a configuração de preferências do usuário no portal, consulte o *IBM Cognos Analytics Administration and Security Guide*.

Procedimento

1. Inicie o IBM Cognos Configuration.
2. No menu **Ações**, clique em **Editar Configuração Global**.
3. Na janela **Configuração global**, clique na guia **Geral**.
4. Clique na coluna **Valor** de **Fuso horário do servidor** e selecione outro fuso horário na lista.
5. No menu **Arquivo**, clique em **Salvar**.

Codificação para E-mails

Por padrão, os componentes do IBM Cognos usam codificação UTF-8 em e-mails. Este valor define a codificação padrão usada pelo serviço de entrega nesta instância para todos os e-mails. Você pode ter clientes de e-mail mais antigos ou e-mails enviados do IBM Cognos para telefones celulares e PDAs que não reconhecem UTF-8. Se for o caso, mude a codificação de e-mail para um valor que funcione com todos os clientes de e-mail (por exemplo, ISO-8859-1, Shift-JIS). Cada instância do IBM Cognos que tem um serviço de entrega disponível deve ser alterada.

A codificação especificada afeta toda a mensagem, incluindo o assunto, anexos, nomes de anexos e corpo de texto simples ou HTML.

Os valores de codificação são mostrados na seguinte tabela:

Tabela 36. Valores de Codificação Suportados

Conjunto de caracteres	Valor de codificação suportado
UTF-8	utf-8
Europa Ocidental (ISO 8859-1)	iso-8859-1
Europa Ocidental (ISO 8859-15)	iso-8859-15
Europa Ocidental (Windows-1252)	windows-1252
Europa Central e Oriental (ISO 8859-2)	iso-8859-2
Europa Central e Oriental (Windows-1250)	windows-1250
Cirílico (ISO 8859-5)	iso-8859-5
Cirílico (Windows-1251)	windows-1251
Turco (ISO 8859-9)	iso-8859-9
Turco (Windows-1254)	windows-1254
Grego (ISO 8859-7)	iso-8859-7
Grego (Windows-1253)	windows-1253
Japonês (EUC-JP)	euc-jp
Japonês (ISO-2022-JP)	iso-2202-jp
Japonês (Shift-JIS)	shift_jis
Chinês tradicional (Big5)	big5
Chinês simplificado (GB-2312)	gb2312
Coreano (EUC-KR)	euc-kr
Coreano (ISO 2022-KR)	ISO 2022-KR
Coreano (KSC-5601)	ksc_5601
Tailandês (Windows-874)	windows-874
Tailandês (TIS-620)	tis-620

Mudança da codificação de e-mails

É possível alterar a codificação de e-mail para um valor que funcione em todos os clientes de e-mail.

Procedimento

1. Inicie o IBM Cognos Configuration.
2. No menu **Ações**, clique em **Editar Configuração Global**.
3. Na janela **Configuração global**, clique na guia **Geral**.
4. Clique na coluna **Valor** na propriedade **Codificação de e-mail**.
5. Role a tela até a definição desejada e clique nela.
6. No menu **Arquivo**, clique em **Salvar**.

Customizando configurações de cookies

Com base nos requisitos do ambiente do IBM Cognos, você pode precisar modificar as configurações usadas pelos componentes do IBM Cognos para criar cookies. É possível usar o IBM Cognos Configuration para customizar o domínio do cookie, o caminho e o sinalizador seguro.

Os componentes do IBM Cognos determinam o domínio do cookie a partir da solicitação de HTTP enviada pelo cliente, que normalmente é um navegador da

Web. Na maioria das configurações de rede, as solicitações de HTTP passam por intermediários como servidores proxy e firewalls conforme viajam do navegador para os componentes do IBM Cognos. Alguns intermediários modificam as informações que os componentes do IBM Cognos usam para calcular o domínio do cookie e esses componentes do IBM Cognos não podem configurar cookies. O sintoma comum deste problema é os usuários serem solicitados repetidamente para fazer logon. Para evitar este problema, configure o domínio de cookies.

Para configurar o valor correto para o domínio de cookies, use o formato e o valor que representam a cobertura mais abrangente para o host conforme sugerido a seguir:

- Para o valor de Domínio, use o nome do computador ou servidor independente. Especifique esse nome sem quaisquer pontos. Por exemplo, `mycompany`
- O valor de Domínio também pode especificar um sufixo. Os sufixos incluem .com, .edu, .gov, .int, .mil, .net ou .org. Inclua um ponto de prefixo. Por exemplo, `.mycompany.com`
- Outros níveis podem ser usados em um valor de Domínio. Inclua um ponto de prefixo. Por exemplo, `.accounts.mycompany.com`
- Um valor de Caminho pode restringir cookies ainda mais. O caminho mais geral é /. Um caminho de `/payables` restringe o cookie a todos os caminhos que começam com "payable" (e todos os subdiretórios). Um caminho de `/payables/` restringe o cookie para o diretório "payables" (e todos os subdiretórios).

Além disso, para segurança, os administradores podem configurar o atributo HTTPOnly para bloquear scripts de leitura ou manipulação do cookie de passaporte do CAM durante uma sessão do usuário com seu navegador da Web. Para obter mais informações sobre esse atributo, consulte o *Guia de administração e segurança do IBM Cognos Analytics*.

Procedimento

1. Em cada computador que tiver o Content Manager, inicie o IBM Cognos Configuration.
2. No menu **Ações**, clique em **Editar Configuração Global**.
3. Clique na guia **Geral**.
4. Clique na coluna **Valor** em **Configurações de cookie**, para cada propriedade que deseja mudar e especifique o novo valor.

   Se deixar a propriedade **Domínio** em branco, o dispatcher obtém o domínio do nome do host ou da solicitação.
5. Clique em **OK**.

Mudança da versão do endereço IP

Os produtos IBM Cognos suportam duas versões de endereço IP: IPv4 e IPv6. O IPv4 usa endereços IP de 32 bits e o IPv6 usa endereços IP de 128 bits.

Por exemplo:

- IPv4: 192.168.0.1:80
- IPv6: [2001:0db8:0000:0000:0000:148:57ab]:80

No IBM Cognos Configuration, é possível selecionar IPv4 ou IPv6 para comunicação do IBM Cognos usando a propriedade **Versão IP para Resolução do Nome do Host**. Como padrão, usa-se IPv4.

A configuração é aplicada somente ao computador em que foi definida. Se você selecionar **Usar endereços IPv4**, todas as conexões de saída do IBM Cognos nesse computador serão estabelecidas usando IPv4 e o dispatcher aceitará apenas conexões IPv4 recebidas. Se você selecionar **Usar endereços IPv6**, todas as conexões de saída do IBM Cognos nesse computador serão estabelecidas usando IPv6 e o dispatcher aceitará conexões IPv4 e IPv6 recebidas.

Os computadores do cliente IPv4 conseguem se comunicar com computadores de dispatcher configurados para IPv6.

Os nomes do host especificados dentro de um URI são resolvidos com base no valor da propriedade **Versão IP para resolução do nome do host**. Entretanto, se um URI tiver sido especificado com um endereço numérico, ele terá precedência sobre essa configuração e a comunicação ocorrerá utilizando IPv4.

Para o IBM Cognos Configuration aceitar endereços IPv6 nas propriedades do URI local, você deve iniciar o IBM Cognos Configuration com a opção -ipv6. É possível especificar a opção cada vez que você abre o IBM Cognos Configuration a partir da linha de comandos.

No Windows, é possível configurar a opção permanentemente incluindo a opção no atalho do menu Iniciar.

Configurando a Versão IP

Use o IBM Cognos Configuration para selecionar a versão IP.

Procedimento

1. Inicie o IBM Cognos Configuration.
2. Na janela **Explorer**, clique em **Ambiente**.
3. Clique na caixa **Valor** para **Versão IP para resolução do nome do host** e, a seguir. em **Use endereços IPv4** ou **Use endereços IPv6**.
4. No menu **Arquivo**, clique em **Salvar**.
5. Feche o IBM Cognos Configuration.

Configurando Manualmente o IBM Cognos Configuration para Iniciar com a Opção IPv6

É possível configurar manualmente o IBM Cognos Configuration para usar a opção IPv6 especificando a opção no comando start.

Procedimento

1. Acesse o diretório *install_location*/bin ou o *install_location*/bin64.
2. Inicie o IBM Cognos Configuration incluindo a opção IPv6 no comando da seguinte forma:
   - No Windows, digite
     ```
     cogconfig.bat -ipv6
     ```
   - No UNIX ou Linux, digite
     ```
     ./cogconfig.sh -ipv6
     ```
3. Edite as propriedades do URI que utilizam o formato IPv6, especifique os valores e, no menu **Arquivo**, clique em **Salvar**.

Configurando o IBM Cognos Configuration para Sempre Começar com a Opção IPv6 no Windows

É possível configurar o IBM Cognos Configuration para sempre começar usando a opção IPv6 em sistemas operacionais Microsoft Windows configurando a opção no atalho do menu Iniciar.

Procedimento

1. No menu **Iniciar**, clique com o botão direito em **IBM Cognos Configuration** e selecione **Propriedades**.
2. Na guia **Atalho**, na caixa **Destino**, digite `"install_location\bin\cogconfigw.exe -ipv6"`
3. Clique em **OK**.

Configuração do URI de descoberta de colaboração

É possível configurar o IBM Cognos Analytics e o IBM Cognos Workspace para usar o IBM Connections para a tomada de decisão colaborativa. A integração com o IBM Connections permite que usuários corporativos colaborem ao criar ou visualizar relatórios, executar análise ou monitorar áreas de trabalho. Os usuários têm acesso às atividades do IBM Connections de dentro do IBM Cognos Workspace e para a página inicial do IBM Connections de dentro do IBM Cognos Analytics e do IBM Cognos Workspace.

O URI de descoberta de Colaboração especifica o servidor IBM Connections a ser usado como o provedor de colaboração. Quando um URI é especificado, o suporte relacionado à colaboração é incluído no IBM Cognos Analytics da seguinte forma:

- um link é incluído na página de boas-vindas do portal do IBM Cognos Analytics. Se o usuário tiver acesso à página inicial do IBM Connections, o link será chamado **Acessar Minha Rede Social** e vinculará o usuário à página inicial. Se o usuário tiver acesso às atividades do IBM Connections, mas não à página inicial, o link será chamado **Minhas Atividades** e vinculará o usuário à página de atividades.
- um link com a página inicial do IBM Connections é incluído no menu Ativar no portal
- um link para a página inicial do IBM Connections é incluído no menu Ações no IBM Cognos Workspace
- o botão de menu **Colaborar** é incluído na barra do aplicativo da área de trabalho no IBM Cognos Workspace. Isto permite que o usuário crie ou visualize uma atividade da área de trabalho no IBM Connections.

Procedimento

1. No **IBM Cognos Administration**, na guia **Configuração**, clique em **Dispatchers e Serviços** para visualizar a lista de dispatchers.
2. Na barra de ferramentas, clique no botão Configurar Propriedades - configuração.
3. Clique na guia **Configurações**.
4. Para a categoria **Ambiente**, **URI de descoberta de colaboração**, digite o URI da seguinte maneira:

   `http://server_name:port_number/activities/serviceconfigs`

   Por exemplo, `http://server_name:9080/activities/serviceconfigs`

   em que *server_name* representa o nome do servidor no qual o IBM Connections está instalado.

5. Clique em **OK**.

Configurando o IBM Cognos Workspace

O IBM Cognos Workspace está incluído com o servidor IBM Cognos Analytics. Ele entrega recursos dinâmicos e customizáveis que permitem montar de maneira rápida e fácil áreas de trabalho interativas usando conteúdo do IBM Cognos, bem como origens de dados externos. Depois de testar se esse IBM Cognos Workspace está executando, configure o acesso às funções e aos recursos seguros.

Complete as tarefas de configuração a seguir.

__ • Configurar o acesso ao IBM Cognos Workspace.

__ • Configurar os Tipos MIME Suportados no Microsoft Internet Information Services.

Depois que as tarefas de configuração tiverem sido concluídas, é possível realizar as seguintes tarefas conforme necessário:

__ • Configurar um banco de dados para anotações .

__ • Configurar o IBM Cognos Workspace para usar o conteúdo de um TM1 Data Server.

__ • Configurar o IBM Cognos Workspace para acessar IBM Cognos TM1 Applications.

__ • Alterar os estilos em seus relatórios.

__ • Usar as amostras.

Configurando Acesso ao IBM Cognos Workspace ou às suas Funções

Configure o acesso ao IBM Cognos Workspace, concedendo as permissões necessárias para o recurso Painel Executivo para namespaces, usuários, grupos ou funções especificados.

É possível conceder acesso total ao IBM Cognos Workspace ou é possível conceder acesso apenas à função de publicação.

O IBM Cognos Analytics deve estar configurado e em operação para que seja possível configurar o acesso para o IBM Cognos Workspace.

Concedendo Acesso Total ao IBM Cognos Workspace

Para conceder acesso ao IBM Cognos Workspace e toda a sua funcionalidade, conceda permissões de execução e travessia para o recurso de Painel Executivo.

Informações adicionais sobre como configurar a permissão para que os usuários possam ser localizados em uma nota técnicahttp://www.ibm.com/support/docview.wss?uid=swg21498402 (www.ibm.com/support/docview.wss?uid=swg21498402) no website da IBM.

Procedimento

1. No portal do IBM Cognos Analytics, ative o **IBM Cognos Administration**.
2. Na guia **Segurança**, clique em **Capacidades**.
3. Localize o recurso **Painel Executivo**, clique no botão de ações  próximo do nome do recurso e selecione **Configurar Propriedades**.

4. Selecione a guia **Permissões**.
5. Conceda permissão de Execução a todos os grupos de usuários que devem ter acesso ao IBM Cognos Workspace e, em seguida, clique em **OK**.

Concedendo Acesso à Função de Publicação ao IBM Cognos Workspace

Para conceder acesso apenas à função de publicação no IBM Cognos Workspace, conceda permissões de passagem para o recurso Painel Executivo e permissões de execução para a função protegida Painéis de Publicação em Espaços de Colaboração.

Procedimento

1. No portal do IBM Cognos Analytics, ative o **IBM Cognos Administration**.
2. Na guia **Segurança**, clique em **Capacidades**.
3. Encontre e selecione a função **Painel executivo**.
4. Clique no botão de ações  próximo de **Painéis de Publicação em Espaços de Colaboração** e clique em **Configurar Propriedades**.
5. Selecione a guia **Permissões**.
6. Para definir permissões de acesso explicitamente para cada entrada, selecione **Substituir as permissões de acesso obtidas da entrada pai**.
7. Para cada grupo de usuários, selecione a caixa de seleção para a entrada e, na caixa ao lado da lista, selecione as caixas de seleção para conceder permissões à entrada.
8. Se desejar adicionar novas entradas à lista, clique em **Adicionar** e escolha como selecionar as entradas:
   - Para escolher dentre as entradas disponíveis, clique no namespace apropriado e depois assinale as caixas de seleção próximas dos usuários, grupos ou funções.
   - Para procurar por entradas, clique em **Procurar** e, na caixa Procurar string, digite a expressão que deseja buscar. Para opções de procura, clique em **Editar**. Localize a entrada que desejar e clique nela.
   - Para digitar o nome de entradas que você deseja incluir, clique em **Digitar** e digite os nomes de grupos, funções ou usuários usando o seguinte formato, em que um ponto e vírgula (;) separa cada entrada: *namespace*/*group_name*;*namespace*/*role_name*;*namespace*/*user_name*;

   Em seguida, é possível conceder permissões para cada nova entrada.
9. Clique em **OK**.

Configurando Tipos MIME Suportados no Microsoft Internet Information Services

Se você usar o Microsoft Internet Information Services (IIS) 6.0, para que o IBM Cognos Workspace seja carregado com êxito, deverá definir o tipo MIME que o IBM Cognos Workspace usa.

Procedimento

1. Abra o console de gerenciamento do Microsoft IIS.
2. Clique com o botão direito do mouse no nome do computador local e clique em **Propriedades**.
3. Clique em **Tipos de MIME**.
4. Clique em **Novo**.

5. Na caixa **Ramal**, digite **.cfg**.
6. Na caixa **Tipo MIME**, digite **text/plain**.
7. Aplique as novas configurações.

   As mudanças entrarão em vigor quando o processo do trabalho for atualizado. Para evitar espera, é possível reiniciar o World Wide Web Publishing Service. Para obter mais informações, procure na biblioteca online do Microsoft por *Manipulando Tipos MIME no Internet Explorer*.

Criando espaços de tabela para a tarefa manual e para o banco de dados de anotação no IBM Db2 on z/OS

Se você estiver usando o Db2 on z/OS, um administrador de banco de dados deverá executar scripts para criar os espaços de tabela necessários para a tarefa manual e para o banco de dados de anotações. O script deve ser modificado para substituir os parâmetros de espaço reservado com os adequados a seu ambiente.

Certifique-se de usar a convenção de nome para o Db2 on z/OS. Por exemplo, todos os nomes de parâmetros devem iniciar com uma letra e o comprimento não deve exceder seis caracteres. Para obter mais informações, consulte o Db2 Knowledge Center.

É possível usar o banco de dados de armazenamento de conteúdo ou um banco de dados separado para o banco de dados de tarefa manual e de anotações. Em qualquer dos casos, você deve executar os scripts para criar os espaços de tabela.

Procedimento

1. Conecte-se ao banco de dados como um usuário com privilégios para criar e arrastar tablespaces e para permitir a execução de instruções SQL.
2. Para criar os espaços de tabela de tarefas manuais, acesse o diretório *install_location*/configuration/schemas/hts/zosdb2.
   a. Faça uma cópia de backup do arquivo de script HTS_tablespaces.sql e salve o arquivo em outro local.
   b. Abra o arquivo de script HTS_TABLESPACES.sql original e use a tabela a seguir para ajudá-lo a substituir os parâmetros genéricos pelos parâmetros apropriados para seu ambiente.

Tabela 37. Nomes e descrições de parâmetros de espaço de tabela para tarefas manuais noDb2 for z/OS

Nome do parâmetro	Descrição
NCCOG	Especifica o nome do banco de dados.
DSN8G810	Especifica o nome do grupo de armazenamento.
BP32K	Especifica o nome do buffer pool de 32 k.

   Consulte o script para uma lista completa dos parâmetros necessários.
   c. Salve e execute o script.
   d. Abra o arquivo de script HTS2_CREATE_Db2zos.sql e use a tabela a seguir para ajudá-lo a substituir os parâmetros genéricos pelos parâmetros apropriados para seu ambiente.

Tabela 38. Nomes e descrições de parâmetros de espaço de tabela para tarefas manuais noDb2 for z/OS

Nome do parâmetro	Descrição
NCCOG	O nome do banco de dados.

Consulte o script para uma lista completa dos parâmetros necessários.

e. Salve e execute o script.

3. Para criar os espaços de tabela de anotações, acesse o diretório *install_location*/configuration/schemas/ans/zosdb2.
   a. Faça uma cópia de backup do arquivo de script ANN_TABLESPACES.sql e salve o arquivo em outro local.
   b. Abra o arquivo de script ANN_TABLESPACES.sql original e use a tabela a seguir para ajudá-lo a substituir os parâmetros genéricos pelos parâmetros apropriados para seu ambiente.

Tabela 39. Nomes e descrições de parâmetros de espaço de tabela para anotações noDb2 for z/OS

Nome do parâmetro	Descrição
NCCOG	O nome do banco de dados.
DSN8G810	O nome do grupo de armazenamento.
BP32K	O nome do buffer pool de 32 k.

Consulte o script para uma lista completa dos parâmetros necessários.

c. Salve e execute o script.
d. Abra o arquivo de script ANS2_CREATE_Db2zos.sql e use a tabela a seguir para ajudá-lo a substituir os parâmetros genéricos pelos parâmetros apropriados para seu ambiente.

Tabela 40. Nomes e descrições de parâmetros de espaço de tabela para anotações noDb2 for z/OS

Nome do parâmetro	Descrição
NCCOG	O nome do banco de dados.

Consulte o script para uma lista completa dos parâmetros necessários.

e. Salve e execute o script.

Configurando um Banco de Dados para Tarefas Manuais e Anotações

Por padrão, os dados usados para o recurso Tarefas Manuais e Anotações no IBM Cognos Workspace são armazenados no mesmo banco de dados que o armazenamento de conteúdo. É possível configurar um banco de dados separado para Human Tasks e Anotações.

Para configurar o banco de dados, primeiro é necessário criá-lo, além de uma conta de usuário na qual o banco de dados operará e, em seguida, configurar o recurso Human Tasks e Anotações para usar o novo banco de dados.

Procedimento

1. Crie um banco de dados usando as mesmas instruções que "Diretrizes para Criar o Armazenamento de Conteúdo" na página 8.

Se você estiver usando o IBM Db2 on z/OS para seu banco de dados, os espaços de tabela necessários deverão ser criados executando dois scripts. Para obter mais informações, consulte "Criando espaços de tabela para a tarefa manual e para o banco de dados de anotação no IBM Db2 on z/OS" na página 224.

2. Crie uma conta de usuário, que será usada para operar o banco de dados.
3. Na instância em que os Componentes da Camada de Aplicativos são instalados, inicie o IBM Cognos Configuration.
4. No **Explorer**, clique com o botão direito do mouse em **Serviços de Tarefa Manual e Anotação** e selecione **Novo Recurso** > **Banco de Dados**.
5. Na caixa de diálogo **Novo recurso - Banco de dados**, digite um nome para o banco de dados, selecione o tipo e clique em **OK**.
6. Na janela de propriedades de recursos do banco de dados, configure o seguinte:
   - Especifique os valores obrigatórios para todas as propriedades marcadas com um asterisco.
   - Especifique a **ID do usuário e senha** para a conta que opera o banco de dados.
7. No menu **Arquivo**, clique em **Salvar**.

   As credenciais de logon são imediatamente criptografadas.
8. Para testar a conexão com o novo banco de dados, no menu **Ações**, clique em **Testar**.
9. Repita essas etapas em cada instância de Componentes da Camada de Aplicativos e do Content Manager.

Configurando o IBM Cognos Workspace para Usar Dados do IBM Cognos TM1

Para poder usar dados do IBM Cognos TM1 no IBM Cognos Workspace, você deve modificar os arquivos de configuração na instalação do IBM Cognos Analytics.

Para configurar o servidor de dados TM1 para IBM Cognos Workspace, você deve executar as seguintes tarefas:

__ • Configurar informações de conexão para o TM1 Server.
__ • Configurar os nomes de seu servidor IBM Cognos TM1 conforme apareceriam no IBM Cognos Workspace.
__ • Opcionalmente, alterar o nome da pasta Visualizações.

Configure Informações de Conexão para o TM1 Server

Você deve modificar um arquivo de configuração para configurar informações de conexão para os TM1 Servers.

É fornecido um arquivo de contribuição de amostra com sua instalação do IBM Cognos Analytics. Se estiver usando uma instalação distribuída, o arquivo de configuração estará disponível nos computadores nos quais foram instalados os Componentes da Camada de Aplicativos.

Se o gateway do IBM Cognos Analytics estiver sendo executado em um computador diferente do computador do TM1 Web, assegure-se de usar nomes de domínio completos para os valores de nome do servidor, como `TM1WebHost`. Por exemplo, use `http://mycomputer.mydomain.com/ibmcognos` em vez de

http://*mycomputer*/ibmcognos. Além disso, é necessário usar os nomes completos de domínio para os valores de nome do servidor na seção **Ambiente** do IBM Cognos Configuration.

Procedimento

1. No computador em que instalou os Componentes da Camada de Aplicativos do IBM Cognos Analytics, acesse o diretório *install_location*\configuration\icd\contributions\contrib e renomeie o arquivo tm1_contribution.atom.sample como tm1_contribution.atom.
2. Abra o arquivo tm1_contribution.atom em um editor de texto.

   O arquivo contém três seções <atom:entry>. Deve-se alterar os valores de uma seção <atom:entry> para cada TM1 Server que desejar acessar no IBM Cognos Workspace. Se você tiver mais servidores TM1 que deseja incluir, deve-se incluir as seções <atom:entry> conforme necessário. Deve-se também comentar quaisquer seções <atom:entry> extras. A terceira seção <atom:entry> no arquivo de amostra já está comentada.

   A primeira seção <atom:entry> destina-se a um servidor TM1 que não usa autenticação do Cognos.

   A segunda seção <atom:entry> destina-se a um servidor TM1 que usa autenticação do Cognos.
3. Na seção <atom:entry> adequada para a autenticação necessária, substitua os valores de **TM1WebHostName** e **TM1HostName** pelo nome ou endereço IP do servidor da web TM1 e do servidor de dados TM1.

   Por exemplo, altere as seções destacadas da amostra.

   ```
   TM1WebHost=TM1WebHostName&amp;
   TM1WebVirtualDirectory=tm1web&amp;
   TM1Host=TM1HostName&amp;
   ```
4. Para um servidor TM1 que não usa a autenticação do IBM Cognos, altere as seções destacadas mostradas para o valor de TM1DataServer:

   ```
   TM1DataServer=TM1ServerHostWithoutCAM&amp;
   TM1username=admin&amp;TM1pass=apple
   ```

   Substitua **admin** e **apple** pelo ID do usuário e senha da conta do administrador que é usada para o servidor TM1.
5. Para um servidor TM1 que usa a autenticação do IBM Cognos, altere as seções destacadas mostradas para o valor TM1DataServer:

   ```
   TM1DataServer=CamAuthenticatedTM1ServerHost
   ```
6. Se você não estiver usando os valores padrão, altere as propriedades a seguir:
   - https

     Essa propriedade descreve o protocolo usado para o TM1 Web Server. Se o TM1 Web estiver em execução com HTTP seguro, substitua **0** por **1**.
   - TM1WebVirtualDirectory

     Essa propriedade é o nome do diretório virtual para o TM1 Web. Se o nome do diretório da Web TM1 não for tm1web, substitua o valor da propriedade TM1WebVirtualDirectory pelo nome correto.

     Por exemplo,

     ```
     TM1WebVirtualDirectory=planningweb&amp;
     ```
   - TM1Toolbar

     Esta propriedade determina se a barra de ferramentas interna está visível. Versões do TM1Web anteriores à versão 9.5.2 não permitem uma barra de ferramentas externa. O valor padrão de TM1Toolbar é **0**. Para exibir a barra de ferramentas interna, configure o valor para **1**.

7. Se estiver definindo diversas conexões do servidor TM1, crie uma seção <atom:entry> para cada servidor TM1.

   Todos os valores atom:id em todas as entradas .atom devem ser exclusivos. Por exemplo,

   ```
   <atom:entry>
     <atom:id>tag:ibm.cognos.icd.com,2010-01-01:/tm1_rootfeed_2
   </atom:id>
   ```

   ```
   <atom:entry>
     <atom:id>tag:ibm.cognos.icd.com,2010-01-01:/tm1_rootfeed_2b
   </atom:id>
   ```

   As amostras são exclusivas em razão de tm1_rootfeed_2 e tm1_rootfeed_2b.

   Certifique-se de usar nomes exclusivos para valores como **tm1_rootfeed_1**, **rootfeed_title_1** e **rootfeed_summary_1**.
8. Certifique-se de comentar a linha ou de excluir quaisquer seções <atom:entry> não utilizadas.
9. Salve e feche o arquivo.
10. Reinicie os serviços do IBM Cognos. Se você desejar alterar os nomes dos TM1 Servers, à medida que eles aparecem no IBM Cognos Workspace, poderá reiniciar os serviços após a próxima tarefa.

Configure os Nomes do IBM Cognos TM1 Server

É possível definir os nomes dos seus TM1 Servers como faria se eles aparecessem no IBM Cognos Workspace.

Se você usar idiomas diferentes do inglês, poderá criar arquivos de idioma adicionais para exibir os nomes no IBM Cognos Workspace.

Procedimento

1. No computador em que instalou os Componentes da Camada de Aplicativos do IBM Cognos Analytics, acesse o diretório *install_location*\configuration\icd\contributions\contrib.
2. Abra o arquivo chamado tm1_en.properties em um editor de texto.
3. Altere o texto que aparece após o sinal de igual (=) para fornecer um nome significativo para o TM1 Server definido para o título.

   Por exemplo, se você definiu uma conexão do servidor TM1 usando a seção rootfeed_title_1 no arquivo tm1_contribution.atom na tarefa anterior, altere o nome para que apareça como:

   ```
   rootfeed_title_1 = MyTM1Server
   ```
4. Altere a descrição da propriedade rootfeed_summary_1 para fornecer uma descrição significativa para o servidor TM1.

   Por exemplo, se você definiu um nome para a conexão do servidor TM1 usando rootfeed_title_1, altere o valor de rootfeed_summary_1 como a seguir:

   ```
   rootfeed_summary_1 = Detail about MyTM1Server
   ```
5. Inclua novos valores para cada TM1 Server que foi incluído no arquivo tm1_contribution.atom na tarefa anterior. Certifique-se de corresponder às seções rootfeed_title e rootfeed_summary com os valores definidos no arquivo tm1_contribution.atom.
6. Se o ambiente suportar diversos idiomas:
   - Faça uma cópia do arquivo tm1_en.properties.
   - Renomeie o arquivo como tm1_*language_code*.properties, em que *language_code* é o código de dois caracteres do idioma que você está usando, como ja ou es.

É fornecido um arquivo de propriedades em Francês de amostra: `tm1_fr.properties`.

7. Reinicie os serviços do IBM Cognos para que as mudanças entrem em vigor.

Altere o Nome da Pasta Visualizações

Opcionalmente, é possível alterar o nome que é exibido no IBM Cognos Workspace para a pasta **Visualizações**.

Por padrão, o IBM Cognos Workspace exibe uma pasta Aplicativos e uma pasta Visualizações para cada servidor TM1 identificado no arquivo `tm1_contribution.atom`. O nome da pasta Aplicativos é retornado pelo TM1 Server. O nome da pasta Visualizações é determinado por um arquivo de mensagens que é fornecido com o IBM Cognos Workspace.

Procedimento

1. Acesse o diretório *install_location*`\templates\ps\messages`.
2. Crie uma cópia do arquivo `tm1buxmsgs_en.xml` e nomeie-o usando o código de idioma adequado.

   É fornecido um arquivo de tradução em Francês de amostra: `tm1buxmsgs_fr.xml`.
3. Abra o novo arquivo de tradução em um editor XML.
4. Substitua a palavra `Views` na seção a seguir por um valor adequado:

   ```
   <string id="TM1_VIEWS" type="String" usage="TM1 views">Views</string>
   ```
5. Salve e feche o novo arquivo.
6. Repita as etapas para cada idioma suportado.

Configurando o IBM Cognos Workspace para Acessar IBM Cognos TM1 Applications

O servidor IBM Cognos Analytics pode acessar o Web client dos aplicativos IBM Cognos TM1 por meio de um iwidget externo que é exibido na área de janela de conteúdo da área de trabalho do IBM Cognos. Antes que o iwidget possa ser exibido, use a documentação do TM1 Applications para executar as tarefas a seguir.

Procedimento

1. Instale os Aplicativos do IBM Cognos TM1.
2. Configure os aplicativos IBM Cognos TM1 para interoperabilidade com o servidor IBM Cognos Analytics.

   Ao copiar o arquivo `icon_active_application.gif` para a pasta de imagens do portal do servidor do Cognos Analytics, copie também este arquivo para a pasta *install_location*`/webcontent/icd/feeds/images`.
3. Implemente seus aplicativos.

   Os aplicativos IBM Cognos TM1 geram uma URL, que é detectada pelo servidor IBM Cognos Analytics.

Resultados

A URL do TM1 Contributor é exibida em **Pastas Públicas** na área de janela de conteúdo do IBM Cognos Workspace.

Alterando o estilo de Objetos de Relatório no IBM Cognos Workspace

Ao arrastar um objeto de relatório em uma área de trabalho, ele aparece no estilo de gradiente prateado e azul do seu produto. É possível configurar o objeto de relatório para que apareça no estilo de autoria original, alterando uma propriedade global no arquivo de configuração IBM Cognos Viewer.

Os objetos de relatório que são afetados pela configuração global incluem consultas, análises, relatórios e partes de relatórios que foram criados usando o estilo do IBM Cognos Versão 1.x, o estilo da Versão 8.x e o estilo financeiro (balanço). Esses objetos irão assumir a configuração global mesmo se tiverem sido salvos antes da configuração global. As miniaturas de área de trabalho serão afetadas pela configuração global apenas se a miniatura for executada novamente.

Alguns objetos de relatório não são afetados pela configuração global e sempre serão renderizados no estilo criado, como relatórios do PowerPlay e miniaturas de objetos de relatório.

Procedimento

1. Para cada instância do Content Manager e dos Componentes da Camada de Aplicativos acesse o *diretório install_location*/webapps/p2pd/WEB-INF/classes.
2. Abra o arquivo viewerconfig.properties em um editor de texto.
3. Para fazer os objetos de relatório aparecerem no estilo original criado, altere o valor de **useAuthoredReportStyles** para true.
4. Salve o arquivo e, em seguida, reinicie os serviços.

Acessando as Amostras do IBM Cognos Workspace

As amostras do IBM Cognos Workspace são incluídas com as amostras do IBM Cognos Analytics.

Usuários de negócios podem acessar as amostras para o IBM Cognos Workspace selecionando a opção para abrir áreas de trabalho existentes e, em seguida, selecionando **Amostras** > **Modelos** > **Amostras do Cognos Workspace**.

Para obter mais informações sobre a instalação e a configuração das amostras, consulte o *Guia de Amostras do IBM Cognos Analytics*. Para obter mais informações sobre como usar as amostras, consulte o *Guia do Usuário do IBM Cognos Workspace*.

Configuração do roteador para testar a disponibilidade do dispatcher

Se você usar um roteador para distribuir solicitações para dispatchers do IBM Cognos, e o roteador puder testar a disponibilidade de um servidor usando uma URL de teste, é possível configurar o roteador para testar a disponibilidade de um dispatcher do IBM Cognos.

Procedimento

Configure o roteador para usar uma URL com o caminho /p2pd/servlet/ping.
Se o dispatcher não estiver pronto, a seguinte resposta é exibida:
503 Serviço não disponível
Se o dispatcher estiver pronto, a seguinte resposta é exibida:
200 OK

Configurando o IBM Cognos Analytics para trabalhar com outros produtos IBM Cognos

Alguns produtos IBM Cognos fornecem funcionalidades que não estão disponíveis no IBM Cognos Analytics.

É possível continuar a utilizar esses produtos no mesmo ambiente. Pode ser necessário executar tarefas de configuração adicionais para garantir que o IBM Cognos Analytics possa acessar objetos que foram criados usando outros produtos IBM Cognos. Exigências adicionais de acesso dependem de como se escolhe executar os dois produtos.

Ativando Agentes e Relatórios Programados para Origens de Dados do IBM Cognos Planning Contributor

Para executar agentes e relatórios programados, que são baseados nas origens de dados do IBM Cognos Planning Contributor, você deve especificar uma senha secreta compartilhada. Isso ajuda a garantir uma comunicação segura entre os servidores IBM Cognos Analytics e o Contributor Data Server.

Procedimento

1. No computador com Componentes da Camada de Aplicativos, inicie o IBM Cognos Configuration.
2. Na janela **Explorer**, clique em **Acesso a dados**, **IBM Cognos Planning**, **Servidor de dados contribuintes**.
3. Na janela **Propriedades**, clique na caixa **Valor** próxima da propriedade **Senha com Assinatura** e clique no botão de edição  quando ele aparecer.
4. Na caixa de diálogo **Valor - Senha de assinatura**, digite a senha que será assinada digitalmente.

   A senha faz distinção entre maiúsculas e minúsculas e deve corresponder à propriedade **Senha com Assinatura** que você configura nas propriedades IBM Cognos Series 7, Configuration Manager, **Cognos Planning/Cognos BI - Contributor Data Server/Geral**.
5. No menu **Arquivo**, clique em **Salvar**.

Resultados

Uma assinatura digital, baseada na senha, é criada. A assinatura digital é codificada pelo IBM Cognos Analytics e decodificada pelo Contributor Data Server.

Capítulo 8. Configurando provedores de autenticação

Os componentes do IBM Cognos são executados com dois níveis de acesso: anônimo e autenticado. Por padrão, o acesso anônimo fica ativado.

É possível utilizar ambos os tipos de logon com sua instalação. Se você optar por usar apenas logon autenticado, deverá desativar o acesso anônimo. Para obter informações adicionais, consulte Desativar acesso anônimo.

Para logon autenticado, você deve configurar componentes do IBM Cognos Analytics com um namespace apropriado para o tipo de provedor de autenticação em seu ambiente. É possível configurar vários namespaces para autenticação e, em seguida, escolha no tempo de execução qual namespace deseja utilizar. Para obter mais informações, consulte o *Guia de administração e segurança*.

Se você atualizou do ReportNet e o IBM Cognos detectar um namespace configurado que não está mais configurado, o namespace desconfigurado aparecerá na lista de provedores de autenticação no portal Administração. Configure o namespace se ainda precisar das informações de conta de usuário. Caso contrário, exclua o namespace. Além disso, ao atualizar de uma versão para outra, utilize o mesmo namespace de autenticação para ambas as versões. Caso contrário, o conteúdo seguro antigo não estará disponível porque a nova versão não pode conter as mesmas políticas, usuários, funções e grupos.

Os componentes do IBM Cognos suportam os seguintes tipos de servidores como fontes de autenticação:

- Servidor Active Directory
- Provedor de Autenticação Customizada
- Namespace do IBM Cognos Series 7
- LDAP
- Conexão do OpenID
- CA SiteMinder
- RACF
- SAP

Se utilizar mais de um computador com Content Manager, configure provedores de autenticação idênticos em cada local com o Content Manager. Isso significa que o tipo de provedor de autenticação selecionado e a forma como foi configurado devem ser idênticos em todos os locais para todas as plataformas. A configuração deve conter informações que sejam acessíveis a todos os Content Managers.

Quando o IBM Cognos é instalado em um único computador baseado em Linux, ou quando o Content Manager é instalado em um computador baseado em Linux, o IBM Cognos pode ser configurado para usar apenas servidores de diretório compatíveis com LDAP V3 e provedores customizados como fontes de autenticação.

Alguns provedores de autenticação requerem que bibliotecas externas para o ambiente do IBM Cognos estejam disponíveis. Se essas bibliotecas não estiverem disponíveis no Linux, o provedor de autenticação não poderá ser inicializado.

Se deseja configurar um dos seguintes como a origem de autenticação, é necessário instalar o Content Manager em um sistema operacional que ele suporte:

- Namespace do IBM Cognos Series 7 (Windows, Solaris, AIX)
- Active Directory Server (apenas Windows)
- SAP BW (Todos, exceto Power PC, z/OS, z/Linux)

Se ativar a segurança, será preciso configurar definições de segurança imediatamente depois de completar os processos de instalação e configuração. Para obter mais informações, consulte o *Guia de administração e segurança*.

Importante: Não desative a segurança após ativá-la. Configurações de permissão existentes farão referência a usuários, grupos ou papéis que não mais existem. Embora isso não afete como as permissões funcionam, um usuário administrando as configurações de permissão pode ver entradas "desconhecidas". Como essas entradas referem-se a usuários, grupos e papéis que não mais existem, é possível excluí-las facilmente. No entanto, entradas "desconhecidas" também podem aparecer se você não estiver autenticado em todos os namespaces. Neste cenário, não exclua entradas "desconhecidas".

Após você configurar um provedor de autenticação para componentes do IBM Cognos, é possível ativar a conexão única entre o ambiente do provedor de autenticação e os componentes do IBM Cognos. Isso significa que um usuário faz logon uma vez e pode, depois, trocar para um outro aplicativo sem que precise fazer logon novamente.

Os usuários podem selecionar namespaces quando efetuarem login no portal IBM Cognos Analytics. É possível ocultar namespaces Java Customizados e namespaces CA SiteMinder dos usuários. Para obter mais informações, consulte “Ocultação do namespace dos usuários durante o login” na página 256.

Desativando o acesso anônimo

Se desejar configurar o IBM Cognos Analytics apenas para logon autenticado, é preciso desativar o acesso anônimo ao aplicativo.

Por padrão, os componentes do IBM Cognos não requerem autenticação do usuário. Os usuários podem fazer logon anonimamente.

Procedimento

1. Em cada computador no qual o Content Manager está instalado, inicie o IBM Cognos Configuration.
2. Na janela **Explorer**, em **Segurança** > **Autenticação**, clique em **Cognos**.

   O namespace Cognos armazena informações sobre grupos e funções, contatos e listas de distribuição do IBM Cognos e assim por diante, e referências a objetos em outros namespaces de segurança.
3. Na janela **Propriedades**, clique na caixa próxima à propriedade **Permitir acesso anônimo** e selecione **Falso**.
4. No menu **Arquivo**, clique em **Salvar**.

Resultados

Agora você deve configurar um namespace para que os usuários tenham que fornecer credenciais de logon quando acessarem o IBM Cognos Analytics.

Restringindo o acesso de usuário ao namespace Cognos

É possível configurar o acesso ao IBM Cognos Analytics para que somente usuários que são membros de qualquer grupo ou função no namespace **Cognos** possam acessar o aplicativo.

Certifique-se de que você é membro da função integrada **Administrador do sistema** no namespace **Cognos** antes de ativar essa configuração.

Procedimento

1. Em cada computador que tiver o Content Manager, inicie o IBM Cognos Configuration.
2. Na janela **Explorer**, em **Segurança**, clique em**Autenticação**.
3. Na janela**Propriedades**, altere o valor de **Restringir o acesso de membros ao namespace interno?** para **Verdadeiro**.
4. No menu **Arquivo**, clique em **Salvar**.

O que Fazer Depois

Agora você deve remover o grupo **Todos** de alguns grupos e funções integrados do Cognos e assegurar que os usuários autorizados pertençam a pelo menos um grupo ou função do Cognos. Essas tarefas são executadas por administradores nas interfaces de administração do Cognos Analytics. Para obter informações adicionais, consulte o *IBM Cognos Analytics Managing Guide* ou o *IBM Cognos Analytics Administration and Security Guide*.

Configurando o Lightweight Third-Party Authentication

É possível configurar os componentes do IBM Cognos Analytics para usar o IBM Lightweight Third-Party Authentication (LTPA). As práticas descritas nesse tópico são baseadas no ambiente distribuído do Cognos Analytics 11.0.7 com o IBM Tivoli Directory Server LDAP ou com o Microsoft Active Directory como fontes de autenticação.

Para implementar o LTPA, o Cognos Analytics deve ser configurado para usar uma fonte de autenticação configurada no contêiner do WebSphere Liberty no qual ele é executado. É possível configurar a conexão única entre o Cognos Analytics e o WebSphere Liberty usando a configuração de mapeamento de identidade no namespace do Cognos. Por exemplo, é possível configurar o WebSphere Liberty para usar um servidor LDAP ou Active Directory para autenticação e, em seguida, configurar o Cognos Analytics para usar o mesmo LDAP ou o Active Directory e configurar o mapeamento de identidade para usar REMOTE_USER.

Para o Cognos Analytics, isso significa que um usuário deve ser autenticado para uma identidade designada à sessão HTTP antes de acessar o Cognos Analytics dentro de mesma sessão. A autenticação é concluída apresentando credenciais para um sistema de segurança externo para Cognos. O sistema de segurança pode fornecer a identidade e algum tipo de informação de credenciais adequadas para estabelecer a conexão única para outros sistemas, geralmente na forma de um token SSO. Candidatos típicos para tais sistemas de segurança são proxies de autenticação, como o IBM Tivoli WebSEAL, o Oracle Oblix, o Computer Associates SiteMinder ou quaisquer outras soluções de software ou hardware que podem autenticar uma sessão HTTP e persistir essa autenticação em um token.

O WebSphere Liberty tem muitas opções diferentes para autenticação de usuários. Para obter mais informações, consulte a documentação do WebSphere Liberty: https://www.ibm.com/support/knowledgecenter/en/SSD28V_8.5.5/com.ibm.websphere.wlp.nd.iseries.doc/ae/twlp_sec.html

Configurando o LTPA usando um namespace LDAP

O procedimento a seguir descreve como configurar o LTPA para o Cognos Analytics ao usar o LDAP do IBM Tivoli Directory Server como a fonte de autenticação.

Para obter detalhes sobre como configurar o LDAP, consulte "Configurando componentes do IBM Cognos para uso com LDAP" na página 256

Procedimento

1. Em cada local em que você instalou o Content Manager, abra o IBM Cognos Configuration.
2. Na janela **Explorer**, em **Segurança**, clique com o botão direito do mouse em **Autenticação** e, em seguida, clique em **Novo Recurso** > **Namespace**.
3. Na caixa **Nome**, digite um nome para o namespace de autenticação.
4. Na lista **Tipo**, selecione **LDAP – Valores padrão gerais**.
5. Na janela **Propriedades**, na propriedade **ID do namespace**, especifique um identificador exclusivo para o namespace.
6. Defina as seguintes propriedades:

   Host e porta
   O host completo e a porta do servidor LDAP.

   Nome distinto de base
   Por exemplo, `o=organization_name.com`

   Consulta de usuário
   Por exemplo, `uid=${userID},ou=people`

   Usar identidade externa
   `Verdadeiro`

   Mapeamento de identidade externa
   Por exemplo, `uid=${environment("REMOTE_USER")},ou=people`
7. Se desejar que o provedor de autenticação LDAP se vincule ao servidor de diretório usando **Ligar DN de usuário e senha** quando executar procuras, em seguida, especifique esses valores.

   Se não houver valores especificados, o provedor de autenticação LDAP vincula como anônimo.

   Se o mapeamento de identidade externa estiver ativado, **Vincular DN do usuário e senha** é utilizado para todos os acessos LDAP. Se o mapeamento de identidade externa não estiver ativado, **Vincular DN do usuário e senha** são usados apenas quando um filtro de procura for especificado para a propriedade **Consulta de usuário**. Nesse caso, quando o DN de usuário está estabelecido, solicitações subsequentes para o servidor LDAP são executadas sob o contexto de autenticação do usuário.
8. Se você não usa o mapeamento de identidade externa, use as credenciais de ligação para procurar pelo servidor de diretórios LDAP usando as seguintes etapas:
   - Certifique-se de que **Utilizar identidade externa** esteja definido como **Falso**.
   - Defina **Usar credenciais de ligação para buscar** como **Verdadeiro**.

- Especifique a ID e a senha do usuário para **Vincular DN do usuário e senha**.

Se não especificar um ID do usuário e senha e o acesso anônimo for ativado, a procura será feita usando anônimo.

9. Verifique as configurações de mapeamento para os objetos e atributos necessários.

   Dependendo da configuração do LDAP, você pode precisar alterar alguns valores padrão para garantir a comunicação bem-sucedida entre componentes do IBM Cognos e o servidor LDAP.

   Os atributos LDAP mapeados para a propriedade **Nome** em **Mapeamento de pastas**, **Mapeamentos de grupos** e **Mapeamentos de contas** devem estar acessíveis a todos os usuários autenticados. Além disso, a propriedade **Nome** não pode ficar em branco.

10. No menu **Arquivo**, clique em **Salvar**.
11. Crie um arquivo XML chamado `local-server.xml` e coloque-o no diretório *install_location*`/configuration`.
12. No arquivo `local-server.xml`, insira valores que sejam apropriados para seu ambiente:

```
<?xml version="1.0" encoding="UTF-8"?>
<server>
 <featureManager>
  <feature>ldapRegistry-3.0</feature>
  <feature>appSecurity-2.0</feature>
 </featureManager>
 <ldapRegistry id="id" realm="realm"
  host="host" port="port" ignoreCase="true"
  baseDN="o=basedn" ldapType="Custom" sslEnabled="false">
  <idsFilters
   userFilter="(uid=%v,ou=people)"
   userIdMap="*:uid"
   groupFilter='(objectclass=groupofnames)'
   groupIdMap="*:cn" />
 </ldapRegistry>
      <webAppSecurity allowFailOverToBasicAuth="true"
displayAuthenticationRealm="true"/>
</server>
```

13. Se o Cognos Analytics estiver configurado para usar SSL, consulte o "Configurando o Protocolo SSL para Componentes do IBM Cognos" na página 184 para obter mais informações.
14. Para verificar a configuração, efetue logon em `http://`*host*`:`*port*`/bi` ou em `https://`*host*`:`*port*`/bi` para sistemas ativados para SSL, em que host é o domínio completo do host do Cognos Analytics.

    A página de logon do Cognos Analytics não deverá ser exibida. Em vez disso, o navegador exibirá um prompt para que você efetue logon.

O que Fazer Depois

Se você deseja configurar a conexão única (SSO) entre o aplicativo Cognos Analytics que foi configurado com a autenticação LTPA e se o aplicativo estiver implementado em uma instância do WebSphere, instale a chave do WebSphere em cada dispatcher do Cognos Analytics no qual o LTPA foi configurado e atualize o arquivo `local-server.xml` com o elemento `<ltpa>` a seguir:

```
<ltpa keysFileName="yourLTPAKeysFileName.keys"
keysPassword="keysPassword" expiration="120" />
```

Para obter mais informações, consulte a Documentação do WebSphere Liberty.

Configurando o LTPA usando um namespace do Active Directory

O procedimento a seguir descreve como configurar o LTPA para o Cognos Analytics com o Microsoft Active Directory como a fonte de autenticação.

Procedimento

1. Em cada local em que você instalou o Content Manager, abra o IBM Cognos Configuration.
2. Na janela **Explorer**, em **Segurança**, clique com o botão direito do mouse em **Autenticação** e, em seguida, clique em **Novo Recurso** > **Namespace**.
3. Na caixa **Nome**, digite um nome para o namespace de autenticação.
4. Na lista **Tipo**, selecione **LDAP - Valores padrão para Active Directory** e, em seguida, clique em **OK**.

   O novo recurso provedor de autenticação aparece na janela **Explorer**, no componente **Autenticação**. Valores padrão são gerados para você. Marque-os e faça mudanças conforme necessário.
5. Na janela **Propriedades**, na propriedade **ID do Namespace**, especifique um identificador exclusivo para o namespace.

   Dica: Não use dois pontos (:) na propriedade ID do namespace.
6. Especifique os valores para todas as outras propriedades necessárias para garantir que os componentes do IBM Cognos possam localizar e usar seu provedor de autenticação existente.
   - Para **Consulta de usuário**, insira `(sAMAccountName=${userID})`
   - Se você usa conexão única, para **Usar identidade externa**, configure o valor para **True**.
   - Se você usa conexão única, para **Mapeamento de identidade externa**, insira `(sAMAccountName=${environment("REMOTE_USER")})`

     Se desejar remover o nome de domínio da variável REMOTE_USER, insira `(sAMAccountName=${replace(${environment("REMOTE_USER")}, "domain\\","")})`.

     Importante: Certifique-se de usar apenas a variável REMOTE_USER. Utilizar outra variável pode causar uma vulnerabilidade de segurança.
   - Para **Ligar DN do usário e senha**, insira **user@domain**.
   - Para **Identificador Exclusivo**, insira `objectGUID`
7. Crie um arquivo XML chamado `local-server.xml` e coloque-o no diretório *install_location*/configuration.
8. No arquivo `local-server.xml`, insira valores que sejam apropriados para seu ambiente:

```
<?xml version="1.0" encoding="UTF-8"?>
<server>
 <featureManager>
  <feature>ldapRegistry-3.0</feature>
  <feature>appSecurity-2.0</feature>
 </featureManager>
 <ldapRegistry id="id" realm="realm"
 host="host" port="port" ignoreCase="true"
 baseDN="DC=dc,DC=dc,DC=dc" bindDN="CN=doejohn,
              OU=Users,DC=dc,DC=dc,DC=dc"
 bindPassword="password" ldapType="Microsoft Active Directory" sslEnabled="false">
  <actived Filters
   userFilter="(&amp;(sAMAccountName=%v)(objectcategory=user))"
```

```
    groupFilter="(&amp;(cn=%v)(objectcategory=group))"
    userIdMap="user:sAMAccountName"
    groupIdMap="*:cn"
    groupMemberIdMap="memberOf:member" >
   </actived Filters>
  </ldapRegistry>
  <webAppSecurity allowFailOverToBasicAuth="true"
displayAuthenticationRealm="true"/>
</server>
```

9. Se o Cognos Analytics estiver configurado para usar SSL, consulte o "Configurando o Protocolo SSL para Componentes do IBM Cognos" na página 184 para obter mais informações.
10. Para verificar a configuração, efetue logon em `http://host:port/bi` ou em `https://host:port/bi` para sistemas ativados para SSL, em que host é o domínio completo do host do Cognos Analytics.

    A página de logon do Cognos Analytics não deverá ser exibida. Em vez disso, o navegador exibirá um prompt para que você efetue logon.

O que Fazer Depois

Se você deseja configurar a conexão única (SSO) entre o aplicativo Cognos Analytics que foi configurado com a autenticação LTPA e se o aplicativo estiver implementado em uma instância do WebSphere, instale a chave do WebSphere em cada dispatcher do Cognos Analytics no qual o LTPA foi configurado e atualize o arquivo `local-server.xml` com o elemento `<ltpa>` a seguir:

```
<ltpa keysFileName="yourLTPAKeysFileName.keys"
keysPassword="keysPassword" expiration="120" />
```

Para obter mais informações, consulte a Documentação do WebSphere Liberty.

Provedor de autenticação OpenID Connect

OpenID Connect é uma camada de identidade simples na parte superior do protocolo OAuth 2.0. Ele é usado para identidade federada e autenticação com vários aplicativos que usam o mesmo provedor de identidade. O OpenID Connect é o provedor de autenticação baseado na web preferencial se você desejar federar o IBM Cognos Analytics com outros aplicativos.

OpenID Connect é um padrão moderno que incorpora os padrões OpenID e OAuth 2.0. É suportado para instalações no local e na nuvem do Cognos Analytics.

O Cognos Analytics suporta os seguintes tipos de provedores de identidade OpenID Connect:

- ADFS (Active Directory Federation Services)
- Azure AD (Active Directory)
- Google
- IBMid (provedor de identidade IBM)
- OKTA
- Ping
- SalesForce
- SiteMinder

Dica: Entre em contato com o administrador do provedor de identidade em sua organização, ou a organização de vendas e suporte, para descobrir qual versão do produto você deve usar.

Proxy de autenticação do OpenID Connect Aplica-se à versão 11.0.10 e a versões subsequentes, a menos que seja substituído de outra forma

O Cognos Analytics agora fornece outro tipo de provedor, 'Proxy de Autenticação do OpenID Connect' no Cognos Configuration. Esse menu oferece a opção de ter um Provedor de Conexão Confiável (TSP) para o OpenID Connect. Semelhante às entradas do OpenID Connect, será exibida a lista de Provedores de Identidade atualmente suportados.

Entradas de definição de configuração adicionais em Propriedades avançadas agora estão visíveis. Será necessário configurar a solicitação que você deseja transmitir para o provedor real, assim como o ID de namespace do provedor real.

- Nome da solicitação da identidade: especifica o nome da solicitação que será fornecido para o namespace de destino (por exemplo, John Doe)
- Nome do ambiente confiável: especifica o nome da variável de ambiente que será usado para transferir a solicitação para o namespace de destino (por exemplo, REMOTE_USER)
- ID de namespace de redirecionamento: especifica o ID do namespace que será chamado com a solicitação obtida do provedor de identidade do OpenID (por exemplo, LDAP)

Alavancando a conexão única do provedor de identidade

Se seu provedor de identidade OpenID Connect suporta conexão única e a autenticação de dois fatores, o Cognos Analytics pode alavancar essa funcionalidade.

Se o provedor de identidade não suporta conexão única, quando um usuário fizer uma solicitação de autenticação para o Cognos Analytics, esse usuário será redirecionado para a página de logon do provedor de identidade OpenID Connect. Depois de fornecer as informações necessárias, o usuário é redirecionado de volta para o Cognos Analytics com um código de autorização que é resgatado por um token de ID que contém a identidade do usuário. O usuário pode então acessar o Cognos Analytics.

Se o provedor de identidade suportar conexão única, o usuário receberá o token de ID quando fizer a solicitação de autenticação para o Cognos Analytics, e poderá acessar o aplicativo imediatamente.

Federando o IBMid com o provedor de identidade SAML 2.0

IBMid é o provedor de identidade IBM OpenID Connect. Se o seu provedor de identidade (IdP) não suporta o OpenID Connect, mas suporta o SAML 2.0, será possível usar o IBMid para configurar um namespace do OpenID Connect como seu provedor de autenticação no Cognos Analytics. Basta escolher IBMid como seu provedor de identidade ao configurar o namespace do OpenID Connect.

Com esta configuração de namespace, é possível federar o Cognos Analytics com a maioria dos provedores de identidade SAML 2.0. Como resultado, quando os usuários efetuarem logon no Cognos Analytics, eles serão redirecionados para a página de conexão do IBMid na qual digitam seu endereço de e-mail. Se o endereço de e-mail for reconhecido pelo IBMid, os usuários serão redirecionados para a página de logon do provedor de identidade SAML 2.0 de sua organização. Nesta página, os usuários concluem o processo de autenticação fornecendo suas

credenciais. Em seguida, eles podem acessar o Cognos Analytics.

Configurando um namespace do OpenID Connect

Para usar um provedor de identidade OpenID Connect com o IBM Cognos Analytics, você deve configurar um namespace do OpenID Connect.

Se você usar o IBMid como seu provedor de identidade OpenID Connect, consulte Gerenciando namespaces do OpenID Connect para obter informações adicionais.

Se os usuários tiverem problemas de autenticação depois de você configurar com sucesso seu namespace do OpenID Connect, use a criação de log de diagnóstico no componente **Gerenciar** do Cognos Analytics para resolver problemas. É preciso criar um novo tópico de criação de log que seja baseado no tópico **AAA** predefinido. Modifique o tópico de criação de log **AAA** incluindo nele o seguinte código:

```
{
"loggerDefinitions": [
{
"loggerName": "com.ibm.cognos.camaaa.internal.OIDC",
"level": "DEBUG",
"additivity": true
}
],
"topicName": "OIDC"
}
```

Para obter informações adicionais sobre a criação de log de diagnóstico, consulte Tipos e arquivos de criação de log.

Procedimento

1. Abra o IBM Cognos Configuration no computador do Content Manager.
2. Em **Segurança** > **Autenticação**, clique com o botão direito e selecione **Novo recurso** > **Espaço de nome**.
3. Para **Tipo (Grupo)**, selecione **OpenID Connect**.
4. Para **Tipo**, selecione um dos provedores de identidade da lista suspensa que inclui os provedores de identidade suportados.
5. Digite o nome do namespace no campo **Nome** e, em seguida, clique em **OK**.

   O novo namespace é incluído na área de janela **Explorer** em **Segurança** > **Autenticação**, e suas propriedades são exibidas na área de janela de propriedades.
6. Especifique valores para as propriedades de namespace.

   Dica: As informações sobre cada propriedade são exibidas na interface com o usuário quando se clica na propriedade.

   - O **ID de namespace** é usado no CAMID.
   - Especifique valores para **Terminal de descoberta**, **Identificador de cliente** e **Segredo do cliente OpenID Connect**, conforme sugerido pelo administrador do OpenID Connect.
   - Atualize a **URL de retorno** com sua URL de gateway ou de dispatcher, conforme mostrado no exemplo a seguir:

     `http://mycompany:9300/bi/completeAuth.jsp`

     Se você usar um balanceador de carga em seu ambiente, inclua a entrada DNS do balanceador de carga na **URL de retorno** na frente dos nós de gateway ou de dispatcher, conforme mostrado no exemplo a seguir:

`https://MyLoadbalancerDNS.mycompany.com:443/ibmcognos/bi/completeAuth.jsp`

Neste exemplo, o gateway do Cognos Analytics é instalado no servidor da web.

Se estiver usando um conjunto de nós de dispatcher atrás do balanceador de carga onde o gateway do Cognos Analytics não esteja instalado no servidor da web, a **URL de retorno** pode ser semelhante à seguinte:

`https://MyLoadbalancerDNS.mycompany.com:9300/bi/completeAuth.jsp`

Dica: As propriedades de **Multilocação** não precisam ser especificadas agora.

7. Importe o certificado da autoridade de certificação raiz do OpenID Connect para o keystore do Cognos Analytics usando o Third-Party Certificate Tool.
   - Em sistemas operacionais UNIX ou Linux, digite `ThirdPartyCertificateTool.sh -i -T -r cert.cer -p NoPassWordSet`
   - Em sistemas operacionais Windows, digite `ThirdPartyCertificateTool.bat -i -T -r cert.cer -p NoPassWordSet`

   Dica: Substitua a variável *cert* pelo nome do arquivo de certificado que é usado pelo provedor de identidade OpenID Connect. Para IBMid, o nome do arquivo é `blueid.cer`.
   O comando importa o conteúdo para o arquivo `CAMKeystore` no diretório `certs` usando a senha especificada.
8. Execute as mesmas etapas de configuração em seu computador com Content Manager de backup.
9. Reinicie o serviço IBM Cognos no Content Manager e nos computadores com Content Manager de backup.

Resultados

Todos os usuários que estão registrados com o provedor de identidade OpenID Connect agora devem ter acesso ao Cognos Analytics.

Configurando Componentes do IBM Cognos para Usar o Active Directory Server

Se instalar o Content Manager em um computador de sistema operacional Microsoft Windows, é possível configurar um namespace do Active Directory como uma fonte de autenticação.

Se instalar o Content Manager em um computador baseado em UNIX, você deve em vez disso usar um namespace do LDAP para configurar o Active Directory como sua fonte de autenticação. Se instalar um Content Manager em uma combinação de computadores Windows e UNIX, você deve usar um namespace LDAP para configurar o Active Directory para todos os Content Managers. Ao utilizar o namespace de LDAP para autenticar em relação ao Servidor do Active Directory, ficará limitado somente aos recursos do LDAP. Você não tem acesso a recursos do Active Directory, como propriedades avançadas para domínios e conexão única com delegação de Kerberos.

Se instalar o Content Manager em um computador baseado em Linux, as mesmas restrições se aplicam ao UNIX. É preciso utilizar um namespace do LDAP para configurar o Active Directory como origem de autenticação.

Se quiser usar Microsoft SQL Server ou Microsoft Analysis Server como uma origem de dados e usar conexão única para autenticação, será necessário usar o Active Directory como fonte de autenticação.

Não é possível conectar ao Catálogo global do Active Directory, que é um servidor de cache para o Servidor do Active Directory. Se a conexão utiliza a porta 3268, será preciso alterá-la. Por padrão, o Servidor do Active Directory utiliza a porta 389.

Procedimento

1. Configure os componentes do IBM Cognos para usarem um namespace Active Directory Server
2. Ative a comunicação segura para o servidor do Active Directory, se necessário.
3. Ative a conexão única entre o Active Directory e os componentes do IBM Cognos

Configurando um namespace do Active Directory

É possível utilizar o Servidor do Active Directory como seu provedor de autenticação.

Você também tem a opção de disponibilizar propriedades de usuário customizadas a partir do Active Directory Server para componentes do IBM Cognos.

Antes de Iniciar

Para o IBM Cognos trabalhar corretamente com o Active Directory Server, certifique-se de que o grupo Usuários Autenticados tenha privilégios de Leitura para a pasta do Active Directory em que os usuários estão armazenados.

Se estiver configurando um namespace do Active Directory para suportar conexão única com uma origem de dados do Microsoft SQL Server ou Microsoft Analysis Server, certifique-se da seguinte configuração:

- O gateway do IBM Cognos é instalado em um servidor da web IIS que é configurado para Autenticação Integrada no sistema operacional Microsoft Windows.
- O gateway é designado ao website intranet local em seu navegador da web.
- O Content Manager está instalado em um servidor Windows 2008 ou Windows 2012.
- Content Manager, Componentes da Camada de Aplicativos, servidor da web IIS e o servidor de origem de dados (Microsoft SQL Server ou Microsoft Analysis Server) pertencem ao domínio do Active Directory.
- A conexão de origem de dados para o Microsoft SQL Server ou Microsoft Analysis Server está configurada para **Namespace Externo** e o namespace deve ser o namespace do Active Directory.

Para obter mais informações sobre origens de dados, consulte o *Guia de administração e segurança do IBM Cognos Analytics*.

Procedimento

1. Em cada local em que você instalou o Content Manager, abra o IBM Cognos Configuration.
2. Na janela **Explorer**, em **Segurança**, clique com o botão direito do mouse em **Autenticação** e, em seguida, clique em **Novo Recurso** > **Namespace**.

3. Na caixa **Nome**, digite um nome para o namespace de autenticação.
4. Na lista **Tipo**, clique no namespace apropriado e clique em **OK**.

   O novo recurso do provedor de autenticação aparece na janela **Explorer**, no componente Autenticação.
5. Na janela **Propriedades**, na propriedade **ID do namespace**, especifique um identificador exclusivo para o namespace.
6. Especifique os valores para todas as outras propriedades necessárias para garantir que os componentes do IBM Cognos possam localizar e usar seu provedor de autenticação existente.
7. Especifique os valores para a propriedade **Host e porta**.

   Para suportar o failover do Servidor do Active Directory, é possível especificar o nome do domínio em vez de um controlador de domínio específico. Por exemplo, utilize *mydomain*.com:389 em vez de dc1.*mydomain*.com:389.
8. Se desejar procurar detalhes quando a autenticação falhar, especifique a ID e senha do usuário para a propriedade **Credenciais de ligação**.

   Utilize as credenciais de um usuário do Servidor do Active Directory que tenha privilégios de busca e leitura para esse servidor.
9. No menu **Arquivo**, clique em **Salvar**.
10. Teste a conexão em um novo namespace. Na janela **Explorer**, em **Autenticação**, clique com o botão direito no novo recurso de autenticação e clique em **Testar**.

    É solicitado que insira credenciais para um usuário no namespace para concluir o teste.

    Dependendo de como seu namespace estiver configurado, será possível inserir um ID do usuário válido e senha para um usuário no namespace ou o DN do usuário de ligação e senha.

Resultados

IBM Cognos carrega, inicializa e configura as bibliotecas do provedor para o namespace.

Disponibilizando Propriedades de Usuário Customizadas para o Active Directory para Componentes do IBM Cognos

É possível usar atributos de usuário arbitrários do Active Directory Server nos componentes do IBM Cognos. Para tal configuração, é preciso adicionar esses atributos como propriedades customizadas para o namespace do Active Directory.

As propriedades customizadas estão disponíveis como parâmetros de sessão no Framework Manager. Para obter mais informações sobre os parâmetros de sessão, consulte o *Guia do Usuário do Framework Manager*

Utilize também as propriedades customizadas dentro dos blocos de comando para configurar sessões e conexões do Oracle. Utilize blocos de comando com conexões leves do Oracle e bancos de dados privados virtuais. Para obter mais informações, consulte o *IBM Cognos AnalyticsGuia de administração e segurança*.

Procedimento

1. Em cada local em que você instalou o Content Manager, abra o IBM Cognos Configuration.
2. Na janela **Explorer**, em **Segurança** > **Autenticação**, clique no namespace do Active Directory.

3. Na janela **Propriedades**, clique na coluna **Valor** para **Propriedades Customizadas** e clique no ícone de edição.
4. Na janela **Valor - Propriedades customizadas**, clique em **Adicionar**.
5. Clique na coluna **Nome** e digite o nome que você quer que os componentes do IBM Cognos usem para o parâmetro de sessão.
6. Clique na coluna **Valor** e digite o nome do parâmetro de conta no servidor do Active Directory.
7. Repita as etapas de 4 a 6 para cada coluna customizada.
8. Clique em **OK**.
9. No menu **Arquivo**, clique em **Salvar**.

Ativação da comunicação segura para o Servidor do Active Directory

Se estiver utilizando uma conexão SSL para o Servidor do Active Directory, será preciso copiar o certificado do Servidor do Active Directory ao local com o Content Manager.

Procedimento

1. Em cada computador com Content Manager, utilize o navegador web para conectar ao Servidor do Active Directory e copie o certificado raiz da CA para um local com o Content Manager.
2. Inclua o certificado raiz CA no armazenamento de certificados da conta que você está usando para a atual sessão do IBM Cognos:
   - Se estiver executando a sessão do IBM Cognos sob uma conta do usuário, use o mesmo navegador da Web da etapa 1 para importar o certificado raiz CA no armazenamento de certificados para sua conta do usuário.

     Para obter informações, consulte a documentação de seu navegador web.
   - Se estiver executando a sessão do IBM Cognos sob a conta local, use o Microsoft Management Console (MMC) para importar o certificado raiz CA no armazenamento de certificados para o computador local.

     Para obter mais informações, consulte a documentação do MMC.
3. No IBM Cognos Configuration, reinicie o serviço:
   - Na janela **Explorer**, clique em **Serviço do IBM Cognos**, **IBM Cognos**.
   - No menu **Ações**, clique em **Reiniciar**.

Inclusão ou exclusão de domínios utilizando Propriedades avançadas

Quando você configura um namespace de autenticação para IBM Cognos, os usuários de apenas um domínio podem efetuar login. Usando as propriedades Avançadas para Active Directory Server, os usuários de domínios relacionados (pai/filho) e de árvores de domínios não relacionados na mesma floresta também podem efetuar login. Não há suporte entre florestas; deve haver um namespace para cada floresta.

Se você configurar um parâmetro denominado chaseReferrals como true, os usuários no domínio autenticado original e todos os domínios-filhos da árvore de domínio poderão efetuar login no IBM Cognos. Os usuários de um domínio pai do domínio autenticado original ou em uma árvore de domínio diferente não podem efetuar login.

Se você configurar o parâmetro denominado MultiDomainTrees como true, os usuários em todas as árvores de domínio na floresta poderão efetuar login no IBM Cognos.

Procedimento

1. Em cada local em que você instalou o Content Manager, abra o IBM Cognos Configuration.
2. Na janela **Explorer**, em **Segurança** > **Autenticação**, clique no namespace do Active Directory.
3. Na janela **Propriedades**, especifique a propriedade **Host e porta**:
   - Para usuários em um domínio, especifique o host e a porta de um controlador de domínio para o domínio único.
   - Para usuários em uma árvore de domínio, especifique o host e a porta do controlador de nível superior para a árvore de domínio.
   - Para usuários em todas as árvores de domínio na floresta, especifique o host e a porta de qualquer controlador de domínio na floresta.
4. Clique na coluna Valor de **Propriedades Avançadas** e clique no ícone de edição.
5. Na janela **Valor - Propriedades avançadas**, clique em **Adicionar**.
6. Especifique duas novas propriedades, **chaseReferrals** e **MultiDomainTrees**, com os valores da seguinte tabela:

Tabela 41. Configurações de Propriedades Avançadas

Autenticação para	**chaseReferrals**	**MultiDomainTrees**
Um domínio	Falso	Falso
Uma árvore de domínio	Verdadeiro	Falso
Todas as árvores de domínio na floresta	Verdadeiro	Verdadeiro

7. Clique em **OK**.
8. No menu **Arquivo**, clique em **Salvar**.

Ativar a Conexão Única entre o Active Directory Server e os Componentes do IBM Cognos

Por padrão, o provedor do Active Directory usa a autenticação do Kerberos. Ele integra-se com o servidor da web Microsoft Internet Information Services (IIS) para conexão única se a autenticação do Windows (anteriormente denominada Desafio/Resposta do NT) estiver ativada no servidor da web IIS.

Se a autenticação do Windows for ativada, será solicitado que reinsira as informações de autenticação ao acessar o conteúdo do IBM Cognos que é assegurado pelo namespace do Active Directory.

Se usar a autenticação do Kerberos, será possível escolher usar o Service for User (S4U). O S4U permite que os usuários acessem o IBM Cognos Analytics a partir de computadores que não estão no domínio do Active Directory. Para ativar o S4U, você deve usar a delegação restrita.

Por exemplo, tenha usuários cujos computadores não pertençam ao domínio, mas que tenham a conta de domínio. Quando eles abrem seus navegadores da web, é

solicitada sua conta de domínio. No entanto, eles obtém o ticket Kerberos apenas com privilégio de Identidade, o que impede que eles sejam autenticados para o IBM Cognos Analytics. Para resolver esse problema, é possível usar o S4U.

Se não desejar a autenticação do Kerberos, será possível configurar o provedor para acessar a variável de ambiente **REMOTE_USER** para atingir a conexão única.

Importante: Certifique-se de usar apenas a variável **REMOTE_USER**. Utilizar outra variável pode causar uma vulnerabilidade de segurança.

Para ativar a conexão única para usar a autenticação do Kerberos, você deve garantir a conclusão das seguintes tarefas:

1. Configure a autenticação do Windows no servidor da web Microsoft IIS para o aplicativo ibmcognos/cgi-bin.
2. Instale o Content Manager em um computador que faça parte do domínio do Active Directory para os Content Managers ativo e em espera.
3. Configure os computadores, ou a conta de usuário na qual o Content Manager é executado, para que sejam confiáveis.

Para obter mais informações, consulte os seguintes documentos de nota técnica:

- Nota técnica Ativando a conexão única para o CRN ou Cognos protegida contra o Active Directory (www.ibm.com/support/docview.wss?uid=swg21341889)
- Nota técnica Ao usar conexão única (SSO) do Kerberos com Active Directory no Cognos, é solicitado que o usuário forneça credenciais (www.ibm.com/support/docview.wss?uid=swg21659267)

Ativando a conexão única entre os componentes do Active Directory Server e do IBM Cognos para usar o REMOTE_USER

Se não desejar a autenticação do Kerberos, será possível configurar o provedor para acessar a variável de ambiente **REMOTE_USER** para atingir a conexão única.

Deve-se configurar a propriedade avançada **singleSignonOption** com o valor **IdentityMapping**. É preciso também especificar credenciais de ligação para o namespace do Active Directory.

O Microsoft IIS configura o **REMOTE_USER** por padrão ao ativar a autenticação do Windows. Se a autenticação do Kerberos não for usada, a conexão única com as origens de dados do Microsoft OLAP (MSAS) não será possível.

Ao definir o **REMOTE_USER**, também é possível escolher salvar o **REMOTE_USER** como uma credencial confiável. Salvar como uma credencial confiável significa que as tarefas planejadas autenticam o **REMOTE_USER** com os privilégios da **Credencial de Ligação**.

Importante: Certifique-se de usar apenas a variável **REMOTE_USER**. Utilizar outra variável pode causar uma vulnerabilidade de segurança.

Procedimento

1. No computador em que você instalou o Content Manager, abra o IBM Cognos Configuration.
2. Na janela **Explorer**, em **Segurança** > **Autenticação**, e selecione o namespace Active Directory.
3. Clique na coluna **Valor** de **Propriedades avançadas** e, em seguida, clique no ícone de edição.

4. Na caixa de diálogo **Valor - Propriedades avançadas**, clique em **Adicionar**.
5. Na coluna **Nome**, digite `singleSignonOption`
6. Na coluna **Valor**, digite `IdentityMapping`.
7. Se você desejar salvar o REMOTE_USER como uma credencial confiável, na caixa de diálogo **Valor - Propriedades Avançadas**, clique em **Incluir**.
8. Na coluna **Nome**, digite `trustedCredentialType`.
9. Na coluna **Valor**, digite `IdentityMappingForTC`.
10. Clique em **OK**.
11. Clique na coluna **Valor** para **Credenciais de Ligação** e, em seguida, clique no ícone de edição.
12. Na caixa de diálogo **Valor - Credenciais de ligação**, especifique uma ID do usuário e senha e, em seguida, clique em **OK**.

Ativando a Conexão Única para Usar a Autenticação do Kerberos

Se o servidor da web IIS for configurado para a autenticação do Windows, não será necessário incluir nenhuma configuração adicional. A autenticação do Kerberos é usada como o padrão.

Ativando a Conexão Única para Usar a Autenticação do Kerberos com a Delegação Restrita

Para poder usar a delegação restrita, você deve definir os nomes principais do serviço (SPN) para os usuários configurados para executar os componentes do IBMCognos e o conjunto de aplicativos da web do Microsoft Internet Information Services (IIS) no domínio do Diretório Ativo.

Se usar o Kerberos com a delegação restrita, deve-se incluir um usuário **`sAMAccountName`** para o Content Manager ao configurar o gateway. Todos os Content Managers ativos e de espera devem ser configurados para serem executados na mesma conta.

Se estiver configurando a conexão única para os servidores do banco de dados, deve-se configurar o **`sAMAccountName`** para o usuário que executa os Componentes da Camada de Aplicativos ao incluir o namespace do Active Directory. Todos os Componentes da Camada de Aplicativos devem ser configurados para serem executados na mesma conta.

Os SPNs são os usuários inseridos nos campos **`sAMAccountName`** no IBM Cognos Configuration.

Por exemplo, suponha que tenha um usuário que executa o componente do Content Manager, outro que executa os Componentes da Camada de Aplicativos e outro que executa o conjunto de aplicativos do servidor da web. O usuário do Content Manager é `CognosCMUser`. O usuário dos Componentes da Camada de Aplicativos é `CognosATCUser`. O usuário do conjunto de aplicativos é `IISUser`. Cada usuário está no domínio `MyDomain`.

1. Deve-se configurar o IIS para que o `MyDomain\IISUser` seja a identidade do conjunto de aplicativos
2. Execute o comando `setspn` para o computador em que o IIS está sendo executado.

   Por exemplo:

   ```
   setspn -A http/IISServerName MyDomain\IISUser
   setspn -A http/IISServerName.MyDomain.com MyDomain\IISUser
   ```

3. Execute o comando `setspn` para os usuários do IBM Cognos.

   Por exemplo:

   ```
   setspn -A ibmcognosba/CognosCMUser MyDomain\CognosCMUser
   setspn -A ibmcognosba/CognosATCUser MyDomain\CognosATCUser
   ```

   Nesses comandos, deve-se usar `ibmcognosba` conforme mostrado nos exemplos. Os nomes de usuários e os domínios devem corresponder a seu ambiente.

   Nota: Neste exemplo, os usuários do **`sAMAccountName`** que devem ser inseridos são `CognosCMUser` e `CognosATCUser`.
4. Se estiver configurando a conexão única para o servidor de banco de dados do Microsoft SQL Server ou do Microsoft SQL Server Analysis Services, você deve configurar o SPN para o servidor de banco de dados. Para obter mais informações, consulte a documentação do servidor de banco de dados.
5. Finalmente, você deve configurar a delegação restrita nos Usuários do Active Directory e na Ferramenta de administração do computador. Na guia **Delegação** de todos os usuários (`IISUser`, `CognosCMUser` e `CognosATCUser`), deve-se selecionar **Confiar neste usuário para delegação somente a serviços especificados** e **Usar somente o Kerberos** para usar o Kerberos com a delegação restrita. Selecione **Confiar neste usuário para delegação somente a serviços especificados** e **Usar o protocolo de autenticação** se estiver usando a extensão do Kerberos do S4U.

   Em seguida, você deve incluir os SPNs necessários. Por exemplo, inclua `ibmcognosba` como um tipo de serviço. E inclua `DomainController1` e `DomainController2` como tipo de serviço `ldap`.

   Se estiver configurando a conexão única para a origem de dados, inclua o serviço MSOLAPSvc3 ou MSQLSVC.

Procedimento

1. No computador em que você instalou o Content Manager, abra o IBM Cognos Configuration.
2. Na janela **Explorer**, em **Segurança** > **Autenticação**, e selecione o namespace Active Directory.
3. Clique na coluna **Valor** de **Propriedades avançadas** e, em seguida, clique no ícone de edição.
4. Na caixa de diálogo **Valor - Propriedades avançadas**, clique em **Adicionar**.
5. Na coluna **Nome**, digite `singleSignonOption`.
6. Na coluna **Valor**, insira um dos valores a seguir:
   - Insira `KerberosS4UAuthentication` se você desejar usar a autenticação do Kerberos primeiro. Se o Kerberos falhar, a autenticação Service For User (S4U) será tentada. Se S4U falhar, serão solicitadas as credenciais para o usuário.
   - Insira `S4UAuthentication` se você desejar usar a autenticação S4U primeiro. Se S4U falhar, serão solicitadas as credenciais para o usuário.
7. Na caixa de diálogo **Valor - Propriedades avançadas**, clique em **Adicionar**.
8. Na coluna **Nome**, digite `trustedCredentialType`.
9. Na coluna **Valor**, insira um dos valores a seguir:
   - Insira `CredentialForTC` se você desejar salvar as credenciais do usuário como uma credencial confiável. Por exemplo, se você desejar usar as credenciais para executar as tarefas planejadas.

- Insira `S4UForTC` se você desejar salvar apenas o nome de usuário autenticado como uma credencial confiável. O nome do usuário é salvo no formato UPN e as tarefas planejadas podem ser executadas com o UPN sem requerer a senha do usuário.

10. Clique em **OK**.
11. Clique na coluna **Valor** para **Componentes da Camada de Aplicativos sAMAccountName**, e insira o **`sAMAccountName`** do usuário que executa os Componentes da Camada do Aplicativo.

    Importante: Esse valor será necessário somente se estiver configurando a conexão única do servidor de banco de dados do Microsoft SQL Server ou do Microsoft SQL Server Analysis Services. Se não estiver configurando a conexão única para o servidor de banco de dados, não altere esse valor.
12. Clique em **Arquivo** > **Salvar**.
13. Reinicie o serviço do IBM Cognos.
14. No computador em que você instalou os componentes do Gateway, abra o IBM Cognos Configuration.
15. Na janela **Explorer**, clique em **Ambiente**.
16. Clique na coluna **Valor** para **sAMAccountName do Content Manager** e insira o **`sAMAccountName`** do usuário que executa o Content Manager.
17. Clique em **Arquivo** > **Salvar**.

Configurando o IBM Cognos para Usar Namespace IBM Cognos Series 7

É possível configurar componentes do IBM Cognos para usar um namespace IBM Cognos Series 7 como o provedor de autenticação. Os usuários são autenticados com base na autenticação e configuração de conexão do namespace do IBM Cognos Series 7.

É necessário que haja um namespace do IBM Cognos Series 7 se você quiser usar PowerCubes e modelos do Transformer do IBM Cognos Series 7 no IBM Cognos Analytics. O namespace deve estar configurado antes de carregar os modelos do Transformer.

Nota: Não é possível usar um arquivo Local Authentication Export (LAE) do IBM Cognos Series 7 para autenticação com componentes do IBM Cognos.

É possível configurar componentes do IBM Cognos para usar diversos provedores de autenticação do IBM Cognos Series 7. Todos os namespaces IBM Cognos Series 7 devem usar o mesmo Servidor do Chamado principal do IBM Cognos Series 7. Caso contrário, é possível receber erros ou solicitações de autenticação mais de uma vez. Para manter o desempenho, verifique também se o Ticket Server está em execução.

Se alterar as informações de configuração armazenadas no servidor de diretório usado para o IBM Cognos Series 7, você deve reiniciar o serviço do IBM Cognos antes de as mudanças entrarem em vigor na instalação do IBM Cognos.

Um usuário deve estar em pelo menos uma classe de usuário do Access Manager para efetuar logon nos componentes do IBM Cognos.

Procedimento

1. Configurar um Namespace do Series 7
2. Ative a comunicação segura para o servidor de diretório usado pelo namespace IBM Cognos Series 7, se necessário
3. Ative conexão única entre o IBM Cognos Series 7 e o IBM Cognos

Configurando um namespace do IBM Cognos Series 7

É possível configurar o IBM Cognos para usar um ou mais namespaces IBM Cognos Series 7 para autenticação.

Procedimento

1. Em cada local em que você instalou o Content Manager, abra o IBM Cognos Configuration.
2. Na janela **Explorer**, em **Segurança**, clique com o botão direito do mouse em **Autenticação** e, em seguida, clique em **Novo Recurso** > **Namespace**.
3. Na caixa **Nome**, digite um nome para o namespace de autenticação.
4. Na lista **Tipo**, clique no namespace apropriado e clique em **OK**.

   O novo recurso do provedor de autenticação aparece na janela **Explorer**, no componente Autenticação.
5. Na janela **Propriedades**, na propriedade **ID do namespace**, especifique um identificador exclusivo para o namespace.
6. Especifique os valores para todas as outras propriedades necessárias para garantir que os componentes do IBM Cognos possam localizar e usar seu provedor de autenticação existente.

   Se a versão de seu namespace IBM Cognos Series 7 for 16.0, assegure que a propriedade **Codificação de Dados** esteja configurada para **UTF-8**. Além disso, os locais onde o Content Manager está instalado devem usar o mesmo código do idioma que os dados no namespace IBM Cognos Series 7.

   O valor do host pode ser um nome de servidor ou um endereço IP. Se você estiver publicando a partir do PowerPlay Enterprise Server para o IBM Cognos Analytics, utilize o mesmo formato de valor utilizado no gerenciador de configuração do IBM Cognos Series 7 para o local do servidor de diretórios. Por exemplo, se o nome do servidor for usado no gerenciador de configuração do IBM Cognos Series 7, você também deve usar o nome do servidor no IBM Cognos Configuration para o IBM Cognos Analytics.
7. Se seu ambiente de namespace incluir a versão 15.2 do namespace IBM Cognos Series 7, você deve desativar a configuração **Series7NamespacesAreUnicode**.
   - Na janela **Propriedades**, no valor **Propriedades Avançadas**, clique no ícone de edição.
   - Na janela **Valor - Propriedades avançadas**, clique em **Adicionar**.
   - Na caixa **Nome**, digite **Series7NamespacesAreUnicode**.
   - Na caixa **Valor**, digite **Falso** e depois clique em **OK**.
8. Na janela **Propriedades**, nas **Configurações de cookies**, assegure-se de que as propriedades **Caminho**, **Domínio** e **Sinalizador seguro ativado**, corresponda às configurações configuradas para o IBM Cognos Series 7.
9. No menu **Arquivo**, clique em **Salvar**.
10. Teste a conexão em um novo namespace. Na janela **Explorer**, em **Autenticação**, clique com o botão direito no novo recurso de autenticação e clique em **Testar**.

É solicitado que insira credenciais para um usuário no namespace para concluir o teste.

Dependendo de como seu namespace estiver configurado, será possível inserir um ID do usuário válido e senha para um usuário no namespace ou o DN do usuário de ligação e senha.

Ativando Comunicação Segura para o Servidor de Diretório Usado pelo Namespace IBM Cognos Series 7

Se estiver usando uma conexão SSL para o Servidor de Diretório usado pelo namespace IBM Cognos Series 7, você deve copiar o certificado do Servidor de Diretório para o local de cada Content Manager.

Para obter mais informações, consulte o *Guia do Administrador* do IBM Cognos Access Manager e a documentação do Directory Server.

Ativando Conexão Única entre o IBM Cognos Series 7 e o IBM Cognos

Se seu namespace IBM Cognos Series 7 tiver sido configurado para integração com seus mecanismos de autenticação externa para conexão única, o provedor do IBM Cognos Series 7 usará automaticamente essa configuração.

Ao configurar conexão única, não será solicitado reinserir informações de autenticação ao acessar o conteúdo do IBM Cognos assegurado pelo namespace IBM Cognos Series 7.

Procedimento

1. Assegure-se de que os componentes do IBM Cognos tenham sido configurados para usar um namespace IBM Cognos Series 7 como um provedor de autenticação.
2. Para o IBM Cognos Series 7, inicie o Gerenciador de Configuração.
3. Clique em **Abrir as configurações atuais**.
4. Na guia **Componentes**, na janela **Explorer**, expanda**Serviços**, **Access Manager - Web Authentication** e clique em **Configurações de cookie**.
5. Na janela **Propriedades**, certifique-se de que as propriedades **Caminho**, **Domínio** e **Sinalizador seguro ativado** correspondam às definições configuradas para o IBM Cognos Analytics.
6. Salve e feche o Configuration Manager.
7. Se o namespace IBM Cognos Series 7 usar o plug-in de Conexão Confiável para conexão única, você deve definir agora a função SaferAPIGetTrustedSignonWithEnv.

Resultados

Agora é possível incluir o IBM Cognos Upfront Series 7 NewsBoxes no IBM Cognos Analytics.

Namespaces IBM Cognos Series 7 e o Plug-in de Conexão Confiável do IBM Cognos Series 7

Se o namespace IBM Cognos Series 7 usar o plug-in de Conexão Confiável para conexão única, você deve definir a função SaferAPIGetTrustedSignonWithEnv em

seu plug-in. Em seguida, será necessário recompilar e reimplementar a biblioteca para obter uma conexão única entre os componentes do IBM Cognos e seu mecanismo de autenticação.

A função SaferAPIGetTrustedSignonWithEnv é uma versão atualizada da função SaferAPIGetTrustedSignon. Essa atualização é necessária, pois o logon do IBM Cognos não é executado no servidor da Web, como é o caso para aplicativos IBM Cognos Series 7. Portanto, não é possível para o plug-in fazer uma chamada getenv() API para recuperar variáveis de ambiente do servidor web. O plug-in pode solicitar que variáveis de ambiente específicas sejam removidas do servidor web utilizando a função SaferAPIGetTrustedSignonWithEnv.

Se você estiver executando produtos IBM Cognos Series 7 e IBM Cognos usando o mesmo plug-in, as funções SaferAPIGetTrustedSignonWithEnv e SaferAPIGetTrustedSignon são necessárias. Para obter informações sobre a função SaferAPIGetTrustedSignon, consulte a documentação do IBM Cognos Series 7.

Função SaferAPIGetTrustedSignonWithEnv

Para que os usuários sejam autenticados com sucesso pelo Access Manager, os signons de OS devem existir e estar ativados no namespace atual.

A memória para o trustedSignonName e trustedDomainName retornados está alocada internamente nesta API. Se a função retorna SAFER_SUCCESS, o Access Manager chama o SaferAPIFreeTrustedSignon para liberar a memória alocada.

A memória para o reqEnvVarList retornado está alocada internamente nesta API. Se a função retorna SAFER_INFO_REQUIRED, o Access Manager chama o SaferAPIFreeBuffer() para liberar a memória alocada.

Implemente tanto a função SaferAPIGetTrustedSignon como a SaferAPIFreeBuffer para registrar com sucesso a biblioteca quando o SaferAPIGetTrustedSignonWithEnv for implementada. A função SaferAPIGetError é necessária apenas se quiser especificar mensagens de erros retornadas do plug-in.

Sintaxe

```
SaferAPIGetTrustedSignonWithEnv(
   EnvVar             envVar[],                  /*[IN]*/
   char               **reqEnvVarList,           /*[OUT]*/
   void               **trustedSignonName,       /*[OUT]*/
   unsigned long      *trustedSignonNameLength,  /*[OUT]*/
   void               **trustedDomainName,       /*[OUT]*/
   unsigned long      *trustedDomainNameLength,  /*[OUT]*/
   SAFER_USER_TYPE    *userType,                 /*[OUT]*/
   void               **implementerData);        /*[IN/OUT]*/
```

Parâmetros para a função SaferAPIGetTrustedSignonWithEnv

Tabela 42. Parâmetros e Descrição para a Função SaferAPIGetTrustedSignonWithEnv

Parâmetro	Descrição
[in] envVar	Uma matriz de nomes e valores de variável de ambiente que foram recuperados do servidor da Web. O final da matriz é representado por uma entrada com um envVarName nula e um envVarValue nula. Observe que na primeira vez que essa API é chamada, a matriz envVar contém apenas o final do marcador de matriz.
[in] reqEnvVarList	Uma sequência que contém uma lista separada por vírgula de nomes de variáveis de ambiente solicitadas pela implementação mais segura. O fim da lista deve ser não terminado.
[out] trustedSignonName	Uma sequência de bytes que identifica o usuário atualmente autenticado. Este valor não precisa ser terminado nulo. Este valor é obrigatório.
[out] trustedSignonNameLength	Um valor de número inteiro que indica o comprimento de trustedSignonName. Este comprimento deve ser excluído do terminador nulo, se houver. Este valor é obrigatório.
[out] trustedDomainName	Uma sequência de bytes que identifica o domínio do usuário atualmente autenticado. Não é necessário terminar esse valor nulo. Se não houver trustedDomainName, o retorno será nulo. Este valor é opcional.
[out] trustedDomainNameLength	Um valor de número inteiro que indica o comprimento de trustedDomainName. Este comprimento deve ser excluído do terminador nulo, se houver. Este valor é obrigatório e deve ser definido como zero se não houver trustedDomainName.
[out] userType	Um valor que indica o tipo de usuário que o Access Manager autenticará. Este valor é obrigatório. Os valores de retorno a seguir são necessários para o Access Manager autenticar usuários com sucesso: **SAFER_NORMAL_USER** Um usuário nomeado. Os signons de OS devem existir e estar ativados no namespace atual. **SAFER_GUEST_USER** Um usuário convidado. Uma conta de usuário convidado deve existir e estar ativada no namespace atual. **SAFER_ANONYMOUS_USER** Um usuário anônimo. Uma conta de usuário anônimo deve existir e estar ativada no namespace atual.

Tabela 42. Parâmetros e Descrição para a Função SaferAPIGetTrustedSignonWithEnv (continuação)

Parâmetro	Descrição
[in/out] implementerData	Um ponteiro utilizado para preservar dados específicos da implementação entre invocações. Uma chamada ocorre sempre que o Access Manager chama o plug-in de conexão confiável. Este valor será válido apenas se o plug-in de conexão confiável tiver sido chamado e se você configurou um valor para ele.

Configurando o IBM Cognos para Usar um Provedor de Autenticação Customizada

Se tiver implementado um provedor de autenticação Java customizado com sua infraestrutura de segurança existente, é possível configurar componentes do IBM Cognos para usá-lo.

É possível usar um provedor de autenticação customizada para acessar e autenticar usuários para uma fonte de autenticação. Também é possível usá-lo como um mecanismo de conexão única para integrar componentes do IBM Cognos com sua infraestrutura de segurança. É possível ocultar namespaces de usuários durante o logon.

Para obter mais informações, consulte o Custom Authentication Provider *Developer Guide*.

Configuração de namespaces de autenticação customizada

É possível configurar os componentes do IBM Cognos para usar um namespace de autenticação customizado. Qualquer configuração adicional para acesso a fonte de autenticação, conexão única ou atributos customizados dependem da implementação do provedor de autenticação customizada.

Certifique-se de que as versões do Java Runtime Environment (JRE) e Java Software Development Kit usadas sejam compatíveis uma com a outra. Se você usar versões suportadas do JRE e Java Software Development Kit que não são compatíveis uma com a outra, o provedor de autenticação Java customizado configurado não aparecerá na lista de namespaces no IBM Cognos Configuration.

Procedimento

1. Em cada local em que o Content Manager está instalado, abra o IBM Cognos Configuration.
2. Na janela **Explorer**, em **Segurança**, clique com o botão direito do mouse em **Autenticação** e, em seguida, clique em **Novo Recurso** > **Namespace**.
3. Na caixa **Nome**, digite um nome para o namespace de autenticação.
4. Na lista **Tipo**, selecione **Custom Java Provider** e clique em **OK**.

   O novo recurso provedor de autenticação aparece na janela **Explorer**, no componente **Autenticação**.
5. Na janela **Propriedades**, na propriedade **ID do Namespace**, especifique um identificador exclusivo para o namespace.

   Dica: Não use dois pontos (:) na propriedade ID do namespace.

6. Especifique os valores para todas as propriedades necessárias para garantir que o IBM Cognos possa localizar e usar seu provedor de autenticação existente.
7. No menu **Arquivo**, clique em **Salvar**.
8. Teste a conexão em um novo namespace. Na janela **Explorer**, em **Autenticação**, clique com o botão direito no novo recurso de autenticação e clique em **Testar**.

   É solicitado que insira credenciais para um usuário no namespace para concluir o teste.

   Dependendo de como seu namespace estiver configurado, será possível inserir um ID do usuário válido e senha para um usuário no namespace ou o DN do usuário de ligação e senha.

Resultados

IBM Cognos carrega, inicializa e configura as bibliotecas do provedor para o namespace.

Ocultação do namespace dos usuários durante o login

É possível ocultar namespaces de usuários durante o login. É possível ter namespaces de conxão confiável sem exibi-los na lista de seleção de namespace que é apresentada aos usuários durante o login.

Por exemplo, talvez você queira integrar a conexão única entre os sistemas, mas manter a capacidade dos clientes de se autenticarem diretamente no IBM Cognos sem precisar escolher um namespace.

Procedimento

1. Em cada local onde você configurou um provedor de autenticação Java customizado, abra o IBM Cognos Configuration.
2. Na janela **Explorer**, em **Segurança** > **Autenticação**, clique no provedor de autenticação Java customizado.
3. Na janela **Propriedades**, clique na caixa próxima a **Selecionável para autenticação** e selecione **Falso**.
4. No menu **Arquivo**, clique em **Salvar**.

Resultados

O namespace não é mostrado na lista de seleção apresentada no login.

Configurando componentes do IBM Cognos para uso com LDAP

É possível configurar os componentes do IBM Cognos para usar um namespace LDAP como provedor de autenticação. É possível usar um namespace LDAP para usuários que estão armazenados em um diretório do usuário LDAP, Active Directory Server, IBM Directory Server, Novell Directory Server ou Oracle Directory Server.

Também é possível usar a autenticação LDAP com as origens de dados do IBM Db2 e doEssbase OLAP ao especificar o namespace LDAP na configuração da conexão de origem de dados. Para obter mais informações, consulte o *IBM Cognos AnalyticsGuia de administração e segurança*.

Você também tem a opção de disponibilizar propriedades de usuário customizadas a partir do namespace LDAP para componentes do IBM Cognos.

Caso queira vincular os usuários ao servidor LDAP, consulte “Mapeamento de LDAP”.

Procedimento

1. “Configurando um Namespace LDAP” na página 258
2. Disponibilize as propriedades de usuário customizadas para componentes do IBM Cognos, se necessário
3. Ative a comunicação segura para o servidor LDAP, se necessário
4. Ative a conexão única entre LDAP e componentes do IBM Cognos, se necessário

Mapeamento de LDAP

Para vincular um usuário ao servidor LDAP, o provedor de autenticação do LDAP deve construir o nome distinto (DN). Se a propriedade Utilizar identidade externa estiver definida como Verdadeira, usará a propriedade Mapeamento de identidade externa para tentar resolver o DN do usuário. Se não puder encontrar a variável do ambiente ou o DN no servidor LDAP, tentará utilizar a propriedade Consulta de usuário para construir o DN.

Se os usuários estão hierarquicamente armazenados dentro do servidor de diretórios, será possível configurar as propriedades Consulta de usuário e Mapeamento de identidade externa para utilizar filtros de busca. Quando o provedor de autenticação LDAP executa estas procuras, ele usa os filtros especificados para a Consulta do usuário e Propriedades de mapeamento de identidade externas. Ele também liga-se ao servidor de diretório usando o valor especificado para a propriedade DN de usuário de ligação e senha ou usando anônimo se nenhum valor for especificado.

Quando um namespace do LDAP for configurado para usar a propriedade de mapeamento de identidade externo para autenticação, o provedor de LDAP liga-se ao servidor de diretórios usando o DN de usuário de ligação e senha ou usando anônimo se nenhum valor for especificado. Todos os usuários que efetuam logon no IBM Cognos usando o mapeamento de identidade externo veem os mesmos usuários, grupos e pastas como o usuário de ligação.

Se não utilizar o mapeamento de identidade externa, será possível especificar se serão utilizadas credenciais de ligação para procurar o servidor de diretórios LDAP configurando a propriedade **Usar credenciais de vinculação para a busca**. Quando a propriedade é ativada, as procuras são executadas usando as credenciais de usuário de ligação ou usando o anônimo se nenhum valor for especificado. Quando a propriedade é desativada, que é a configuração padrão, as procuras são executadas usando as credenciais do usuário conectado. O benefício de utilizar credenciais de ligação é que em vez de alterar direitos administrativos para vários usuários, é possível alterar os direitos administrativos somente para o usuário vinculado.

Nota: Se usar uma sintaxe de DN, como *uid*=${*userID*}, ou=*mycompany*.com, para as propriedades **Consulta de usuário**, **Mapeamento de identidade externo** ou **DN de usuário ligação e senha**, você deve escapar todos os caracteres especiais usados no DN. Se usar uma sintaxe de procura, como (*uid*=${*userID*}), para as propriedades **Consulta de usuário** ou **Mapeamento de identidade externo**, você não deve escapar caracteres especiais usados no DN.

Configurando um Namespace LDAP

É possível configurar componentes do IBM Cognos para usarem um namespace LDAP quando os usuários estiverem armazenados em um diretório do usuário LDAP. O diretório de usuário LDAP pode ser acessado de outro ambiente de servidor, como o Servidor do Active Directory ou CA SiteMinder.

Se estiver configurando um namespace LDAP para um servidor de diretórios diferente do LDAP, consulte a seção adequada:

- Para Active Directory Server, consulte Configurando um Namespace LDAP para Active Directory Server.
- Para IBM Directory Server, consulte Configurando um Namespace LDAP para IBM Directory Server.
- Para Novell Directory Server, consulte Configurando um Namespace LDAP para Novell Directory Server.
- Para Oracle Directory Server, consulte Configurando um Namespace LDAP para Oracle Directory Server.

Também é possível usar a autenticação LDAP com as origens de dados do IBM Db2 e doEssbase OLAP ao especificar o namespace LDAP na configuração da conexão de origem de dados. Para obter mais informações, consulte o *IBM Cognos AnalyticsGuia de administração e segurança*.

Procedimento

1. Em cada local em que você instalou o Content Manager, abra o IBM Cognos Configuration.
2. Na janela **Explorer**, em **Segurança**, clique com o botão direito do mouse em **Autenticação** e, em seguida, clique em **Novo Recurso** > **Namespace**.
3. Na caixa **Nome**, digite um nome para o namespace de autenticação.
4. Na lista **Tipo**, clique no namespace apropriado e clique em **OK**.

   O novo recurso do provedor de autenticação aparece na janela **Explorer**, no componente Autenticação.
5. Na janela **Propriedades**, na propriedade **ID do namespace**, especifique um identificador exclusivo para o namespace.
6. Especifique os valores para todas as outras propriedades necessárias para garantir que os componentes do IBM Cognos possam localizar e usar seu provedor de autenticação existente.
7. Se desejar que o provedor de autenticação LDAP se vincule ao servidor de diretório usando **Ligar DN de usuário e senha** quando executar procuras, em seguida, especifique esses valores.

   Se não houver valores especificados, o provedor de autenticação LDAP vincula como anônimo.

   Se o mapeamento de identidade externa estiver ativado, **Vincular DN do usuário e senha** é utilizado para todos os acessos LDAP. Se o mapeamento de identidade externa não estiver ativado, **Vincular DN do usuário e senha** são usados apenas quando um filtro de procura for especificado para a propriedade **Consulta de usuário**. Nesse caso, quando o DN de usuário está estabelecido, solicitações subsequentes para o servidor LDAP são executadas sob o contexto de autenticação do usuário.
8. Se não usar o mapeamento de identidade externo, use credenciais de ligação para procurar o servidor de diretório LDAP concluindo a etapa seguir:
   - Certifique-se de que **Utilizar identidade externa** esteja definido como **Falso**.

- Defina **Usar credenciais de ligação para buscar** como **Verdadeiro**.
- Especifique a ID e a senha do usuário para **Vincular DN do usuário e senha**.

Se não especificar um ID do usuário e senha e o acesso anônimo for ativado, a procura será feita usando anônimo.

9. Verifique as configurações de mapeamento para os objetos e atributos necessários.

   Dependendo da configuração do LDAP, você pode precisar alterar alguns valores padrão para garantir a comunicação bem-sucedida entre componentes do IBM Cognos e o servidor LDAP.

   Os atributos LDAP mapeados para a propriedade **Nome** em **Mapeamento de pastas**, **Mapeamentos de grupos** e **Mapeamentos de contas** devem estar acessíveis a todos os usuários autenticados. Além disso, a propriedade **Nome** não pode ficar em branco.
10. No menu **Arquivo**, clique em **Salvar**.
11. Teste a conexão em um novo namespace. Na janela **Explorer**, em **Autenticação**, clique com o botão direito no novo recurso de autenticação e clique em **Testar**.

    É solicitado que insira credenciais para um usuário no namespace para concluir o teste.

    Dependendo de como seu namespace estiver configurado, será possível inserir um ID do usuário válido e senha para um usuário no namespace ou o DN do usuário de ligação e senha.

Resultados

IBM Cognos carrega, inicializa e configura as bibliotecas do provedor para o namespace.

Configurando um namespace do LDAP para o Active Directory Server

Se configurar um novo namespace LDAP para uso com Active Directory Server, valores padrão serão gerados para você.

Procedimento

1. Em cada local em que você instalou o Content Manager, abra o IBM Cognos Configuration.
2. Na janela **Explorer**, em **Segurança**, clique com o botão direito em **Autenticação** e, em seguida, clique em **Novo recurso** > **Namespace**.
3. Na caixa **Nome**, digite um nome para o namespace de autenticação.
4. Na lista **Tipo**, selecione **LDAP - Valores padrão para Active Directory** e, em seguida, clique em **OK**.

   O novo recurso provedor de autenticação aparece na janela **Explorer**, no componente **Autenticação**. Valores padrão são gerados para você. Marque-os e faça mudanças conforme necessário.
5. Na janela **Propriedades**, na propriedade **ID do Namespace**, especifique um identificador exclusivo para o namespace.

   Dica: Não use dois pontos (:) na propriedade ID do namespace.

6. Especifique os valores para todas as outras propriedades necessárias para garantir que os componentes do IBM Cognos possam localizar e usar seu provedor de autenticação existente.

   As configurações seguintes são exemplos:

   - Para **Consulta de usuário**, insira `(sAMAccountName=${userID})`
   - Caso utilize um único signon, em **Utilizar identidade externa** defina o valor como **Verdadeiro**.
   - Se você usar conexão única, para **Mapeamento de identidade externa**, especifique `(sAMAccountName=${environment("REMOTE_USER")})`

     Se desejar remover o nome de domínio da variável REMOTE_USER, insira `(sAMAccountName=${replace(${environment("REMOTE_USER")}, "domain\\","")})`.

     Importante: Certifique-se de usar apenas a variável REMOTE_USER. Utilizar outra variável pode causar uma vulnerabilidade de segurança.
   - Para **Ligar DN do usário e senha**, insira `user@domain`.
   - Para **Identificador Exclusivo**, insira `objectGUID`
7. Se desejar que o provedor de autenticação LDAP se vincule ao servidor de diretório usando **Ligar DN de usuário e senha** quando executar procuras, em seguida, especifique esses valores.

   Se não houver valores especificados, o provedor de autenticação LDAP vincula como anônimo.
8. Se você não usar o mapeamento de identidade externa, use as credenciais de ligação para procurar o servidor de diretório LDAP fazendo o seguinte:
   - Certifique-se de que **Utilizar identidade externa** esteja definido como **Falso**.
   - Defina **Usar credenciais de ligação para buscar** como **Verdadeiro**.
   - Especifique a ID e a senha do usuário para **Vincular DN do usuário e senha**.
9. No menu **Arquivo**, clique em **Salvar**.
10. Teste a conexão em um novo namespace. Na janela **Explorer**, em **Autenticação**, clique com o botão direito no novo recurso de autenticação e clique em **Testar**.

    É solicitado que insira credenciais para um usuário no namespace para concluir o teste.

    Dependendo de como seu namespace estiver configurado, será possível inserir um ID do usuário válido e senha para um usuário no namespace ou o DN do usuário de ligação e senha.

Resultados

IBM Cognos carrega, inicializa e configura as bibliotecas do provedor para o namespace.

Configurando um namespace LDAP para o IBM Directory Server

Se configurar um novo namespace LDAP para uso com IBM Directory Server, valores padrão serão gerados para você.

Procedimento

1. Em cada local em que você instalou o Content Manager, abra o IBM Cognos Configuration.

2. Na janela **Explorer**, em **Segurança**, clique com o botão direito em **Autenticação** e, em seguida, clique em **Novo recurso** > **Namespace**.
3. Na caixa **Nome**, digite um nome para o namespace de autenticação.
4. Na lista **Tipo**, clique em **LDAP - Valores padrão para IBM Tivoli** e, em seguida, clique em **OK**.

   O novo recurso de namespace de autenticação aparece na janela **Explorer**, sob o componente **Autenticação**. Marque-os e faça mudanças conforme necessário.
5. Na janela **Propriedades**, na propriedade **ID do Namespace**, especifique um identificador exclusivo para o namespace.

   Dica: Não use dois pontos (:) na propriedade ID do namespace.
6. Especifique os valores para todas as outras propriedades obrigatórias para garantir que o IBM Cognos possa localizar e usar seu namespace de autenticação existente.
   - Para **Consulta de usuário**, especifique `(cn=${userID})`
   - Para **Ligar DN de usuário e senha**, especifique *cn=root*
7. Se desejar que o provedor de autenticação LDAP se vincule ao servidor de diretório usando **Ligar DN de usuário e senha** quando executar procuras, em seguida, especifique esses valores.

   Se não houver valores especificados, o provedor de autenticação LDAP vincula como anônimo.
8. Se você não usar o mapeamento de identidade externa, use as credenciais de ligação para procurar o servidor de diretório LDAP fazendo o seguinte:
   - Certifique-se de que **Utilizar identidade externa** esteja definido como **Falso**.
   - Defina **Usar credenciais de ligação para buscar** como **Verdadeiro**.
   - Especifique a ID e a senha do usuário para **Vincular DN do usuário e senha**.
9. No menu **Arquivo**, clique em **Salvar**.

Configurando um namespace LDAP para o Novell Directory Server

Se configurar um novo namespace LDAP para uso com um Novell Directory Server, será preciso modificar as configurações e alterar os valores para todas as propriedades dos objetos do Novell Directory.

Procedimento

1. Em cada local em que você instalou o Content Manager, abra o IBM Cognos Configuration.
2. Na janela **Explorer**, em **Segurança**, clique com o botão direito em **Autenticação** e, em seguida, clique em **Novo recurso** > **Namespace**.
3. Na caixa **Nome**, digite um nome para o namespace de autenticação.
4. Na lista **Tipo (grupo)**, clique em **LDAP**, em seguida, na lista **Tipo**, escolha **LDAP - valores padrão geral** e, em seguida, clique em **OK**.

   O novo recurso de namespace de autenticação aparece na janela **Explorer**, sob o componente **Autenticação**.
5. Na janela **Propriedades**, na propriedade **ID do namespace**, especifique um identificador exclusivo para o namespace.

   Dica: Não use dois pontos (:) na propriedade ID do namespace.

6. Especifique os valores para todas as outras propriedades obrigatórias para garantir que o IBM Cognos possa localizar e usar seu namespace de autenticação existente.
   - Para **Consulta de usuário**, especifique `(cn=${userID})`
   - Para **Ligar DN de usuário e senha**, especifique o DN base para um usuário de administração, como `cn=Admin,o=COGNOS`
7. Se desejar que o provedor de autenticação LDAP se vincule ao servidor de diretório usando **Ligar DN de usuário e senha** quando executar procuras, em seguida, especifique esses valores.

   Se não houver valores especificados, o provedor de autenticação LDAP vincula como anônimo.
8. Se você não usar o mapeamento de identidade externa, use as credenciais de ligação para procurar o servidor de diretório LDAP fazendo o seguinte:
   - Certifique-se de que **Utilizar identidade externa** esteja definido como **Falso**.
   - Defina **Usar credenciais de ligação para buscar** como **Verdadeiro**.
   - Especifique a ID e a senha do usuário para **Vincular DN do usuário e senha**.
9. Para configurar as propriedades de mapeamento avançadas do LDAP para uso com objetos do Novell Directory Server, utilize valores especificados na seguinte tabela.

Tabela 43. Valores de Mapeamento Avançado do LDAP para Uso com Objetos do Novell Directory Server

Mapeamentos	Propriedade LDAP	Valor LDAP
Pasta	Classe do objeto	organizationalunit,organization,contêiner
	Descrição	descrição
	Nome	ou,o,cn
Grupo	Classe do objeto	groupofnames
	Descrição	descrição
	Membro	membro
	Nome	cn
Conta	Classe do objeto	inetOrgPerson
	Telefone comercial	telephonenumber
	Código do idioma do conteúdo	Idioma
	Descrição	descrição
	E-mail	correio
	Fax/telefone	facsimiletelephonenumber
	Nome fornecido	givenname
	Telefone residencial	homephone
	Telefone celular	móvel
	Nome	cn
	Pager	pager
	Senha	(deixar em branco)
	Endereço postal	postaladdress
	Código do idioma do produto	Idioma

Tabela 43. Valores de Mapeamento Avançado do LDAP para Uso com Objetos do Novell Directory Server (continuação)

Mapeamentos	Propriedade LDAP	Valor LDAP
	Sobrenome	sn
	Nome de usuário	uid

Essas propriedades de mapeamento representam mudanças que são baseadas em uma instalação padrão do Novell Directory Server. Se modificar o esquema, poderá ter de fazer mais mudanças de mapeamento.

Os atributos LDAP mapeados para a propriedade **Nome** em **Mapeamento de pastas**, **Mapeamentos de grupos** e **Mapeamentos de contas** devem estar acessíveis a todos os usuários autenticados. Além disso, a propriedade **Nome** não pode ficar em branco.

Para que os usuários efetuem login com êxito no portal, eles precisam ter permissão de leitura para os atributos `ou` e `o`.

10. No menu **Arquivo**, clique em **Salvar**.

Configurando um namespace LDAP para o Oracle Directory Server

Se configurar um novo namespace LDAP para uso com o Oracle Directory Server, valores padrão serão gerados para você.

Procedimento

1. Em cada local em que você instalou o Content Manager, abra o IBM Cognos Configuration.
2. Na janela **Explorer**, em **Segurança**, clique com o botão direito em **Autenticação** e, em seguida, clique em **Novo recurso** > **Namespace**.
3. Na caixa **Nome**, digite um nome para o namespace de autenticação.
4. Na lista **Tipo**, clique em **LDAP - Valores padrão para o Oracle Directory Server** e, em seguida, clique em **OK**.

   O novo recurso de namespace de autenticação aparece na janela **Explorer**, sob o componente **Autenticação**. Marque-os e faça mudanças conforme necessário.
5. Na janela **Propriedades**, na propriedade **ID do namespace**, especifique um identificador exclusivo para o namespace.

   Dica: Não use dois pontos (:) na propriedade ID do namespace.
6. Especifique os valores para todas as outras propriedades obrigatórias para garantir que o IBM Cognos possa localizar e usar seu namespace de autenticação existente.

   As configurações seguintes são exemplos:

   - Para **Consulta de Usuário**, digite `(uid=${userID})`
   - Caso utilize um único signon, em **Utilizar identidade externa** defina o valor como **Verdadeiro**.
   - Se utilizar conexão única para **Mapeamento de identidade externa**, especifique qualquer atributo, como a ID de domínio do usuário ou a ID do usuário:

     ```
     (ntuserdomainid=$environment("REMOTE_USER")})
     (uid=${environment("REMOTE_USER")})
     ```

Importante: Certifique-se de usar apenas a variável REMOTE_USER. Utilizar outra variável pode causar uma vulnerabilidade de segurança.

- Para **Identificador exclusivo**, digite `nsuniqueid`

7. Se desejar que o provedor de autenticação LDAP se vincule ao servidor de diretório usando **Ligar DN de usuário e senha** quando executar procuras, em seguida, especifique esses valores.

   Se não houver valores especificados, o provedor de autenticação LDAP vincula como anônimo.
8. Se você não usar o mapeamento de identidade externa, use as credenciais de ligação para procurar o servidor de diretório LDAP fazendo o seguinte:
   - Certifique-se de que **Utilizar identidade externa** esteja definido como **Falso**.
   - Defina **Usar credenciais de ligação para buscar** como **Verdadeiro**.
   - Especifique a ID e a senha do usuário para **Vincular DN do usuário e senha**.
9. No menu **Arquivo**, clique em **Salvar**.

Tornar propriedades de usuário customizadas para LDAP disponíveis para componentes do IBM Cognos

É possível usar atributos de usuário arbitrários do provedor de autenticação LDAP nos componentes do IBM Cognos. Para configurar isso, é preciso adicionar esses atributos como propriedades customizadas para o namespace LDAP. As propriedades customizadas estão disponíveis como parâmetros de sessão no Framework Manager.

Utilize também as propriedades customizadas dentro dos blocos de comando para configurar sessões e conexões do Oracle. Utilize blocos de comando com as conexões leves do Oracle e bancos de dados privados virtuais. Para obter mais informações, consulte o *IBM Cognos AnalyticsGuia de administração e segurança*.

Para obter mais informações sobre os parâmetros de sessão, consulte o *Guia do Usuário do Framework Manager*.

Procedimento

1. Em cada local em que instalou o Content Manager, abra o Cognos Configuration.
2. Na janela **Explorer**, em **Segurança** > **Autenticação** e selecione o namespace do LDAP.
3. Na janela **Propriedades**, clique na coluna **Valor** para **Propriedades Customizadas** e clique no ícone de edição.
4. Na janela **Valor - Propriedades customizadas**, clique em **Adicionar**.
5. Clique na coluna **Nome** e digite o nome que deseja que os componentes IBM Cognos usem para o parâmetro de sessão.
6. Clique na coluna **Valor** e digite o nome do parâmetro de conta no provedor de autenticação do LDAP.
7. Repita as duas etapas anteriores para cada parâmetro customizado.
8. Clique em **OK**.
9. No menu **Arquivo**, clique em **Salvar**.

Ativando a comunicação segura para o servidor LDAP

O protocolo LDAP seguro (LDAPS) criptografa a comunicação entre o componente do Access Manager do Content Manager e o servidor de diretórios. O LDAPS

impede que informações delicadas no servidor de diretórios e as credenciais do LDAP sejam enviadas como texto simples.

Para ativar o LDAPS, instale um certificado de servidor que tenha sido assinado por uma autoridade de certificação no servidor de diretórios. Em seguida, crie um banco de dados de certificados para armazenar os certificados. Finalmente, configure o servidor de diretório e o namespace IBM Cognos LDAP para usar LDAPS.

O certificado do servidor deve ser uma cópia de

- O certificado de raiz confiável e todos os outros certificados que compõem a cadeia de confiança para o certificado do servidor de diretório

  O certificado raiz confiável é o certificado da autoridade de certificação raiz que assinou o certificado do servidor de diretórios.
- O certificado do servidor de diretório apenas

Os certificados devem estar codificados como Base64 no formato ASCII (PEM). Todos os certificados, exceto o certificado raiz confiável, não devem ter sua própria assinatura.

Antes de Iniciar

O IBM Cognos funciona com ambas as versões `cert8.db` e `cert7.db` do banco de dados do certificado de cliente. Deve-se usar a ferramenta `certutil` do Netscape Security Services (NSS) para criar os bancos de dados de certificados. O IBM Cognos não aceita outras versões dos arquivos `cert8.db`, incluindo esses arquivos da ferramenta `certutil` fornecida com o Microsoft Active Directory. O IBM Cognos agora inclui a ferramenta `certutil` em plataformas em que o Netscape Security Services (NSS) não está listado como um requisito do sistema. Para plataformas nas quais o NSS estiver listado como um requisito do sistema, use essa versão da ferramenta `certutil`.

Procedimento

1. Crie um diretório para o banco de dados de certificados.
2. Crie o banco de dados de certificados digitando o comando a seguir:

   `certutil -N -d` *`certificate_directory`*

   Em que *`certificate_directory`* é o diretório que criou na etapa 1.

   Este comando cria um arquivo `cert8.db` e um arquivo `key3.db` no novo diretório.
3. Adicione o certificado da autoridade de certificação (CA) ou o certificado do servidor de diretórios ao banco de dados de certificado digitando o comando adequado para o tipo de certificado:
   - Para um certificado CA:

     `certutil -A -n` *`certificate_name`* `-d` *`certificate_directory`* `-i CA.cert -t C,C,C`
   - Para um certificado de servidor de diretório:

     `certutil -A -n` *`certificate_name`* `-d` *`certificate_directory`* `-i` *`server_certificate`*`.cert -t P`

   Em que *`certificate_name`* é um alias que você designa, como o nome de CA ou nome do host; e *`server_certificate`* é o prefixo do arquivo de certificado do servidor de diretório.

4. Copie o diretório de banco de dados de certificados para o diretório *install_location*/configuration em cada local em que o Content Manager está instalado.
5. Configure o servidor de diretórios para utilizar LDAPS e reinicie o servidor de diretórios.

   Para obter mais informações, consulte a documentação do servidor de diretórios.
6. Em cada local do Content Manager em que você configurou o namespace LDAP para usar um servidor de diretório, inicie o IBM Cognos Configuration.
7. Na janela **Explorer**, em **Segurança** > **Autenticação**, clique no namespace do LDAP.
8. Na janela **Propriedades**, para a propriedade **Host e porta**, altere a porta para proteger a porta LDAPS.

   Para a propriedade **Banco de dados de certificado SSL**, especifique o caminho para o arquivo cert7.db.
9. Na janela **Explorer**, clique com o botão direito no namespace do LDAP e clique em **Testar**.

   Se o teste falhar, revise as propriedades, garantindo que o certificado correto seja utilizado.
10. No menu **Arquivo**, clique em **Salvar**.
11. No menu **Ações**, clique em **Reiniciar**.
12. Repita as etapas de 6 a 11 em um local sim, um não, em que o Content Manager estiver instalado.

Ative a conexão única entre o LDAP e componentes IBM Cognos

A conexão única com componentes do IBM Cognos é obtida por meio da configuração da propriedade Mapeamento de Identidade Externa.

O Mapeamento de identidade externa pode referir-se a uma variável de ambiente CGI ou uma variável de cabeçalho HTTP. Para um gateway de servidor de aplicativos ou entrada de dispatcher que estiver apontando para componentes IBM Cognos, o Mapeamento de identidade externo pode se referir à variável de sessão userPrincipalName. O valor resolvido da propriedade Mapeamento de identidade externo no tempo de execução deve ser um DN de usuário válido.

Quando um namespace do LDAP é configurado para usar a propriedade Mapeamento de identidade externo para autenticação, o provedor do LDAP liga-se ao servidor de diretórios usando o DN de usuário de ligação e senha ou usando anônimo se nenhum valor for especificado. Todos os usuários que efetuam logon no IBM Cognos usando o mapeamento de identidade externo veem os mesmos usuários, grupos e pastas como o usuário de ligação.

Se você quiser que os componentes do IBM Cognos trabalhem com aplicativos que usam Java ou segurança de servidor de aplicativos, é possível configurar a propriedade Mapeamento de Identidade Externa para obter o ID do usuário do usuário principal de Java. Inclua o token ${environment("USER_PRINCIPAL")} no valor para a propriedade. Para obter mais informações, consulte a ajuda on-line para o IBM Cognos Configuration.

É possível aplicar a edição de expressão limitada à propriedade Mapeamento de identidade externo usando a operação de substituição.

Operação de Substituição

A operação de substituição retorna uma cópia da sequência com todas as ocorrências da antiga subsequência substituída pela nova subsequência.

As seguintes regras aplicam-se:

- O caractere \ escapa os caracteres nos parâmetros da função. Caracteres como \ e " precisam escapar.
- Chamadas de funções aninhadas não são suportadas.
- Caracteres especiais não são suportados.

Sintaxe

```
${replace(str , old , new)}
```

Parâmetros para a operação de substituição

Tabela 44. Parâmetros e Descrição para a Operação de Substituição

Parâmetro	Descrição
`str`	A string de busca.
`old`	A subsequência a ser substituída pela nova.
`new`	A subsequência que substitui a antiga.

Exemplos

```
${replace(${environment("REMOTE_USER")},"NAMERICA\\",)}
```

```
${replace(${environment("REMOTE_USER")},"NAMERICA\\","")}
```

Provedor de autenticação CA SiteMinder

É possível configurar o IBM Cognos Analytics para usar um namespace do CA SiteMinder como uma origem de autenticação.

O provedor de autenticação usa um CA SiteMinder Software Development Kit para implementar um agente customizado. A implementação do agente customizado requer a configuração de Propriedades de agente no console administrativo do servidor de políticas CA SiteMinder para suportar agentes 4.x.

Requisitos de configuração do CA SiteMinder

Configure os itens a seguir no CA SiteMinder Policy Server:

- O Cognos Analytics deve permitir alguns caracteres especiais e sequências de caracteres na URL do Cognos Analytics Server 11.0.x. Para evitar erros, remova as seguintes sequências de caracteres da lista no parâmetro **BadURLChars** do Objeto de configuração do agente no CA SiteMinder Policy Server:
  - um til (~)
  - um ponto (.)
  - ponto e uma barra (./)
  - barra e um ponto (/.)
  - sinal de maior que (>)

Dica: Os clientes que integram URLs em seus relatórios devem verificar os caracteres transmitidos nos parâmetros URL e assegurar que o CA SiteMinder não irá tratar esses caracteres como **BadURLChars** ou **BadCSSChars**. Para obter informações adicionais, consulte a documentação do CA SiteMinder.

- O Cognos Analytics requer quatro verbos para sua funcionalidade. Ative os seguintes valores no CA SiteMinder Policy Server: GET, POST, PUT e DELETE.

CA SiteMinder Configurado Para Mais de um Diretório do Usuário

Se o seu ambiente do CA SiteMinder estiver configurado para mais de um diretório de usuário, é necessário utilizar o tipo de namespace **SiteMinder** no IBM Cognos Configuration.

Após configurar o namespace SiteMinder no IBM Cognos Configuration, será necessário também incluir um LDAP correspondente ou o namespace Active Directory Server no IBM Cognos Configuration para cada diretório do usuário definido no CA SiteMinder.

Ao configurar um namespace LDAP correspondente, certifique-se de que a propriedade **Mapeamento de identidade externa** esteja ativada e que o token **REMOTE_USER** seja incluído no valor da propriedade. Isso não significa que o CA SiteMinder deve ser configurado para definir o **REMOTE_USER**.

Ao configurar um namespace correspondente do Active Directory, certifique-se de que a propriedade **singleSignonOption** esteja configurada como **IdentityMapping**.

O namespace **SiteMinder** transmite informações sobre o usuário internamente para o namespace LDAP correspondente usando a variável de ambiente **REMOTE_USER** quando ele recebe uma identificação de usuário bem-sucedida do ambiente do CA SiteMinder.

Para obter mais informações, consulte “Ativando a conexão única entre os componentes do Active Directory Server e do IBM Cognos para usar o REMOTE_USER” na página 247.

Importante: Certifique-se de usar apenas a variável **REMOTE_USER**. Utilizar outra variável pode causar uma vulnerabilidade de segurança.

CA SiteMinder Configurado com Apenas um Diretório do Usuário

Se o seu ambiente do CA SiteMinder estiver configurado com apenas um diretório de usuário, não é necessário utilizar o tipo de namespace **SiteMinder** no IBM Cognos Configuration.

Nesse caso, é possível utilizar o diretório de usuário como sua fonte de autenticação configurando o namespace adequado, ou é possível configurar o **SiteMinder** com um diretório de usuário. Por exemplo, se o diretório do usuário CA SiteMinder é LDAP, é possível configurar os componentes do IBM Cognos com um namespace LDAP ou com um namespace **SiteMinder**, referindo-se a um diretório do usuário que é um namespace LDAP.

Se o diretório de usuário do CA SiteMinder é o Active Directory, é possível utilizar um namespace do Active Directory ou um namespace LDAP que é configurado para uso com o Active Directory.

Se deseja usar diretamente o diretório do usuário como fonte de autenticação ao invés de configurar um namespace **SiteMinder**, é possível configurar o namespace LDAP ou Active Directory apropriado. Nesse caso, verifique as propriedades do Objeto de Configuração do Agente no servidor de políticas do CA SiteMinder. Certifique-se de que **SetRemoteUser** esteja ativado.

Ao configurar o namespace do Active Directory, certifique-se de que a propriedade **singleSignonOption** esteja configurada como **IdentityMapping**.

Ao configurar um namespace LDAP correspondente, certifique-se de que a propriedade **Mapeamento de identidade externa** esteja ativada e que o token **REMOTE_USER** seja incluído no valor da propriedade.

Para obter mais informações, consulte "Ativando a conexão única entre os componentes do Active Directory Server e do IBM Cognos para usar o REMOTE_USER" na página 247.

Importante: Certifique-se de usar apenas a variável **REMOTE_USER**. Utilizar outra variável pode causar uma vulnerabilidade de segurança.

Configurando um namespace SiteMinder

Se você configurou o CA SiteMinder para mais de um diretório do usuário, é necessário utilizar o tipo de namespace **SiteMinder** no IBM Cognos Configuration. Após incluir o namespace SiteMinder, você também deve incluir um namespace LDAP correspondente para cada diretório do usuário em seu ambiente do CA SiteMinder.

Você também pode utilizar o tipo de namespace **SiteMinder** se os usuários estão armazenados em um servidor LDAP ou em um servidor Active Directory.

É possível ocultar namespaces de usuários durante o login. É possível ter namespaces de conexão confiável sem exibi-los na lista de seleção de namespace que é apresentada aos usuários durante o login. Por exemplo, talvez você queira integrar a conexão única entre os sistemas, mas manter a capacidade dos clientes de se autenticarem diretamente no IBM Cognos sem precisar escolher um namespace.

Antes de Iniciar

Para utilizar o namespace **SiteMinder**, você deve obter os arquivos de biblioteca requeridos do CA SiteMinder, que são mostrados na tabela a seguir, e incluir os arquivos no caminho de biblioteca apropriado para o seu sistema operacional.

Tabela 45. Arquivos de Biblioteca do CA SiteMinder

Sistema operacional	arquivo de biblioteca do CA SiteMinder
Solaris e AIX	`libsmagentapi.so`

Microsoft Windows de 64 bits	`smagentapi.dll`
	
	`smerrlog.dll`

Procedimento

1. No computador no qual instalou o Content Manager, anexe o diretório que contém o arquivo de biblioteca do CA SiteMinder para a variável de ambiente do caminho de biblioteca apropriada.

- Para sistemas operacionais Solaris, **LD_LIBRARY_PATH**
- Para sistemas operacionais AIX, **LIBPATH**
- Para sistemas operacionais Microsoft Windows, **PATH**

2. Abra o IBM Cognos Configuration.
3. Na janela **Explorer**, em **Segurança**, clique com o botão direito do mouse em **Autenticação** e clique em **Novo recurso** > **Namespace**.
4. Na caixa **Nome**, digite um nome para o namespace de autenticação.
5. Na lista **Tipo**, selecione o **SiteMinder** e depois em **OK**.
6. Selecione o namespace que você incluiu.
7. Para a propriedade **ID do Namespace**, especifique um identificador exclusivo para o namespace.

   Dica: Não utilize dois pontos (:) no identificador.
8. Especifique valores para as outras propriedades necessárias.

   Dica: Se não desejar que os usuários vejam o nome do namespace quando efetuarem login, configure a propriedade **Selecionável para autenticação** como **False**.
9. Na janela **Explorer**, em **Segurança** > **Autenticação**, dê um clique direito no namespace que você incluiu e clique em **Novo recurso** > **Servidor de Políticas do SiteMinder**.
10. Na caixa **Nome**, digite um nome para o servidor de políticas e clique em **OK**.
11. Na janela **Propriedades**, especifique a propriedade **Host** e qualquer outros valores de propriedade que deseja alterar.
12. Na janela **Explorer**, dê um clique com o botão direito no novo servidor de políticas do SiteMinder que você incluiu e clique em **Novo recurso** > **Diretório do usuário**.
13. Na caixa **Nome**, digite um nome para o diretório de usuário e clique em **OK**.

    Importante: O nome deve corresponder ao nome do diretório do usuário que está localizado no servidor de política.
14. Na janela **Propriedades**, digite um valor para a propriedade **Referência à ID do namespace**.
15. Configure um diretório do usuário para cada diretório do usuário no SiteMinder Policy Server.
16. Clique em **Arquivo** > **Salvar**.
17. Teste a conexão em um novo namespace. Na janela **Explorer**, em **Autenticação**, clique com o botão direito no novo recurso de autenticação e clique em **Testar**.

    É solicitado que insira credenciais para um usuário no namespace para concluir o teste.

    Dependendo de como seu namespace estiver configurado, será possível inserir um ID do usuário válido e senha para um usuário no namespace ou o DN do usuário de ligação e senha.
18. Configure um LDAP correspondente ou um namespace Active Directory para cada diretório de usuário.

    Certifique-se de utilizar o mesmo valor para a propriedade **ID do namespace** utilizada para a propriedade **ID do Namespace** para o namespace SiteMinder.

Configurando o IBM Cognos para Usar SAP

Para utilizar um servidor SAP como provedor de autenticação, é preciso utilizar uma versão de SAP BW suportada.

No SAP BW, é possível atribuir usuários a grupos ou papéis de usuários ou ambos. O provedor de autenticação SAP utiliza apenas papéis.

Os direitos de autorização requeridos pelo usuário do SAP dependem de quem usa os componentes do IBM Cognos: usuários ou administradores.

Configurações de Autorização do SAP para Usuários do IBM Cognos

Os objetos de autorização na tabela a seguir são requeridos para qualquer usuário do IBM Cognos.

Tabela 46. Configurações de Autorização do SAP para Usuários do IBM Cognos

Objeto de autorização	Campo	Valor
S_RFC Verificação de autorização do acesso RFC	Atividade	
	Nome do RFC a ser protegido	RFC1 RS_UNIFICATION, SDTX, SH3A, SU_USER, SYST, SUSO
	Nome do RFC a ser protegido	FUGR
S_USER_GRP Manutenção mestre de usuário: Grupos de usuário	Atividade	03
	Nome do grupo de usuários	*

Alguns dos valores apresentados, tais como *, são valores padrão que se pode desejar modificar para o ambiente.

Configurações de Autorização do SAP para Administradores do IBM Cognos

Se os usuários executarem as tarefas administrativas e as procuras por usuários e funções, os valores da seguinte tabela deverão ser incluídos no objeto de autorização S_RFC além dos valores para os usuários do IBM Cognos.

Tabela 47. Configurações de Autorização do SAP para Administradores do IBM Cognos

Objeto de autorização	Campo	Valor
S_RFC Verificação de autorização do acesso RFC	Atividade	16
	RFC_NAME	PRGN_J2EE, SHSS, SOA3
	Tipo de objeto RFC a ser protegido	FUGR

Alguns dos valores mostrados, como *, são valores padrão que você poderá desejar modificar para seu ambiente.

Conectividade entre SAP BW e IBM Cognos no UNIX

Para configurar a conectividade entre o SAP BW e os componentes do IBM Cognos em um sistema operacional UNIX, certifique-se de instalar o arquivo de biblioteca compartilhado do SAP (fornecido pelo SAP) e de incluí-lo na variável de ambiente do caminho da biblioteca da seguinte forma:

- Solaris

  LD_LIBRARY_PATH=$LD_LIBRARY_PATH:<librfccm.so_directory>
- AIX

  LIBPATH=$LIBPATH:<librfc.a_directory>

Configuração de namespaces SAP

É possível configurar componentes do IBM Cognos para usar um servidor SAP como fonte de autenticação.

Antes de Iniciar

Se tiver instalado seu produto IBM Cognos em um servidor de 64 bits, você também deverá copiar os arquivos de biblioteca SAP RFC no diretório de instalação do IBM Cognos.

Procedimento

1. Se estiver sendo executado em um servidor 64 bits, faça o seguinte:
   - Acesse o diretório de instalação do SAP no servidor 64 bits.
   - Copie todos os arquivos da biblioteca SAP RFC de 64 bits para *install_location*\bin64.
   - Copie todos os arquivos de biblioteca SAP RFC de 32 bits para *install_location*\bin.
2. Se estiver executando em um servidor de 32 bits, copie todos os arquivos de biblioteca SAP de 32 bits do diretório de instalação do SAP para o diretório *install_location*\bin64.
3. No local em que você instalou o Content Manager, abra o IBM Cognos Configuration.
4. Na janela **Explorer**, em **Segurança**, clique com o botão direito do mouse em **Autenticação** e clique em **Novo Recurso** > **Namespace**.
5. Na caixa **Nome**, digite um nome para o namespace de autenticação.
6. Na lista **Tipo**, clique em **SAP** e depois em **OK**.

   O novo recurso do provedor de autenticação aparece na janela **Explorer**, no componente Autenticação.
7. Na janela **Propriedades**, na propriedade **ID do namespace**, especifique um identificador exclusivo para o namespace.

   Importante: Não use dois pontos (:) na propriedade ID do namespace.
8. Especifique os valores para todas as propriedades necessárias para garantir que os componentes do IBM Cognos possam localizar e usar seu provedor de autenticação existente.

   Dependendo do ambiente, para a propriedade **Host**, pode ser necessário adicionar a string roteadora de SAP ao nome host SAP.

9. Se o sistema SAP codifica o conteúdo de cookies, ative o recurso de decodificação de chamados:
   - Na janela **Propriedades**, de **Propriedades Avançadas**, clique no Valor e, em seguida, clique no ícone de edição.
   - Clique em **Incluir**.
   - Insira o nome `URLDecodeTickets` e o valor `true`
   - Clique em **OK**.

   Todos os chamados de logon SAP serão decodificados pelo namespace SAP antes de estabelecer uma conexão.
10. No menu **Arquivo**, clique em **Salvar**.
11. Teste a conexão em um novo namespace. Na janela **Explorer**, em **Autenticação**, clique com o botão direito no novo recurso de autenticação e clique em **Testar**.

    É solicitado que insira credenciais para um usuário no namespace para concluir o teste.

    Dependendo de como seu namespace estiver configurado, será possível inserir um ID do usuário válido e senha para um usuário no namespace ou o DN do usuário de ligação e senha.

Ativar Conexão Única entre SAP e IBM Cognos

É possível ativar conexão única entre SAP Enterprise Portal e componentes do IBM Cognos, bem como ao usar a função de namespace externa de conexões de origem de dados SAP BW.

Para isso, certifique-se de definir os seguintes parâmetros do sistema no servidor SAP BW:

- **`login/accept_sso2_ticket = 1`**
- **`login/create_sso2_ticket = 1`**
- **`login/ticket_expiration_time = 200`**

Exclusão de provedores de autenticação

Caso não sejam mais necessários, é possível excluir os namespaces incluídos ou desconfigurar os detectados pelos componentes do IBM Cognos.

Você não deve excluir o namespace Cognos. Ele contém dados de autenticação que pertencem a todos os usuários e é obrigatório para salvar a configuração.

Quando um namespace é excluído, não é mais possível fazer logon nele. Os dados de segurança para o namespace permanecem no Content Manager até serem permanentemente excluídos no portal. Para obter mais informações, consulte o *IBM Cognos AnalyticsGuia de administração e segurança*.

Procedimento

1. Em cada local em que instalou o Content Manager, abra o Cognos Configuration.
2. Na janela **Explorer**, em **Segurança** > **Autenticação**, clique com o botão direito do mouse no namespace e clique em **Excluir**.
3. Clique em **Sim** para confirmar.

   O namespace desaparece da janela **Explorer** e não é mais possível fazer logon no namespace nesse local.

4. No menu **Arquivo**, clique em **Salvar**.
5. Repita as etapas 1 a 4 para cada local onde o Content Manager foi instalado.

   É preciso agora fazer logon no portal e excluir permanentemente os dados do namespace. Para obter mais informações, consulte o *IBM Cognos AnalyticsGuia de administração e segurança*.

Resultados

Após a exclusão de um namespace, ele aparece como Inativo no portal.

Capítulo 9. Manutenção do desempenho

Esta seção inclui tópicos sobre como usar o IBM Cognos Analytics e outras ferramentas e métricas para manter o desempenho do ambiente do IBM Cognos Analytics.

Métricas de desempenho do sistema

O IBM Cognos Analytics fornece métricas do sistema que podem ser usadas para monitorar o funcionamento de todo o sistema e de cada servidor, dispatcher e serviço. Também é possível definir limites para as pontuações das métricas. Alguns exemplos de métricas de desempenho do sistema são o número de sessões em seu sistema, há quanto tempo o relatório está em uma fila, por quanto tempo uma Java Virtual Machine (JVM) esteve em execução e o número de solicitações e processos no sistema.

As métricas de desempenho do sistema residem no ambiente Java, mas podem ser monitoradas no IBM Cognos Administration por meio do portal. Para obter mais informações sobre as métricas de desempenho do sistema de monitoramento, consulte o *Guia de administração e segurança do IBM Cognos Analytics*.

É possível fazer um instantâneo das métricas do sistema atual para poder acompanhar tendências ao longo do tempo ou rever detalhes sobre o estado do sistema em determinado momento. Para obter mais informações, consulte o tópico sobre o arquivo de dump de métricas no *Guia de Resolução de Problemas do IBM Cognos Analytics*.

Também é possível monitorar métricas do sistema externamente para o IBM Cognos Administration usando Java Management Extensions (JMX), uma tecnologia que fornece ferramentas para o gerenciamento e o monitoramento de aplicativos e redes orientadas a serviços.

Monitoramento das métricas do sistema externamente

É possível monitorar métricas do sistema fora do IBM Cognos Administration usando Java Management Extensions (JMX) padrão de mercado. Primeiro, configure duas propriedades JMX no IBM Cognos Configuration para ativar o acesso seguro às métricas no ambiente Java. Em seguida, use uma ID e senha do usuário seguras para conectar-se às métricas por meio de uma ferramenta de conexão JMX.

Antes de Iniciar

Você deve instalar o Oracle Java SE Development Kit ou Java Software Development Kit da IBM antes de poder usar o recurso de monitoramento externo.

Procedimento

1. No local em que o Content Manager está instalado, inicie o IBM Cognos Configuration.
2. Na janela **Explorer**, clique em **Ambiente**.
3. Na janela **Propriedades**, em **Configurações de dispatcher**, clique em **Porta JMX externa**.

4. Na coluna **Valor**, digite um número de porta disponível.
5. Clique em **Credencial JMX externa**.
6. Na coluna **Valor**, clique no ícone de edição, digite um ID do usuário e senha e, em seguida, clique em **OK**.

   O ID do usuário e a senha garantem que apenas um usuário autorizado possa se conectar aos dados de métrica do sistema no ambiente Java usando a porta especificada na **Porta JMX externa**.
7. Salve as mudanças e reinicie o serviço.
8. Para acessar os dados de métricas do sistema, especifique as seguintes informações na ferramenta de conexão JMX:
   - O URL para se conectar aos dados de métricas do sistema

     Por exemplo,

     `service:jmx:rmi://`*`Content_Manager_server`*`/jndi/rmi://`*`monitoring_server`*`:<`*`JMXport`*`>/proxyserver`

     em que *JMXport* é o valor inserido para a **Porta JMX externa**, *Content_Manager_server* e *monitoring_server* são nomes de máquinas. Não use localhost, mesmo se estiver se conectando localmente.
   - A ID e senha do usuário para proteger a conexão.

     Use os mesmos valores configurados para a **Credencial JMX externa**.

Ativação apenas de serviços obrigatórios

Se alguns serviços do IBM Cognos Analytics não forem necessários no ambiente, é possível desativá-los para melhorar o desempenho de outros serviços.

Por exemplo, para dedicar um computador a executar e distribuir relatórios, é possível desativar os serviços em um computador com Application Tier Components. Quando o serviço de apresentação é desativado, o desempenho dos Application Tier Components melhora.

Nota:

- O serviço de Apresentação deve permanecer ativado em pelo menos um computador no ambiente do IBM Cognos Analytics.
- Se deseja utilizar o Query Studio, ative o Serviço de apresentação.
- Se deseja utilizar o Analysis Studio, ative o Serviço de relatório.
- Se alguns componentes do IBM Cognos Analytics não estiverem instalados em um computador, você deve desativar os serviços associados aos componentes ausentes. Caso contrário, os componentes do IBM Cognos Analytics falharão aleatoriamente.

Serviços do IBM Cognos

Após instalar e configurar o IBM Cognos Analytics, um dispatcher estará disponível em cada computador por padrão. Cada dispatcher possui um conjunto de serviços associados, listados na tabela a seguir.

Tabela 48. Serviços do IBM Cognos

Serviço	Finalidade
Serviço do agente	Executa agentes. Se as condições para um agente forem atendidas durante sua execução, o serviço do agente solicitará que o serviço do monitor execute as tarefas.

Tabela 48. Serviços do IBM Cognos (continuação)

Serviço	Finalidade
Serviço de anotação	Ativa a adição de comentário para relatórios por meio da Área de Trabalho do IBM Cognos. Esses comentários permanecem nas versões do relatório.
Serviço de relatórios em lote	Gerencia solicitações de plano de fundo para executar os relatórios e oferece resultados do serviço de monitoração.
Serviço de cache do Content Manager	Aprimora o desempenho geral do sistema e a escalabilidade do Content Manager ao armazenar em cache os resultados das consultas frequentes em cada dispatcher.
Serviço Content Manager	• Desempenha funções de manipulação de objetos no armazenamento de conteúdo como adição, consulta, atualização, exclusão, movimentação e cópia. • Desempenha funções de gerenciamento do armazenamento de conteúdo como importação e exportação.
Serviço de entrega	Envia e-mails para um servidor SMTP externo em nome de outros serviços, como o serviço de relatório, o serviço de tarefa ou o serviço de agente
Serviço de gerenciamento de eventos	Cria, planeja e gerencia objetos de evento que representam relatórios, tarefas, agentes, manutenção de armazenamento de conteúdo e importações e exportações de implementação.
Serviço do Graphics	Gera gráficos em nome do serviço de relatório. Gráficos podem ser gerados em 4 formatos diferentes: Raster, Vector, Microsoft Excel XML ou PDF.
Serviço Human task	Permite a criação e o gerenciamento de tarefas realizadas por usuários. Uma tarefa realizada por usuários, como a aprovação de relatórios, pode ser atribuída à indivíduos ou grupos em uma base ad hoc ou por qualquer outro serviço.
serviço Interactive Discovery Visualization	Usado pelo Cognos Workspace para fornecer recomendações de visualização.
Serviço de tarefa	Executa tarefas ao sinalizar o serviço do monitor para executar as etapas da tarefa em plano de fundo. As etapas incluem relatórios, outras tarefas, importações, exportações, etc.

Tabela 48. Serviços do IBM Cognos (continuação)

Serviço	Finalidade
Serviço de Log	Registra mensagens de log geradas pelo dispatcher e por outros serviços. O serviço de log pode ser configurado para registrar informação de log em um arquivo, banco de dados, servidor de log remoto, Windows Event Viewer ou log do sistema UNIX. As informação de log podem ser analisadas por clientes ou pelos Cognos Software Services, incluindo: • Eventos de segurança. • Informações do erro do sistema e do aplicativo. • Informações de diagnóstico selecionadas.
Serviço de metadados	Fornece suporte para informações de linhagem de dados exibidas no Cognos Viewer, Relatórios, Query Studio, e Analysis Studio. As informações de linhagem incluem informações como origem de dados e expressões de cálculo.
Serviço de migração	Gerencia a migração do IBM Cognos Série 7 para o IBM Cognos Analytics.
serviço do Mobile	Gerencia as atividades relacionadas ao cliente do IBM Cognos Mobile: • Transforma relatórios e análise para consumo de dispositivos móveis. • Compacta o conteúdo de relatórios e análises para rápida distribuição over-the-air para os dispositivos móveis e acesso a partir desses dispositivos móveis. • Realiza o push do conteúdo de relatório e de análise para os dispositivos móveis. • Facilita solicitações relacionadas a relatórios e a análises de entrada e saída entre o dispositivo móvel e o ambiente para procurar, navegar e executar relatórios. • Sincroniza o armazenamento de conteúdo remoto no servidor com o banco de dados remoto no dispositivo móvel. • Converte mensagens do Simple Object Access Protocol (SOAP) em mensagens convenientes para acesso sem fio. • Comunica-se com o dispositivo móvel.

Tabela 48. Serviços do IBM Cognos (continuação)

Serviço	Finalidade
Serviço de monitor	• Gerencia o monitoramento e a execução de tarefas que estão programadas, que foram enviadas para execução posterior ou executadas como uma tarefa de segundo plano. • Atribui um serviço meta para manipular uma tarefa programada. Por exemplo, o serviço do monitor pode solicitar que o serviço de relatórios em lote execute um relatório, que o serviço de tarefa execute uma tarefa ou que o serviço do agente execute um agente. • Cria objetos do histórico dentro do Content Manager e gerencia o failover e a recuperação para executar entradas.
Serviço do PowerPlay	Gerencia solicitações para a execução de relatórios do PowerPlay.
Serviço de apresentação	• Transforma respostas genéricas em XML de outro serviço no formato de saída, como HTML ou PDF. • Fornece recursos de exibição, navegação e administração
Serviço de consulta	Gerencia as solicitações de consultas dinâmicas e exibe o resultado no serviço em lotes ou de relatórios solicitante.
Serviço de metadados relacionais	Usado pelo Framework Manager e CubeDesigner para importar metadados de bancos de dados relacionais. Também pode ser usado pelo Dynamic Query Analyzer no tempo de execução.
Serviço de dados de relatório	Gerencia a transferência de dados do relatório entre o IBM Cognos Analytics e aplicativos que consomem os dados, tais como o IBM Cognos for Microsoft Office e o IBM Cognos Mobile.
Serviço de Relatório	Gerencia solicitações interativas para executar relatórios e fornece a saída para um usuário.
Serviço de repositório	Gerencia solicitações para recuperar a saída do relatório arquivado de um repositório de archive ou de um armazenamento de objeto.

Ajustando um IBM Db2 Content Store

Se você usa um banco de dados do Db2 para o armazenamento de conteúdo, é possível executar etapas para melhorar a velocidade com a qual as solicitações são processadas.

Por padrão, o Db2 designa tabelas que contêm objetos grandes (LOBS) a um espaço de tabela gerenciado por banco de dados. Como resultado, os LOBS não são gerenciados pelos buffer pools do Db2. Isso resulta em solicitações de E/S

diretas nos LOBS, que afeta o desempenho. Ao reatribuir as tabelas que contêm LOBS a um tablespace gerenciado pelo sistema, o número de solicitações diretas de E/S é reduzido.

Antes de mudar o armazenamento de conteúdo do Db2, aloque espaço de log suficiente para reestruturar o banco de dados.

Para reconfigurar o armazenamento de conteúdo do Db2, faça o seguinte:

- Exporte os dados das tabelas que contêm pelo menos um objeto grande (LOB).
- Crie as tabelas em um espaço de tabela gerenciado pelo sistema.
- Importe os dados em tabelas.

Ajustando os recursos de memória para o serviço do IBM Cognos

Para melhorar o desempenho em um ambiente distribuído, é possível alterar a quantidade de recursos que o serviço do IBM Cognos usa.

Por padrão, o serviço do IBM Cognos é configurado para usar recursos mínimos de memória para otimizar o tempo de inicialização.

As definições de configuração do serviço do IBM Cognos aplicam-se apenas ao servidor de aplicativos que o IBM Cognos Analytics usa por padrão. Se quiser configurar o IBM Cognos Analytics para ser executado em outro servidor de aplicativos, não use o IBM Cognos Configuration para configurar os recursos. Ao invés disso, configure os recursos naquele ambiente do servidor de aplicativos.

O serviço do IBM Cognos está disponível apenas nos computadores em que você instalou o Content Manager ou os Componentes da Camada de Aplicativos.

Procedimento

1. Inicie o IBM Cognos Configuration.
2. Na janela **Explorer**, expanda **Ambiente** > **Serviços do IBM Cognos** e clique em **IBM Cognos**.
3. Na janela **Propriedades**, altere o valor para **Memória máxima em MB**.
   - Para reduzir o tempo de inicialização, a área de cobertura da memória e os recursos que são usados, use a configuração padrão de 4096.
   - Esse valor pode ser ajustado com base nos recursos do sistema disponíveis.
4. No menu **Arquivo**, clique em **Salvar**.

Desempenho do Cognos Mobile

É possível usar vários métodos para estimar e controlar o desempenho do ambiente do IBM Cognos Mobile.

Estimativa de Largura de Banda Requerida pelo IBM Cognos Mobile

O IBM Cognos Mobile envia versões compactadas de relatórios do servidor para o dispositivo móvel.

Cada versão de um relatório é enviada somente uma vez. Então ele é armazenado em cache no dispositivo móvel. Um usuário remoto pode então visualizar o relatório quantas vezes quiser no dispositivo sem consumir largura da banda adicional.

Outras operações, como procurar o armazenamento de conteúdo e responder a prompts nos painéis do Cognos Workspace, também consomem largura da banda. A largura da banda consumida é proporcional à usada por um navegador da área de trabalho executando a mesma ação.

Para calcular os custos em largura da banda, um administrador pode usar a seguinte fórmula como um guia:

```
(number of users) x (average size of a report) x
(number of number of scheduled reports sent to
each user per day)
```

Estimativa do Número Necessário de Servidores

A carga gerada por um usuário usando o IBM Cognos Mobile em um servidor (dispatcher) será mínima se os usuários consumirem somente Relatórios Ativos. Para os usuários dos painéis do Cognos Workspace, o aplicativo inclui qualquer carga adicional nos servidores, comparado a um usuário da área de trabalho.

Redução do tempo de entrega para relatórios em uma rede

Os relatórios que são distribuídos globalmente levam mais tempo para abrir em locais remotos do que para abrir localmente. Além disso, os relatórios HTML levam mais tempo para abrir que relatórios em PDF porque mais solicitações são processadas para relatórios HTML.

É possível reduzir a quantidade de tempo para abrir relatórios em locais remotos de duas maneiras. É possível reduzir o número de solicitações entre o navegador e o servidor executando o relatório em formato PDF. Se relatórios HTML forem obrigatórios, é possível acelerar a entrega do relatório configurando gateways adicionais em alguns locais remotos. O conteúdo estático, como gráficos e folhas de estilo, será entregue mais rapidamente.

Aumento do limite de tempo assíncrono em ambiente de carregamento de uso intenso

Se tiver uma carga de usuário intensa (mais de 165) e os relatórios interativos estiverem em execução contínua em uma instalação distribuída, pode ser necessário aumentar o limite de tempo assíncrono para evitar mensagens de erro. O padrão é 30000.

Pode ser necessário também estabelecer o limite de tempo de fila para 360. Para obter informações, consulte o *IBM Cognos Analytics Guia de Administração e Segurança*.

Para resolver esse problema, aumente o timeout de espera.

Procedimento

1. Vá para o seguinte diretório:
   *install_location*webapps/p2pd/WEB-INF/services/.
2. Abra o arquivo reportservice.xml em um editor de texto.
3. Altere o parâmetro async_wait_timeout_ms para 120000.
4. Salve o arquivo.
5. Reinicie os serviços.

Capítulo 10. Configurando manualmente o IBM Cognos Analytics em sistemas operacionais UNIX e Linux

O console conectado ao computador do sistema operacional UNIX ou Linux no qual o IBM Cognos Analytics está sendo instalado pode não suportar uma interface gráfica de usuário baseada em Java.

Você deve executar as tarefas a seguir manualmente:

__ • Mudar as definições de configuração padrão editando o arquivo `cogstartup.xml` localizado no diretório *`install_location`*`/configuration`.

__ • Mudar o suporte de idioma ou moeda ou o mapeamento de localidade editando o arquivo `coglocale.xml` localizado no diretório *`install_location`*`/configuration`.

__ • Aplicar a configuração e as configurações do código de idioma ao computador executando o IBM Cognos Configuration no modo silencioso.

Para todas as instalações, algumas tarefas de configuração são necessárias para que o IBM Cognos Analytics funcione no ambiente. Se os componentes do IBM Cognos Analytics forem distribuídos entre vários computadores, a ordem de configuração e de início dos computadores é importante.

Outras tarefas de configuração são opcionais e dependem do ambiente do relatório. É possível alterar o comportamento padrão do IBM Cognos Analytics, editando o arquivo `cogstartup.xml` para alterar os valores de propriedades. Também é possível usar arquivos de amostra que ativam o IBM Cognos Analytics para usar recursos que já existem no ambiente.

Alterar Manualmente Definições de Configuração Padrão

Se o console que está conectado ao computador do sistema operacional UNIX ou Linux não suportar uma interface gráfica de usuário baseada em Java, edite o `cogstartup.xml` para configurar o IBM Cognos Analytics para funcionar em seu ambiente.

Importante: Algumas definições de configuração não são salvas no arquivo `cogstartup.xml` a menos que você use a interface gráfica com o usuário. Por exemplo, o fuso horário do servidor não é configurado para os componentes do IBM Cognos quando você modifica o arquivo `cogstartup.xml` diretamente e, em seguida, executa IBM Cognos Configuration no modo silencioso. Neste caso, outras configurações de usuário que dependem do fuso horário do servidor podem não funcionar como o esperado.

Se quiser que o IBM Cognos Analytics use um recurso, como um provedor de autenticação que já existe no ambiente, é possível incluir um componente na configuração. Isso é feito copiando o código XML necessário de arquivos de amostra no arquivo `cogstartup.xml` e, em seguida, editando os valores para se adaptarem ao ambiente.

Por padrão, o arquivo `cogstartup.xml` é codificado usando UTF-8. Quando salvar o arquivo `cogstartup.xml`, assegure-se de alterar a codificação da localidade do usuário para que corresponda à codificação usada. A codificação do código do idioma do usuário é definida pelas variáveis de ambiente.

Ao editar o arquivo cogstartup.xml, lembre-se de que o XML faz distinção entre maiúsculas e minúsculas. Essa sensibilidade é importante em todos os usos de texto, incluindo rótulos de elemento e de atributos, elementos e valores.

Antes de editar o arquivo cogstartup.xml, assegure-se de

- Fazer uma cópia de backup.
- Criar o armazenamento de conteúdo em um computador disponível na rede.
- Revisar os requisitos de configuração para seu tipo de instalação.

Procedimento

1. Acesse o diretório *install_location*/configuration.
2. Abra o arquivo cogstartup.xml em um editor.
3. Localize a definição de configuração que deseja alterar consultando a ajuda e os comentários da descrição que aparecem antes da tag inicial dos elementos <crn:parameter>.
4. Altere o valor do elemento <crn:value> de acordo com seu ambiente.

   Dica: Use o atributo type para ajudá-lo a determinar o tipo de dados para a propriedade de configuração.
5. Repita as etapas 3 e 4 até que os valores da configuração sejam adequados ao ambiente.
6. Salve e feche o arquivo.

Resultados

Agora você deve usar um editor de XML de validação para validar suas mudanças com relação às regras no arquivo cogstartup.xsd, localizado em *install_location*/configuration.

Incluindo um Componente em Sua Configuração

O arquivo cogstartup.xml contém definições de configuração usadas pelo IBM Cognos Analytics e por componentes padrão. É possível alterar os componentes que são usados pelo IBM Cognos Analytics, copiando os elementos XML dos arquivos de amostra no arquivo cogstartup.xml. É possível editar os valores de configuração para que se adaptem ao ambiente.

Por exemplo, para usar um banco de dados Oracle para o armazenamento de conteúdo, é possível usar o arquivo de amostra ContentManager_*language code*.xml para substituir as informações de conexão com o banco de dados.

O IBM Cognos Analytics só pode usar uma instância por vez dos seguintes elementos:

- O banco de dados para o armazenamento de conteúdo
- Um provedor criptográfico
- Um modelo de configuração para o serviço do IBM Cognos

O usuário deve estar familiarizado com a estrutura dos arquivos XML antes de começar a editá-los.

Procedimento

1. Acesse o diretório *install_location*/configuration/samples.
2. Escolha um arquivo de amostra para abrir em um editor:
   - Para usar o Oracle ou o IBM Db2 para o armazenamento de conteúdo, abra o arquivo ContentManager_*language_code*.xml.
   - Para usar um provedor de autenticação, abra o arquivo Authentication_*language_code*.xml.
   - Para usar um provedor criptográfico, abra o arquivo Cryptography_*language_code*.xml.
   - Para enviar mensagens de log para algum lugar diferente de um arquivo, abra o arquivo Logging_*language_code*.xml.
   - Para usar um modelo médio ou grande para a quantidade de recursos que o processo do IBM Cognos Analytics usa, abra o arquivo CognosService_*language_code*.xml.
3. Copie os elementos de que precisa.

   Dica: Certifique-se de copiar o código incluindo as tags inicial e final para o elemento <crn:instance>.

   Por exemplo, procure os comentários (Begin of) e (End of):

   ```
   <!--
   (Begin of) Db2 template
   -->
   <crn:instance ...>
   ...
   </crn:instance>
   <!--
   End of) Db2 template
   -->
   ```
4. Acesse o diretório *install_location*/configuration.
5. Abra o arquivo cogstartup.xml em um editor.
6. Cole o código do arquivo de amostra no arquivo cogstartup.xml e substitua o elemento <crn:instance> apropriado.
7. Altere o valores desses novos elementos de forma que se adaptem ao ambiente.

   Para o elemento <crn:instance>, não altere o atributo de classe. É possível alterar esses valores para melhor se adaptarem ao ambiente.

   Por exemplo, se utilizar um banco de dados Oracle para o armazenamento de conteúdo, mude apenas o nome do atributo para se adaptar ao ambiente.

   ```
   <crn:instance class="Oracle" name="MyContentStore">
   ```
8. Salve e feche o arquivo.
9. Execute o IBM Cognos Configuration no modo silencioso digitando o seguinte comando:

   ```
   ./cogconfig.sh -s
   ```

   Isso garante que o arquivo seja válido e que as senhas estejam criptografadas.

Alterando as Configurações Criptografadas Manualmente

É possível alterar manualmente as configurações criptografadas, como senhas e credenciais de usuário, no arquivo cogstartup.xml.

Para solicitar que o IBM Cognos Configuration salve uma configuração criptografada, altere o valor e configure o sinalizador de criptografia como false.

Procedimento

1. Acesse o diretório *install_location*/configuration.
2. Abra o arquivo cogstartup.xml em um editor.
3. Localize a configuração criptografada que deseja alterar consultando a ajuda e os comentários da descrição que aparecem antes da tag inicial dos elementos <crn:parameter>.
4. Altere o valor do elemento <crn:value> de acordo com seu ambiente.

   Dica: Use o atributo de tipo para ajudá-lo a determinar o tipo de dado para a propriedade de configuração.
5. Mude o valor da criptografia para falso.

   Por exemplo,

   ```
   <crn:value encrypted="false">
   ```
6. Repita as etapas 3 e 5 até que os valores da configuração sejam adequados ao ambiente.
7. Salve e feche o arquivo.
8. Digite o seguinte comando de configuração:

   ```
   ./cogconfig.sh -s
   ```

Resultados

As novas configurações são salvas e criptografadas.

Configurações Globais em Sistemas Operacionais UNIX e Linux

Se o console conectado ao computador do sistema operacional UNIX ou Linux não suporta uma interface gráfica de usuário baseada em Java, você deve editar manualmente o arquivo coglocale.xml.

É possível alterar as configurações globais

- Para especificar o idioma usado na interface com o usuário quando o idioma no código do idioma do usuário não está disponível
- Para especificar o código do idioma usado em relatórios quando o código do idioma do usuário não está disponível
- Para adicionar suporte à moeda ou código do idioma para reportar dados ou metadados.
- Para adicionar suporte ao idioma à interface com o usuário.

Por padrão, os componentes do IBM Cognos Analytics asseguram que todos os códigos de idioma, que podem vir de diferentes fontes e em vários formatos, usem uma forma normalizada. Isto significa que todos os códigos do idioma expandidos se adaptam às configurações de idioma e código da região.

Antes de adicionar um suporte ao idioma à interface com o usuário é necessário instalar os arquivos de idiomas em todos os computadores da instalação distribuída. Para obter mais informações, consulte o representante de suporte.

Exemplo 1

Um relatório está disponível no Content Manager em dois códigos do idioma, como com en-us (inglês dos Estados Unidos) e fr-fr (francês da França), mas o

código do idioma do usuário está definido para fr-ca (francês do Canadá). O IBM Cognos usa o mapeamento de código do idioma para determinar qual relatório o usuário vê.

Primeiro, o IBM Cognos verifica se o relatório está disponível no Content Manager no código do idioma do usuário. Se ele não estiver disponível no código do idioma do usuário, o IBM Cognos mapeará o código do idioma do usuário para um código do idioma normalizado na guia Mapeamento de Código do Idioma do Conteúdo. Como o código do idioma do usuário é fr-ca, ele será mapeado para fr. O IBM Cognos usa o valor mapeado para ver se o relatório está disponível em fr. Nesse caso, o relatório estará disponível em en-us e fr-fr, e não em fr.

Em seguida, o IBM Cognos mapeia cada um dos relatórios disponíveis para um código do idioma normalizado. Desta forma, en-us se torna en e fr-fr se torna fr.

Já que o relatório e o código do idioma do usuário mapeiam para fr, o usuário com o código do idioma do usuário fr-ca verá o relatório salvo com o código do idioma fr-fr.

Exemplo 2

O código do idioma do usuário e os códigos do idioma do relatório são todos mapeados para o mesmo código do idioma. O IBM Cognos escolhe qual código do idioma usar. Por exemplo, se o código do idioma do usuário for en-ca (inglês do Canadá) e os relatórios estiverem disponíveis em en-us (inglês dos Estados Unidos) e en-gb (inglês do Reino Unido), o IBM Cognos mapeará cada código do idioma para en. O usuário verá o relatório na configuração do código de idioma escolhida pelo IBM Cognos.

Exemplo 3

Os códigos do idioma do relatório e do usuário não mapeiam para um idioma comum. O IBM Cognos escolhe o idioma. Neste caso, pode ser necessário configurar um mapeamento. Por exemplo, se um relatório estiver disponível em en-us (inglês dos Estados Unidos) e fr-fr (francês da França), mas o código do idioma do usuário for es-es (espanhol da Espanha), o IBM Cognos escolherá o idioma.

Alterando Manualmente as Configurações Globais nos Sistemas Operacionais UNIX e Linux

Use as etapas a seguir para alterar as configurações globais nos sistemas operacionais UNIX e Linux usando o arquivo `coglocale`.

Procedimento

1. Em cada computador em que instalou o Content Manager, acesse o diretório *`install_location`*`/configuration`.
2. Abra o arquivo `coglocale.xml` em um editor.
3. Adicione ou modifique o elemento e o atributos requeridos entre as tags de início e fim adequados.

   Os elementos, atributos e tags inicial e final estão listados na tabela a seguir.

Tabela 49. Tags para Configurações Globais

Tipo de elemento	Tag de início	Tag de fim
Idioma	<supportedProductLocales>	</supportedProductLocales>
Códigos do idioma do conteúdo	<supportedContentLocales>	</supportedContentLocales>
Moeda	<supportedCurrencies>	</supportedCurrencies>
Mapeamento de Código de idioma do produto	<productLocaleMap>	</productLocaleMap>
Mapeamento de Localidade do Conteúdo	<contentLocaleMap>	</contentLocaleMap>
Fontes	<supportedFonts>	</supportedFonts>
Configurações de cookie, localização de archive para relatórios	<parameter name="*setting*">	</parameter>

Dica: Para remover o suporte, exclua o elemento.

4. Salve e feche o arquivo.

Resultados

Dica: Use um editor de XML de validação para validar as mudanças em relação às regras no arquivo `cogstartup.xsd`, localizado em *`install_location`*`/configuration`.

Se você incluir um código de moeda não suportado, será necessário incluí-lo manualmente no arquivo `i18n_res.xml` no diretório *`install_location`*`/bin/`. Copie esse arquivo em cada computador IBM Cognos em sua instalação.

Iniciando e parando o Cognos Analytics no modo silencioso em sistemas operacionais UNIX e Linux

Execute o IBM Cognos Configuration no modo silencioso para aplicar as definições de configuração e iniciar os serviços em computadores com sistema operacional UNIX ou Linux que não suportam uma interface gráfica de usuário baseada em Java.

Antes de executar a ferramenta de configuração no modo silencioso, você deve assegurar que o arquivo `cogstartup.xml` seja válido de acordo com as regras definidas no arquivo `cogstartup.xsd`. O arquivo `cogstartup.xsd` está localizado no diretório *`install_location`*`/configuration`.

Iniciando o Cognos Analytics no modo silencioso em sistemas operacionais UNIX e Linux

Use as etapas a seguir para iniciar o software do IBM Cognos Analytics no modo silencioso.

Procedimento

1. Certifique-se de que o arquivo `cogstartup.xml`, localizado no diretório *`install_location`*`/configuration`, tenha sido modificado para o seu ambiente.

   Para obter mais informações, consulte "Alterar Manualmente Definições de Configuração Padrão" na página 283.
2. Acesse o diretório *`install_location`*`/bin64`.
3. Digite o seguinte comando

   ```
   ./cogconfig.sh -s
   ```

   Dica: Para visualizar as mensagens de log que foram geradas durante uma configuração não assistida, consulte o arquivo `cogconfig_response.csv` no diretório *`install_location`*`/logs`.

Resultados

O IBM Cognos Configuration se aplica às definições de configuração especificadas no arquivo `cogstartup.xml`, criptografa as credenciais, gera os certificados digitais e, se aplicável, inicia o serviço ou o processo Cognos.

Parando o Cognos Analytics no modo silencioso em sistemas operacionais UNIX e Linux

Use as etapas a seguir para parar o software IBM Cognos Analytics no modo silencioso.

Procedimento

1. Acesse o diretório *`install_location`*`/bin64`.
2. Digite o seguinte comando

   ```
   ./cogconfig.sh -stop
   ```

Capítulo 11. Instalação, desinstalação e configuração não assistidas

Use uma instalação, desinstalação e configuração não assistidas para realizar o seguinte:

- Instalar uma configuração idêntica em vários computadores da rede.
- Automatizar o processo de instalação e configuração especificando opções e definições para usuários.
- Instalar e configurar componentes em um ambiente UNIX ou Linux que não tem XWindows
- Desinstalar o IBM Cognos Analytics.

Antes de configurar uma instalação e configuração autônomas, verifique se todas as exigências e os pré-requisitos do sistema sejam cumpridos e que todos os outros softwares necessários estejam instalados e configurados.

Use uma instalação não assistida

Use as seguintes etapas para duplicar uma instalação de um computador para outro sem que as informações sejam solicitadas.

Procedimento

1. "Usar um arquivo de modelo de resposta para criar uma instalação Customizada ou Fácil" na página 293 ou execute o assistente de instalação a partir de uma linha de comandos com um parâmetro para salvar um arquivo de resposta. Por exemplo:

   Windows: `ca_srv_<platform>_<build>.exe -r "C:\ResponseFile\ResponseFile.properties"`.

   UNIX ou Linux: `./ca_srv_<platform>_<build> -r "./ResponseFile/ResponseFile.properties"`

   Nota: O diretório, por exemplo, `C:\ResponseFile`, deve existir antes de executar o assistente de instalação.

   11.0.6 Não é preciso executar uma instalação completa para criar um arquivo de resposta. É possível ativar a instalação com a opção -r e executá-la até o painel de resumo, em seguida, cancelar a instalação. O arquivo de propriedades de resposta será criado quando a instalação for encerrada.
2. Após a instalação ser concluída, modifique o arquivo de resposta, conforme necessário.

   O arquivo de resposta contém valores que correspondem aos valores usados quando o assistente de instalação foi executado para criar o arquivo de resposta. A senha inserida durante a instalação é criptografada no arquivo de resposta.
3. No computador onde planeja instalar o software, faça o seguinte:
   - Insira o disco de instalação do produto apropriado e copie os conteúdos do disco em seu computador.
   - Copie os arquivos de instalação do produto transferidos por download em seu computador.

4. Em uma janela de comandos ou do terminal, acesse o diretório do sistema operacional em que os arquivos de instalação foram copiados e digite o comando a seguir:
   - No Windows, em que *location* é o diretório no qual o arquivo *response filename* foi criado ou copiado:

     ca_srv_<platform>_<build> -f *location**response_filename* -i silent

     Dica:

     Ative o arquivo de resposta de instalação não assistida a partir de um arquivo de lote. Isso faz o processo de instalação aguardar a instalação ser completamente concluída antes de retornar. Além disso, inclua um comando de eco %errorlevel% no término de seu arquivo de lote para saber o código de saída das entradas de arquivo de lote de instalação. Por exemplo, *install_location*\ca_srv_win64_11.0.3.16051211.exe -i silent -f *location**response_filename* echo %errorlevel%

     Se ocorrer um erro durante a instalação, a janela de prompt de comandos da instalação poderá exibir rapidamente algumas informações importantes. O código de saída exibido deve ser 0 (zero) para o sucesso. Se o código de saída não for 0, haverá duas opções.
     a. Visualizar o log de instalação localizado em *install_location*\logs\IBM_Cognos_Analytics_Install_<timestamp>.log
     b. Visualizar um log de saída adicional na pasta temporária do usuário %TEMPDIR%\install_output_log_cognos_analytics.txt. Esse arquivo de log exibe uma lista de códigos de saída possíveis e suas descrições. Também é possível procurar pela frase Erro de Instalação: para obter detalhes adicionais.
   - No UNIX ou Linux:

     ./ca_srv_<platform>_<build> -f *location/response_filename* -i silent
   - Para instalar em um idioma suportado, use a opção -l <lang_code>.

     Por exemplo, para instalar em francês e criar um arquivo de resposta:

     Windows: ca_srv_<platform>_<build>.exe -l <lang_code> –r *location**response_filename*.

     UNIX ou Linux: ./ca_srv_<platform>_<build> -l <lang_code> –r *location/response_filename*

     Para usar o arquivo de resposta e instalar em francês, por exemplo, no Windows:

     c:\CAinstallkit\ca_srv_win64_11.0.3.16051211.exe -l fr -i silent -f c:\responselocation\responsefile.properties echo %errorlevel%

Tabela 50. Códigos de Idioma Suportados

Código	Idioma
pt-BR	English
es	Espanhol
fr	Francês
ele	Italiano
ja	Japonês
ko	Coreano
pt-br	Português do Brasil

Tabela 50. Códigos de Idioma Suportados (continuação)

Código	Idioma
zh_CN	Chinês simplificado
zh_TW	Chinês tradicional

Resultados

Se um status de retorno diferente de zero (0) é apresentado, verifique os arquivos de registros para mensagens de erro. Os erros são registrados no diretório *install_location*\logs em um arquivo do log de erros do resumo. O formato do nome do arquivo é tl-*product_code-versão-yyyymmdd-hhmm*_summary-error.txt.

Se ocorrerem erros antes de ocorrer inicialização suficiente, mensagens de log serão enviadas para um arquivo de log no diretório Temp. O formato do nome do arquivo é tl-*product_code-versão-yyyymmdd-hhmm*.txt.

Depois de resolver todos os erros, é possível definir uma configuração não assistida.

Usar um arquivo de modelo de resposta para criar uma instalação Customizada ou Fácil

Neste tópico são documentados dois modelos de arquivo de resposta que o ajudam a criar instalações não assistidas sem a execução de uma instalação para a geração de um arquivo de resposta.

.

Procedimento

1. Corte e cole a partir deste tópico para criar o arquivo de resposta a ser usado, para uma instalação Customizada ou para uma instalação Fácil.
2. Faça as mudanças no arquivo de resposta criado, seguindo os comentários das diretrizes no arquivo.

Modelo de arquivo de resposta de instalação Customizada:

```
#Modelo de arquivo de Resposta para a instalação sileciosa do IBM Cognos Analytic Software
#
#This template is for a "Custom" install. If you want to do an "Easy" install
#please use other template, located below.
#
#(C) Copyright IBM(R) Corp. 2016. Todos os Direitos Reservados.

#Remember to make a copy of this file before editing it.

#Please DO NOT change the following variable since this is a "Custom" install
BISRVR_INSTALLTYPE_CUSTOM=1

#Required - Install type for "Custom" install
#-------------------------------------------------------------
#You must select one of the following install types
#  If you want to perform "Custom/First Install",
#    set BISRVR_CUSTOM_FIRST to be 1, set the other to be 0
#  If you want to perform "Custom/Connect and install",
#    set BISRVR_CUSTOM_EXPAND to be 1, set the other to be 0
#-------------------------------------------------------------
BISRVR_CUSTOM_FIRST=
```

```
BISRVR_CUSTOM_EXPAND=

#Required - Features
#-------------------------------------------------------------------------
#For "Custom/First install", feature DATATIER must be selected.
#    Other features can be selected at the same time too.
#For Custom Expand Install, you must select at least one of the features.
#
#BISRVR_FEATURE_DATATIER is called "Content repository" in GUI install.
#BISRVR_FEATURE_APPTIER is called "Application services" in GUI install.
#BISRVR_FEATURE_GATEWAY is called "Optional Gateway" in GUI install.
#-------------------------------------------------------------------------
BISRVR_FEATURE_DATATIER=
BISRVR_FEATURE_APPTIER=
BISRVR_FEATURE_GATEWAY=

#Required - Install Location
#-------------------------------------------
#The installation location
#It is called "Install location" in GUI
# DEFAULT:
#   on UNIX, and Linux
#      /opt/ibm/cognos/analytics
#   on Windows
#   C:\\Program Files\\ibm\\cognos\\analytics
#-------------------------------------------
USER_INSTALL_DIR=

#Required - Input Required for "Custom/Connect and install"
#-----------------------------------------------------------------------------
#The URL of the First Install and Cognos administrator credentials are required for
#  "Custom/Connect and install"
#
#BISRVR_CANALYTICS_URL is called "Cognos Analytics URL" in GUI install
#BISRVR_NAMESPACE is called "Namespace" in GUI install
#BISRVR_COGNOSUSER is called "Cognos administrator user ID" in GUI install
#BISRVR_COGNOSUSER_PASSWORD is called "Password" in GUI install.
# A senha deve ser criptografada. It can be obtained by recording a GUI install.
#-----------------------------------------------------------------------------
BISRVR_CANALYTICS_URL=
BISRVR_NAMESPACE=
BISRVR_COGNOSUSER=
BISRVR_COGNOSUSER_PASSWORD=

#Optional - Options for Windows Install
#-----------------------------------------------------------------------------
#The following two entries are for Windows only
#BISRVR_SHORTCUT is called "Program folder" in GUI install
#BISRVR_ALLUSERS is called "Make shortcut visible to all users in the Start menu"
# in GUI install. Set to 1 if you want the shortcut visible.
#-----------------------------------------------------------------------------
#BISRVR_SHORTCUT=
#BISRVR_ALLUSERS=

#End of Custom install template
#-----------------------------------------------------------------------------
```

Modelo de arquivo de resposta de instalação Fácil:

```
#Modelo de arquivo de Resposta para a instalação sileciosa do IBM Cognos Analytic Software
#
#This template is for an "Easy" install. If you want to do a "Custom" install
#please use other template, located above.
#
#(C) Copyright IBM(R) Corp. 2016. Todos os Direitos Reservados.

#Remember to make a copy of this file before editing it.
```

```
#Required - Install type for "Easy install"
#-----------------------------------------------------------------
#You must select one of the following install types
#  If you want to perform "Easy install/First Install",
#    set BISRVR_INSTALLTYPE_READY to be 1, set the other to be 0
#  If you want to perform "Easy install/Connect and Install",
#    set BISRVR_INSTALLTYPE_EXPAND to be 1, set the other to be 0
#-----------------------------------------------------------------
BISRVR_INSTALLTYPE_READY=
BISRVR_INSTALLTYPE_EXPAND=

#Required - Install Location
#-------------------------------------------
#The installation location
#It is called "Install location" in GUI
# DEFAULT:
#   on UNIX, and Linux
#      /opt/ibm/cognos/analytics
#   on Windows
#   C:\\Program Files\\ibm\\cognos\\analytics
#-------------------------------------------
USER_INSTALL_DIR=

#Required - Input Required for "Easy install"
#-------------------------------------------------------------------------------
#Cognos administrator credentials are required for "Easy install".
#BISRVR_COGNOSUSER is called "Cognos administrator user ID" in GUI install.
#BISRVR_COGNOSUSER_PASSWORD is called "Password" in GUI install.
# A senha deve ser criptografada. It can be obtained by recording a GUI install.
#-------------------------------------------------------------------------------
BISRVR_COGNOSUSER=
BISRVR_COGNOSUSER_PASSWORD=

#Required - Input Required for "Easy install/Connect and Install"
#-----------------------------------------------------------------
#BISRVR_CANALYTICS_URL is called "Cognos Analytics URL" in GUI install
#-----------------------------------------------------------------
#BISRVR_CANALYTICS_URL=

#Optional - Options for Windows Install
#-------------------------------------------------------------------------------
#The following two entries are for Windows only
#BISRVR_SHORTCUT is called "Program folder" in GUI install
#BISRVR_ALLUSERS is called "Make shortcut visible to all users in the Start menu"
# in GUI install. Set to 1 if you want the shortcut visible.
#-------------------------------------------------------------------------------
#BISRVR_SHORTCUT=
#BISRVR_ALLUSERS=

#End of Easy install template
#-------------------------------------------------------------------------------
```

O que Fazer Depois

Execute o arquivo de resposta de acordo com as instruções no tópico “Use uma instalação não assistida” na página 291.

Usar uma Configuração Não Assistida

Para usar uma configuração não assistida, você deve exportar uma configuração de uma instalação existente que tenha os mesmos componentes do IBM Cognos Analytics instalados. É possível então executar o IBM Cognos Configuration no modo silencioso.

A configuração exportada contém as propriedades dos componentes do IBM Cognos Analytics que foram instalados em um computador.

Antes de Iniciar

Certifique-se de que as definições de configuração no computador para onde estiver exportando a configuração sejam apropriadas para uso em outro computador com os mesmos componentes instalados. Por exemplo, se você alterou a parte do nome do host da propriedade URI do Gateway de localhost para um endereço IP ou nome de computador, certifique-se de que esta configuração seja apropriada para a configuração do novo computador.

Procedimento

1. No IBM Cognos Configuration, no menu **File**, clique em **Exportar como**.
2. Quando solicitado sobre exportar o conteúdo descriptografado, clique em **Sim**.
3. Se desejar exportar a configuração atual para uma pasta diferente, na caixa **Procurar em**, localize e abra a pasta.
4. Na caixa **Nome de arquivo**, digite um nome para o arquivo de configuração.
5. Clique em **Salvar**.
6. Copie o arquivo de configuração exportado para o diretório *install_location*/configuration no computador em que planeja usar a configuração não atendida.
7. Renomeie o arquivo para cogstartup.xml.
8. Acesse o diretório *install_location*/bin ou o *install_location*/bin64.
9. Digite o seguinte comando:
   - No UNIX ou Linux, digite
     ```
     ./cogconfig.sh -s
     ```
   - No Windows, digite
     ```
     cogconfig.bat -s
     ```

   Dica: Para visualizar as mensagens de log que foram geradas durante uma configuração não assistida, consulte o arquivo cogconfig_response.csv no diretório *install_location*/logs.

   Verifique se a configuração não assistida foi bem-sucedida analisando o status de retorno. Um valor igual a zero (0) indica êxito e todos os outros valores indicam que ocorreu um erro.

Resultados

O IBM Cognos Configuration aplica as definições de configuração especificadas no arquivo cogstartup.xml, criptografa credenciais, gera certificados digitais e, se aplicável, inicia o serviço ou processo do IBM Cognos.

Use uma Desinstalação Não Assistida

Use uma desinstalação não assistida para automatizar uma remoção de componentes em diversos computadores que possuem os mesmos componentes ou removem os componentes em um ambiente UNIX ou Linux que não tem Windows.

Dica: Se ferramentas de monitoramento, como o Process explorer, MMC (Microsoft Management Console) estiverem em execução durante a desinstalação, elas irão

interferir na exclusão dos serviços. Isso se aplica a todos os serviços em geral. Por exemplo, depois de desinstalar o Cognos Analytics, os serviços do produto como ApacheDS, IBM Cognos e Informix não serão totalmente removidos e, em vez disso, eles serão mostrados no painel de serviços como interrompido e desativado. Para evitar isso, certifique-se de que nenhuma ferramenta de monitoramento esteja em execução durante a execução da desinstalação. O encerramento dessas ferramentas de monitoramento após a desinstalação também concluirá a remoção dos serviços.

Procedimento

Execute o assistente de desinstalação a partir de uma linha de comandos com os parâmetros a seguir:
Windows: *install_location*/Uninstall_IBM_Cognos_Analytics.exe -i silent.
UNIX ou Linux: ./*install_location*/Uninstall_IBM_Cognos_Analytics -i silent

Capítulo 12. Desinstalando o IBM Cognos Analytics

É importante utilizar os programas de desinstalação para remover completamente todos os arquivos e as modificações dos arquivos do sistema. Para desinstalar o IBM Cognos Analytics, desinstale os componentes do servidor e as ferramentas de modelagem.

Se estiver executando o IBM Cognos Analytics em um ambiente de servidor de aplicativos, use a ferramenta de administração fornecida com o servidor de aplicativos para parar o aplicativo, se ele estiver em execução, e remover a implementação da parte Java dos componentes do IBM Cognos Analytics. Muitos servidores de aplicativos não removem completamente todos os arquivos ou diretórios de aplicativos implantados durante a desinstalação; desta forma, esta ação deverá ser feita manualmente. Depois de remover completamente a implementação dos componentes do IBM Cognos Analytics, execute as etapas nesta seção para desinstalar nos sistemas operacionais UNIX e Microsoft Windows.

Dica: Se ferramentas de monitoramento, como o Process explorer, MMC (Microsoft Management Console) estiverem em execução durante a desinstalação, elas irão interferir na exclusão dos serviços. Isso se aplica a todos os serviços em geral. Por exemplo, depois de desinstalar o Cognos Analytics, os serviços do produto como ApacheDS, IBM Cognos e Informix não serão totalmente removidos e, em vez disso, eles serão mostrados no painel de serviços como interrompido e desativado. Para evitar isso, certifique-se de que nenhuma ferramenta de monitoramento esteja em execução durante a execução da desinstalação. O encerramento dessas ferramentas de monitoramento após a desinstalação também concluirá a remoção dos serviços.

Importante: Não exclua os arquivos de configuração e de dados se estiver fazendo upgrade para uma nova versão do IBM Cognos Analytics e desejar usar os dados de configuração com a nova versão.

Desinstalar o IBM Cognos Analytics em sistemas operacionais UNIX ou Linux

Se você não precisar mais do IBM Cognos Analytics ou se estiver fazendo upgrade no sistema operacional UNIX ou Linux, desinstale o IBM Cognos Analytics.

A desinstalação não remove os arquivos que foram alterados desde a instalação, tais como os de configuração e dados dos usuários. A localidade da instalação continua no computador, e os arquivos ficam retidos até que sejam excluídos manualmente.

Procedimento

1. Se o console conectado ao computador não suportar uma interface gráfica de usuário baseada em Java, determine a identificação do processo (pid) do processo do IBM Cognos Analytics, digitando o seguinte comando:

   ```
   ps -ef | grep cogbootstrapservice
   ```

2. Pare o processo do IBM Cognos Analytics:
   - Se o XWindows for executado, inicie o IBM Cognos Configuration e no menu **Ações**, clique em **Parar**.

- Se não utilizar o XWindows, digite

  ```
  kill -TERM pid
  ```

3. Para desinstalar o IBM Cognos Analytics, acesse o diretório *install_location* e digite o comando apropriado:
   - Caso utilize o XWindows, digite

     ```
     ./uninst -u
     ```
   - Se não estiver usando o XWindows, execute uma desinstalação não assistida (consulte "Use uma instalação não assistida" na página 291).
4. Siga os prompts para completar a desinstalação.
5. Exclua todos os arquivos de Internet temporários dos computadores de navegadores web.

Desinstalar o IBM Cognos Analytics nos sistemas operacionais Microsoft Windows

Se você não precisar mais do IBM Cognos Analytics ou se estiver fazendo upgrade, desinstale todos os componentes do IBM Cognos Analytics e o serviço do IBM Cognos.

Se tiver instalado mais de um componente no mesmo local, escolha os pacotes para desinstalação utilizando o assistente para desinstalação. Todos os componentes do pacote serão desinstalados. Repita o processo de desinstalação em cada computador que contém componentes do IBM Cognos Analytics.

Não é necessário fazer backup dos arquivos de configuração e dados em um sistema operacional Microsoft Windows. Estes arquivos são preservados durante a desinstalação.

Feche todos os programas antes de desinstalar o IBM Cognos Analytics. Do contrário, alguns arquivos poderão não ser removidos.

A desinstalação não remove os arquivos que foram alterados desde a instalação, tais como os de configuração e dados dos usuários. A localidade da instalação continua no computador e os arquivos ficam retidos até que sejam excluídos manualmente. Não exclua os arquivos de configuração e de dados se estiver fazendo upgrade para uma nova versão do IBM Cognos Analytics e desejar usar os dados de configuração com a nova versão.

Procedimento

1. No menu **Iniciar**, clique em **Todos os Programas** > **IBM Cognos Analytics** > **Desinstalar IBM Cognos Analytics**.

   Exibe-se o assistente **Desinstalação**.

   Dica: IBM Cognos Analytics é o nome padrão da Pasta de Programa que é criada durante a instalação. Caso escolha outro nome, acesse a pasta para encontrar o programa.
2. Siga as instruções de desinstalação dos componentes.

   O arquivo `cognos_uninst_log.htm` registra as atividades que o assistente de Desinstalação executa ao desinstalar os arquivos.

   Dica: Para localizar o arquivo de log, verifique o diretório temporário.

3. Exclua todos os arquivos de Internet temporários dos computadores de navegadores web.

   Para obter mais informações, consulte a documentação do navegador web.

Recuperando-se de uma desinstalação malsucedida

Se uma desinstalação for malsucedida, podem permanecer arquivos, entradas de registro e serviços que deveriam ter sido excluídos. Este tópico fornece diretrizes para as instalações Fácil e Customizada.

Procedimento

1. Para uma Fácil, instale primeiro:
   a. Remova o Informix executando o comando uninstall do Informix:

      install_location\informix\bin\ifxdeploy.exe -u *install_location*\informix -delifx

   a. Remova a seguinte chave de registro: HKEY_LOCAL_MACHINE\SOFTWARE\Informix\Online\ol_cognoscm
   b. Remova a pasta de instalação *install_location*
   c. Se esta for a única instalação baseada do InstallAnywhere em sua máquina, será possível remover o arquivo de registro do InstallAnywhere: %PROGRAM FILES%\Zero G Registry\.com.zerog.registry.xml
2. Para todas as outras instalações:
   a. Remova a pasta de instalação *install_location*
   b. Se esta for a única instalação baseada no InstallAnywhere em sua máquina, será possível remover o arquivo de registro do InstallAnywhere:

      No Windows (diretório oculto): %PROGRAM FILES%\Zero G Registry\.com.zerog.registry.xml

      No UNIX: arquivo de registro: .com.zerog.registry.xml localizado em:

      - Se você efetuou login como raiz, o registro global estará localizado em /var
      - Se você efetuou login como um usuário, ele estará localizado no diretório inicial do usuário.

      Se você não tiver certeza sobre o status das instalações do InstallAnywhere, você poderá simplesmente renomear esse arquivo para manter uma cópia dele.

Capítulo 13. IBM Cognos Content Archival

Armazenar o conteúdo arquivado no seu repositório externo fornece a possibilidade de atender os requisitos de conformidade regulamentar e pode melhorar a escalabilidade e o desempenho dos produtos IBM Cognos porque reduz o tamanho do conteúdo no armazenamento de conteúdo.

O software suporta um IBM FileNet Content Manager com repositório externo do IBM FileNet CMIS. Se já tiver o software IBM Filenet CMIS versão 1 instalado, você deve atualizar este software com o fix pack, versão 2. O arquivamento de conteúdo também pode ser configurado para usar o seu sistema de arquivos.

Os administradores criam uma conexão de origem de dados com um repositório externo para permitir que o conteúdo seja movido do armazenamento de conteúdo para o repositório. Os usuários podem visualizar o conteúdo arquivado no repositório externo. Fornecendo resultados da procura para conteúdo recente e arquivado, os usuários podem fazer comparações críticas entre dados atuais e dados históricos. Esse mecanismo eficiente permite que sua empresa atenda aos requisitos corporativos e governamentais, ao mesmo tempo que fornece uma experiência contínua do usuário.

O conteúdo arquivado no repositório externo não é gerenciado no ambiente do IBM Cognos. Por exemplo, se excluir relatórios no IBM Cognos Analytics, as saídas arquivadas não serão excluídas do seu repositório externo.

Para obter mais informações sobre a administração de seus arquivos, consulte o *Guia de Administração e Segurança do IBM Cognos Analytics*.

Há dois cenários de fluxo de trabalho para arquivar seu conteúdo. O primeiro fluxo de trabalho permite que os administradores arquivem pacotes e pastas após a instalação do IBM Cognos Content Archival. O segundo fluxo de trabalho permite que os administradores criem conexões de repositório para novos pacotes e pastas.

Fluxo de Trabalho 1: Arquivando Conteúdo Depois de Instalar o Software de Conectividade

Administradores podem arquivar saídas de relatório salvas para pacotes e pastas específicas ou para todos os pacotes e pastas depois de instalar ou atualizar o IBM Cognos Analytics. Este fluxo de trabalho precisa ser concluído somente uma vez, pois todo o conteúdo está localizado atualmente em seu armazenamento de conteúdo.

- Crie uma conexão de origem de dados como o repositório externo.
- Selecione conexões de repositório para os pacotes e pastas que precisam ser arquivados.
- Crie e execute uma tarefa de manutenção de arquivamento de conteúdo para selecionar pastas e pacotes a arquivar no repositório externo.

Depois de configurar uma conexão do repositório para pacotes e pastas, qualquer nova saída de relatório é arquivada automaticamente, o que significa que não há necessidade de executar a tarefa de manutenção de arquivamento de conteúdo novamente.

Fluxo de Trabalho 2: Criando Conexões do Repositório para Novos Pacotes e Pastas

Os administradores podem criar conexões do repositório para novos pacotes e pastas ao concluir estas tarefas:

- Crie uma conexão de origem de dados como o repositório externo.
- Selecione conexões de repositório para os pacotes e pastas que precisam ser arquivados.

Usando Tarefas de Manutenção de Conteúdo de Arquivamento de Conteúdo

A tarefa de manutenção de conteúdo de arquivamento de conteúdo cria uma referência para as versões de relatório nas pastas e pacotes que você seleciona e configura. A seleção de pastas e pacotes marca o conteúdo e permite que ele permaneça no armazenamento de conteúdo até que seja arquivado em seu repositório externo.

É importante observar que essa tarefa não move o conteúdo do armazenamento de conteúdo para o repositório externo. Você deve selecionar conexões de repositório para seus pacotes e pastas primeiro. As versões do relatório em pastas e pacotes que não são marcadas para arquivamento estão disponíveis para exclusão do armazenamento de conteúdo.

Depois que o conteúdo é marcado, a tarefa de arquivamento de conteúdo está concluída. Uma tarefa em segundo plano no Content Manager localiza os itens marcados e, em seguida, os copia e salva no repositório externo.

A importação do conteúdo para uma pasta ou pacote configurado para arquivamento em um repositório externo não move e arquiva o conteúdo importado automaticamente no repositório. Um administrador deve executar uma tarefa de manutenção de conteúdo do arquivamento de conteúdo para essa pasta ou pacote para arquivar o conteúdo importado.

Tarefas em Segundo Plano

As tarefas XML em segundo plano usadas para mover conteúdo do armazenamento de conteúdo para o repositório externo são archiveTask.xml e deleteTask.xml. O arquivo archiveTask.xml move o conteúdo marcado para um repositório externo. Também é possível usar esse arquivo para configurar tempos de execução de encadeamento e saídas de archive de formatos selecionados. O arquivo deleteTask.xml é um arquivo de configuração que recupera e exclui objetos de versão marcados da fila. Você não deve modificar este arquivo.

Preservar IDs de Conteúdo antes de Arquivar

Se necessário, é possível preservar IDs de conteúdo antes de a saída de relatório ser arquivada.

Os objetos no armazenamento de conteúdo possuem IDs de conteúdo que são excluídos e substituídos por novos IDs por padrão, quando você executa uma implementação de importação e move o conteúdo para um ambiente de destino. Entretanto, pode haver situações em que você deve preservar IDs de conteúdo, por exemplo, ao mover a saída de relatório para um repositório de relatórios externo.

Configurar Arquivamento de Conteúdo

Você deve configurar o ambiente para arquivamento de conteúdo. Para que as mudanças na configuração entrem em vigor, deve-se parar e iniciar os serviços do IBM Cognos.

Criando um Local do Arquivo para o Repositório do Sistema de Arquivos

Para arquivar relatórios ou especificações do relatório para um repositório do sistema de arquivos de arquivamento de conteúdo IBM Cognos, você deve criar uma raiz de alias que aponta para um local de arquivo em uma unidade local ou compartilhamento de rede.

Antes de Iniciar

Você deve ser um administrador e ter acesso ao local do arquivo. O Content Manager e os Componentes da Camada de Aplicativos devem ser capazes de acessar esse local usando um URI de arquivo.

Procedimento

1. Se estiver em execução, pare o serviço IBM Cognos.
2. Inicie o IBM Cognos Configuration.
3. Clique em **Ações** > **Editar Configuração Global.**
4. Na guia **Geral**, selecione as **Raízes de Alias**, clique dentro do campo do valor, clique no botão de edição e quando a caixa de diálogo **Valor - Raiz de Alias** aparecer, clique em **Incluir**.
5. Na coluna **Nome Raiz do Alias**, digite um nome exclusivo para seu repositório do sistema de arquivos.

   Nota: Não há limite para o número de aliases que você pode criar.
6. Digite o caminho para o seu local do sistema de arquivos, em que o file-system-path é o caminho completo para um local de arquivo existente:
   - No Windows, na coluna **windowsURI**, digite `file:///` seguido pelo caminho local, por exemplo, `file:///c:/file-system-path` ou digite `file://` seguido pelo nome do servidor e caminho de compartilhamento, por exemplo `file://server/share`.
   - No UNIX ou Linux, na coluna **unixURI**, digite `file:///` seguido pelo caminho local, por exemplo, `file:///file-system-path`.

   Nota: Caminhos relativos como `file:///../file-system-path`, não são suportados.

   Em uma instalação distribuída, ambos os computadores do Content Manager e dos Componentes da Camada de Aplicativos devem ter acesso ao local do arquivo. Use ambas as URIs apenas em uma instalação distribuída. A URI do UNIX e a URI do Windows em uma raiz de alias devem apontar para o mesmo local no sistema de arquivos.
7. Clique em **OK**.
8. Reinicie o serviço do IBM Cognos. Isto pode levar alguns minutos.

Resultados

Use este nome de repositório do sistema de arquivos para criar uma conexão de origem de dados a ser usada com o software de arquivamento de conteúdo Cognos. Para obter mais informações, consulte *IBM Cognos: Guia de Administração e Segurança.*

Importando as Definições de Classes Customizadas e Propriedades no IBM FileNet Content Manager

Para usar o IBM Cognos Content Archival, você deve importar um conjunto de classes customizadas e arquivos de propriedades no IBM FileNet Content Manager.

As definições e propriedades de classes customizadas incluem metadados específicos de FileNet. É possível instalar arquivos de propriedade e classes customizadas a qualquer momento.

Procedimento

1. Se você tiver o arquivamento FileNet configurado, acesse o diretório *install_location*/configuration/repository/filenet/upgrade/.
2. Se o archiving FileNet ainda não estiver configurado, acesse o diretório *install_location*/configuration/repository/filenet/new/.
3. Copie os arquivos CMECMIntegrationObjects_CEExport._xxx.xml para uma pasta local no servidor FileNet.
4. Abra a ferramenta FileNet Enterprise Manager Administration e conecte-se ao domínio para o repositório externo FileNet.
5. Selecione um Armazenamento de Objeto de destino e clique em **Importar Todos os Itens** para importar as definições no armazenamento de objeto.
6. Na área de janela Importar Opções, clique em **Importar Arquivo de Manifesto** e procure onde os arquivos CMECMIntegrationObjects_CEExport._xxx.xml estão localizados.
7. Selecione o arquivo CMECMIntegrationObjects_CEExport_Manifest.xml e clique em **Importar**.
8. Reinicie o aplicativo FileNet Content Engine e FileNet CMIS para aplicar as mudanças em seu ambiente.

   Nota: Pode demorar muito para que as mudanças sejam atualizadas em todos os nós FileNet.

Importando Definições e Propriedades de Classes Customizadas para o IBM Content Manager 8

Para usar o arquivamento de conteúdo do IBM Cognos com o IBM Content Manager 8, você deve importar um conjunto de arquivos de classes e propriedades customizadas. Você também deve atualizar o arquivo de configuração do CMIS com os tipos de pasta do IBM Cognos.

As definições e propriedades de classes customizadas incluem metadados específicos do IBM Content Manager 8. É possível instalar arquivos de propriedade e classes customizadas a qualquer momento.

Como nenhum Resource Manager é definido durante o processo de instalação, há mensagens de erro de conflito durante o processo de importação.

Antes de Iniciar

Você deve ter o IBM Content Manager 8 instalado com um repositório externo do IBM Content Manager 8 CMIS versão 1.1.

Procedimento

1. Abra o **Cliente de Administração do Sistema** do Content Manager 8.
2. No menu principal, clique em **Ferramentas** > **Importar XML**.
3. Na janela **Opções de Importação XML**, seção **Arquivo para importar**:
   - No campo **Arquivo de modelo de dados**, clique em **Navegar**, e selecione o arquivo `CMECMIntegrationTypes_RMImport_Manifest.xsd` do qual desejar importar os objetos.
   - No campo **Arquivo de objetos administrativos**, clique em **Navegar** e selecione o arquivo `CMECMIntegrationTypes_RMImport_MimeTypes.xml` para importar o arquivo de Objetos administrativos.

   A localização padrão é o diretório *install_location*`/configuration/repository/contentManager8/New`.
4. Para visualizar conflitos, na janela **Opções de Importação XML**, em **Opções de processamento**, selecione **Processar interativamente**.
5. Clique em **Importar** para iniciar o processo de importação.
   a. Na janela **Importar Resultados do Pré-processador**, expanda **Tipos de Item** e dê um clique duplo em um tipo de Item que indicar um conflito.
   b. Na janela **Detalhes de Definição de Importação e Definição de Destino**, na coluna **Destino Resultante**, selecione os nomes para o **Gerenciador de Recursos** e **Coleção** criados ao instalar o Content Manager 8, e clique em **Aceitar**.
   c. Repita as etapas a e b para cada tipo de item que indicar um conflito.
6. Após resolver todos os conflitos, a partir da janela **Importar Resultados do Pré-processador**, clique em **Continuar**.
7. Na janela **Confirmar Seleção de Importação**, clique em **Importar**.
8. Após concluir a importação, clique em **OK**.
9. Para atualizar o arquivo de configuração do CMIS para detectar os tipos de pasta do IBM Cognos, execute o CMIS para o programa de configuração do Content Manager 8 para criar um perfil.
10. Abra o arquivo `cmpathservice.properties` na pasta de perfis de configuração do IBM CMIS para Content Manager.

    Para UNIX, o caminho de arquivo padrão é: `/opt/IBM/CM_CMIS/profiles/profile1`

    Para Windows, o caminho de arquivo padrão é: `C:\Program Files\IBM\CM_CMIS\profiles\profile1`
    a. Localize a linha `folderTypes`.
    b. Inclua os tipos de pastas do IBM Cognos COGNOSREPORT e REPORTVERSION em maiúsculas. Separe cada tipo de pasta com uma vírgula.

       ```
       Por exemplo,
       folderTypes = ClbFolder,COGNOSSREPORT,REPORTVERSION
       ```
    c. Salve e feche o arquivo.
11. Execute o CMIS para o programa de configuração do Content Manager 8 e selecione a opção para reimplementar o arquivo de configuração do CMIS automaticamente.

Nota: Para obter informações adicionais sobre a implementação manual do CMIS, consulte Implementando manualmente o IBM CMIS para Content Manager (http://pic.dhe.ibm.com/infocenter/cmgmt/v8r4m0/topic/com.ibm.installingcmcmis.doc/cmsde001.htm).

12. No console administrativo do perfil Liberty do WebSphere Application Server, reinicie o **CMIS for Content Manager Application**.

Especificando um Tempo Disponível para Executar o Processo de Arquivamento

Para manter o desempenho do sistema alto durante os horários de pico, é possível configurar um período de blecaute a ser especificado quando as tarefas de archive e exclusão são executadas.

Um período de blecaute é um período temporário no qual a movimentação de dados é negada. Por padrão, um período de blecaute não é definido quando o software é instalado.

Procedimento

1. Acesse o diretório *install_location*/webapps/p2pd/WEB-INF/cm/tasks/manager.
2. Usando um editor de texto XML, abra o arquivo tasksManager.xml.
3. Por exemplo, para especificar um período de blecaute semanal das 8h às 17h, de terça-feira a sexta-feira, inclua o elemento <blackoutPeriods> a seguir como um elemento filho do elemento backgroundTasksManager.
   - start time = <hour>08</hour>
   - stop time = <hour>17</hour>
   - dias =

     ```
     <day>Tuesday</day>
     <day>Wednesday</day>
     <day>Thursday</day>
     <day>Friday</day>
     ```
4. Se necessário, diminua o número de encadeamentos disponíveis para os processos de arquivamento e de exclusão. O número máximo de encadeamentos é 7.
5. Salve e feche o arquivo.
6. Reinicie as atividades em segundo plano no serviço do Content Manager.

Especificando o Tempo de Execução de Encadeamento

É possível usar os encadeamentos para planejar o tempo de processamento do sistema operacional.

As tarefas em segundo plano de arquivamento e exclusão usam encadeamentos para mover conteúdo. Os encadeamentos são unidades de tempo de processamento programadas pelo sistema operacional.

Procedimento

1. Acesse o diretório *install_location*/webapps/p2pd/WEB-INF/cm/tasks/config.
2. Usando um editor de texto XML, abra o arquivo archiveTask.xml.
3. Por exemplo, para configurar três encadeamentos que são executados da meia-noite às 8h, um encadeamento que é executado das 8h às 17h, nenhum encadeamento a ser executado das 17h à meia-noite, e todos os encadeamentos que são executados todos os dias da semana, inclua o seguinte elemento XML <executionPeriods> como um elemento filho do elemento backgroundTask.

```
 <executionPeriods>
<executionPeriod>
 <threads>3</threads>
 <startTime>
  <hour>00</hour>
  <minute>00</minute>
 </startTime>
 <stopTime>
  <hour>08</hour>
  <minute>00</minute>
 </stopTime>
 <days>
  <day>Monday</day>
  <day>Tuesday</day>
  <day>Wednesday</day>
  <day>Thursday</day>
  <day>Friday</day>
  <day>Saturday</day>
  <day>Sunday</day>
 </days>
</executionPeriod>
<executionPeriod>
 <startTime>
  <hour>08</hour>
  <minute>00</minute>
 </startTime>
 <stopTime>
  <hour>17</hour>
  <minute>00</minute>
 </stopTime>
 <days>
  <day>Monday</day>
  <day>Tuesday</day>
  <day>Wednesday</day>
  <day>Thursday</day>
  <day>Friday</day>
  <day>Saturday</day>
  <day>Sunday</day>
 </days>
</executionPeriod>
</executionPeriods>
```

4. Salve e feche o arquivo.

Arquivando Formatos Selecionados de Saídas de Relatório

É possível limitar o arquivamento para limitar o arquivamento para formatos de saída específicos. Por padrão, as saídas de qualquer formato, incluindo PDF, XML, HTML e Excel, são arquivadas.

É possível limitar o arquivamento de formatos de saída específicos no repositório.

Procedimento

1. Acesse o diretório *install_location*/webapps/p2pd/WEB-INF/cm/tasks/config.
2. Usando um editor de texto XML, abra o arquivo archiveTask.xml.
3. Por exemplo, para definir o arquivamento somente das versões de saída do relatório PDF, inclua o elemento XML <outputFormats> a seguir como um elemento filho do elemento XML runOptions.

   ```
   <outputFormats>
      <outputFormat>PDF</outputFormat>
     </outputFormats>
   ```

   É possível usar o elemento de amostra outputFormats existente e modificar a lista para especificar os formatos de saída a serem arquivados.

Não é possível arquivar seletivamente diversas versões de saída do relatório de arquivo, por exemplo, HTML com gráficos.

Salve e feche o arquivo.

Especificando quais Especificações de Relatórios Não Estão Arquivadas

Por padrão, a saída de especificação de relatório é arquivada. As especificações de relatório descrevem como os dados foram gerados em um relatório.

Para desligar o arquivamento das especificações de relatório, você deve modificar dois arquivos: `CM.xml`, e `CM_FILENET.xml` ou `CM_CM8.xml`, dependendo de se o conteúdo será arquivado em um repositório do IBM FileNet Content Manager ou em um repositório do IBM Content Manager 8.

Procedimento

1. Acesse o diretório *install_location*`/webapps/p2pd/WEB-INF/repositories/config`.
2. Usando um editor de texto XML, abra o arquivo `CM.xml`.
3. Comente ou remova a seguinte linha: `<property name="specifications" metadataPropertyName="specification" useTempFile="true"`
4. Salve e feche o arquivo.
5. Acesse o diretório *install_location*`/webapps/p2pd/WEB-INF/repositories/config`.
6. Execute umas das seguintes etapas:
   - Se você arquivar o conteúdo no FileNet, abra o arquivo nomeado `CM.FILENET.xml` em um editor de texto.
   - Se você arquivar o conteúdo no IBM Content Manager 8, abra o arquivo nomeado `CM.xml` em um editor de texto.
7. Comente a linha ou remova o elemento a seguir:

```
<property repositoryName="REPORTEXECUTIONSPECIFICATION" repositoryType="ASSOCIATED"
metadataPropertyName="specification">
        <associatedObjectTypes>
          <objectType name="VERSIONSPECIFICATION">
           <properties>
           <property repositoryName="cmis:name" repositoryType="STRING"
metadataPropertyName="reportVersionDefaultName"  valueHandler="com.cognos.cm.
repositoryPluginFramework.
PropertyValueAppendStringHandler" valueHandlerArgument="_specification"/>
          </properties>
         </objectType>
        </associatedObjectTypes>
       </property>
```

   Nota: No arquivo `CM.xml`, o valor de `objectType name` é `<objectType name="$t!-2_VERSIONSPECIFICATIONv-1">`.
8. Reinicie as atividades em segundo plano no serviço do Content Manager. Para obter mais informações, consulte o *IBM Cognos AnalyticsGuia de administração e segurança*.

Apêndice A. Opções da Linha de Comandos do IBM Cognos Configuration

Use as opções da linha de comandos com o comando de configuração para modificar o comportamento do IBM Cognos Configuration quando ele for iniciado.

Tabela 51. Opções e Descrições da Linha de Comandos

Opção	Descrições
`-h`	Exibe os comandos para IBM Cognos Configuration.

`-s`	Executa o IBM Cognos Configuration no modo silencioso.
	
	Usa valores de propriedade especificados no arquivo `cogstartup.xml` para configurar componentes instalados e, em seguida, inicia todos os serviços.
	
	`./cogconfig.sh -s`
	
	`cogconfig.bat -s`

`-stop`	Para todos os serviços do IBM Cognos.
	
	`./cogconfig.sh -stop`
	
	`cogconfig.bat -stop`

`-startupfile` *`path/filename.xml`*	Executa o IBM Cognos Configuration usando um arquivo diferente do `cogstartup.xml` no diretório *`install_location`*`/configuration`.

`-test`	Usa os valores de propriedade especificados no arquivo `cogstartup.xml` para testar as definições de configuração.
	
	`./cogconfig.sh -test`
	
	`cogconfig.bat -test`

`-notest`	Inicia o IBM Cognos Configuration com as tarefas de teste automáticas desativadas.
	
	`./cogconfig.sh -notest`
	
	`cogconfig.bat -notest`
	
	Esta opção não deve ser usada para a primeira vez que você inicia o produto ou se você estiver fazendo mudanças na configuração.

`-utf8`	Salva a configuração na codificação UTF-8.
	
	`./cogconfig.sh -s -utf8`
	
	`cogconfig.bat -s -utf8`

Tabela 51. Opções e Descrições da Linha de Comandos (continuação)

Opção	Descrições

`-l language ID`	Executa o IBM Cognos Configuration usando o idioma especificado pelo identificador de idioma.
	
	Para executar a ferramenta de configuração em modo silencioso usando chinês simplificado
	
	`./cogconfig.sh -l zh-cn`
	
	`cogconfig.bat -l zh-cn`

`-e filename.xml`	Exporta as definições de configuração atual para o arquivo especificado.
	
	`./cogconfig.sh -e filename.xml`
	
	`cogconfig.bat -e filename.xml`

`-log`	Cria um arquivo do log de erros `cogconfig.timestamp.log` no diretório *cognos_location*`/logs`.
	
	`./cogconfig.sh -log`
	
	`cogconfig.bat -log`

`-java:{local|env}`	Executa o IBM Cognos Configuration nos sistemas operacionais do Microsoft Windows usando o Java Runtime Environment versão que é definido como
	• `env`: ambientalmente usando a variável de ambiente **JAVA_HOME**
	• `local`: local do diretório *install_location*`/bin/jre`
	
	Se você não configurar esta sinalização, o IBM Cognos usará a configuração de variável de ambiente **JAVA_HOME**.
	
	Para executar o IBM Cognos Configuration em modo silencioso, usando a JVM local, digite o seguinte comando:
	
	`./cogconfig.sh -s -java:local`
	
	`cogconfig.bat -s -java:local`

É possível usar mais de uma opção de linha de comandos por vez. Por exemplo, é possível executar o IBM Cognos Configuration no modo silencioso e enviar todas as mensagens de erro para um arquivo de log.

Apêndice B. Resolução de problemas

Use essas informações de referência de resolução de problemas e essas soluções como um recurso para ajudá-lo a resolver problemas específicos que podem ser encontrados durante a instalação dos componentes do IBM Cognos Business Intelligence.

Os problemas se caracterizam por seus sintomas. Cada sintoma pode ser rastreado para uma ou mais causas utilizando ferramentas e técnicas específicas de solução de problemas. Após identificado, o problema pode ser solucionado através da implementação de uma série de ações.

Durante a solução de problemas, os arquivos de log podem ajudar. Outra ferramenta de resolução de problemas valiosa é a Comunidade de Suporte, disponível no Portal de Suporte IBM (abre em uma nova janela). O Support Community pode ajudar com soluções para problemas de todos os produtos do IBM Cognos.

Quando não puder solucionar um problema, o recurso final é seu representante de suporte técnico. Para analisar um problema, o representante do suporte técnico necessita de informações a respeito da situação e dos sintomas experimentados. Para ajudar a isolar o problema, colete os dados necessários antes de entrar em contato com o representante.

Resolvendo um Problema

Resolução de problemas é uma abordagem sistemática para resolver um problema. O objetivo da resolução de problemas é determinar por que algo não funciona como o esperado e como resolver o problema.

A primeira etapa no processo de resolução de problemas é descrever o problema completamente. As descrições de problema ajudam você e o representante de suporte técnico da IBM a saber onde começar a procurar a causa do problema. Esta etapa inclui perguntar a si mesmo questões básicas:

- Quais são os sintomas do problema?
- Onde o problema ocorre?
- Quando o problema ocorre?
- Sob quais condições o problema ocorre?
- O problema pode ser reproduzido?

As respostas a estas questões geralmenthe levam a uma boa descrição do problema, que pode então, levar a uma resolução do problema.

Quais são os sintomas do problema?

Ao começar a descrever um problema, a pergunta mais óbvia é "Qual é o problema?" Esta questão pode parecer direta, no entanto, é possível dividi-la em várias questões focadas que criam uma imagem mais descritiva do problema. Estas questões podem incluir:

- Quem, ou o que, está relatando o problema?
- Quais são os códigos e mensagens de erro?

- Como o sistema falha? Por exemplo, o problema é um loop, uma interrupção, um travamento, uma degradação de desempenho ou um resultado incorreto?

Onde o problema ocorre?

Determinar onde o problema se origina nem sempre é fácil, mas é uma das etapas mais importantes na resolução de um problema. Muitas camadas de tecnologia podem existir entre os componentes de relatório ou com falha. Redes, discos e drivers são apenas alguns dos componentes a se considerar ao investigar problemas.

As seguintes questões ajudam a isolar a camada do problema:

- O problema é específico a uma plataforma ou sistema operacional ou é comum entre diversas plataformas ou sistemas operacionais?
- O ambiente e a configuração atuais são suportados?

Se uma camada relatar o problema, o problema não necessariamente se origina nessa camada. Parte da identificação de onde um problema se origina é entender o ambiente no qual ele existe. Reserve um tempo para descrever completamente o ambiente do problema, incluindo o sistema operacional e a versão, todos os softwares e versões correspondentes e o hardware. Confirme que está executando em um ambiente que seja suportado; muitos problemas podem ser rastreados de volta a níveis incompatíveis de software que não são destinados a executar juntos ou não foram testados juntos totalmente.

Quando o problema ocorre?

O desenvolvimento de uma linha de tempo detalhada leva a uma falha, especialmente para casos que são ocorrências únicas. É possível desenvolver mais facilmente uma linha de tempo trabalhando em retrocesso: inicie no horário que um erro foi relatado (o mais preciso possível, mesmo cada milissegundo) e trabalhe em retrocesso por meio dos logs e informações disponíveis. Geralmente, é necessário observar apenas o alcance do primeiro evento suspeito que localizar em um log de diagnóstico.

Para desenvolver uma linha de tempo de eventos detalhada, responda estas questões:

- O problema acontece apenas em um determinado horário do dia ou da noite?
- Com que frequência o problema acontece?
- Que sequência de eventos leva ao horário que o problema é relatado?
- O problema acontece após uma mudança de ambiente, como um upgrade ou uma instalação de software ou hardware?

Sob quais condições o problema ocorre?

Saber quais sistemas e aplicativos estão em execução no horário que um problema ocorre é uma parte importante da resolução de problemas. Essas questões sobre seu ambiente podem ajudar a identificar a causa do problema:

- O problema sempre ocorre quando a mesma tarefa está sendo executada?
- Uma certa sequência de eventos precisa ser feita para que o problema ocorra?
- Outros aplicativos falham ao mesmo tempo?

Responder estes tipos de questões pode ajudar a explicar o ambiente no qual o problema ocorre e correlacionar quaisquer dependências. Lembre-se de que

somente porque diversos problemas podem ter ocorrido mais ou menos no mesmo horário, os problemas não são necessariamente relacionados.

O problema pode ser reproduzido?

Os problemas que podem ser reproduzidos geralmente são mais fáceis de resolver. Entretanto, os problemas que podem ser reproduzidos podem ter uma desvantagem. Se o problema tiver um impacto significativo nos negócios, você não deseja que ele ocorra novamente. Se possível, crie novamente o problema em um ambiente de teste ou desenvolvimento, que normalmente oferece mais flexibilidade e controle durante sua investigação. Responda às questões a seguir:

- O problema pode ser recriado em um sistema de teste?
- Diversos usuários ou aplicativos estão encontrando o mesmo tipo de problema?
- O problema pode ser recriado executando um único comando, um conjunto de comandos ou um determinado aplicativo?

Procurando em Bases de Conhecimento

É possível localizar soluções com frequência procurando nas bases de conhecimento IBM. É possível otimizar seus resultados usando recursos disponíveis, ferramentas de suporte e métodos de procura.

Sobre Esta Tarefa

É possível localizar informações úteis procurando no centro de informações do IBM Cognos, mas às vezes é necessário ver além do centro de informações para resolver problemas.

Procedimento

Para procurar as informações de que precisa nas bases de conhecimento, use uma ou mais das seguintes abordagens:

- Localize o conteúdo necessário usando o IBM Support Portal.

  O IBM Support Portal é uma visualização unificada e centralizada de todas as ferramentas de suporte técnico e informações para todos os sistemas, software e serviços IBM. O IBM Support Portal permite acessar o portfólio de suporte eletrônico IBM a partir de um local. É possível padronizar as páginas para focar nas informações e recursos necessários para prevenção de problemas e uma resolução de problemas mais rápida. Familiarize-se com o Portal de Suporte IBM visualizando os vídeos de demo sobre esta ferramenta. Esses vídeos apresentam a você o IBM Support Portal, exploram outros a resolução de problemas e outros recursos e demonstram como é possível padronizar a página movendo, incluindo e excluindo portlets.
- Procure conteúdo sobre o IBM Cognos usando um dos seguintes recursos técnicos adicionais:
  - APARs do IBM Cognos Analytics (relatórios de problemas)
  - Fóruns e comunidades do IBM Cognos.
- Procure conteúdo usando a procura de cabeçalho da IBM. É possível usar a procura do cabeçalho principal da IBM digitando a sua sequência de procura no campo Procura em qualquer página ibm.com.
- Procure conteúdo usando qualquer mecanismo de procura externo, como Google, Yahoo ou Bing. Se usar um mecanismo de procura externo, é mais provável que seus resultados incluam informações que estejam fora do domínio

ibm.com. Entretanto, às vezes, é possível localizar informações úteis de solução de problema sobre produtos IBM em newsgroups, fóruns e blogs que não estejam no ibm.com.

Dica: Inclua "IBM" e o nome do produto em sua procura se estiver procurando informações sobre um produto IBM.

Obtendo Correções

Uma correção de produto pode estar disponível para resolver seu problema.

Procedimento

Para localizar e instalar correções:

1. Determine qual correção é necessária (Fix Central) (abre na nova janela) (http://www.ibm.com/support/fixcentral/)
2. Faça download da correção. Abra o documento de download e siga o link na seção "Pacote de Download".
3. Aplique a correção seguindo as instruções na seção "Instruções de Instalação" do documento de download.
4. Assine para receber notificações por e-mail semanalmente sobre correções e outras informações do Suporte IBM.

Entrando em Contato com o Suporte IBM

O suporte IBM fornece acesso a uma variedade de recursos IBM para ajuda com questões de software.

Antes de Iniciar

Após tentar localizar sua resposta ou solução usando outras opções de autoajuda como notas técnicas, é possível entrar em contato com o Suporte IBM. Antes de entrar em contato com o Suporte IBM, sua empresa deve ter um contrato de manutenção ativo da IBM e você deve ser autorizado a enviar problemas à IBM. Você também deve ter as seguintes informações em mãos:

- Seu número de identificação de cliente.
- Seu número de solicitação de serviço, se for uma solicitação de serviço em progresso.
- O número de telefone onde você pode ser encontrado.
- A versão do software utilizada.
- A versão do ambiente operacional usada.
- Uma descrição do que estava fazendo quando o problema ocorreu.
- O que as mensagens de erro exibidas dizem, exatamente.
- As ações tomadas para tentar resolver o problema.

Para obter informações sobre os tipos de suporte disponíveis, consulte o tópico Portfólio de Suporte no *Software Support Handbook* (abre na nova janela).

Procedimento

Conclua as seguintes etapas para entrar em contato com o Suporte IBM com um problema:

1. Defina o problema, reúna informações complementares e determine a gravidade do problema. Para obter mais informações, consulte o tópico Obtendo o Suporte IBM (abre na nova janela) no *Software Support Handbook*.
2. Reúna as informações de diagnóstico.
3. Envie o problema para o Suporte IBM de uma das seguintes formas:
   - Usando o IBM Support Assistant (ISA): Use este recurso para abrir, atualizar e visualizar uma Solicitação de Serviço Eletrônica com a IBM. Quaisquer dados que tenham sido coletados podem ser conectados à solicitação de serviço. Isso agiliza a análise e reduz o tempo para resolução.
   - Online através do IBM Support Portal (abre na nova janela): é possível abrir, atualizar e visualizar todas as Solicitações de Serviço a partir do portlet Solicitação de Serviço na página Solicitação de Serviço.
   - Por telefone: para obter o número do telefone a ser chamado, consulte a página da web Diretório de Contatos no Mundo Todo (abre na nova página).

Resultados

Se o problema que enviou for um defeito de software ou documentação ausente ou inexata, o Suporte IBM cria um Authorized Program Analysis Report (APAR). O APAR descreve o problema em detalhes. Sempre que possível, o Suporte IBM fornece uma solução alternativa que é possível de 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 têm o mesmo problema possam se beneficiar da mesma resolução.

Trocando Informações com a IBM

Para diagnosticar ou identificar um problema, talvez seja necessário fornecer ao Suporte IBM dados e informações do seu sistema.

Em outros casos, o Suporte IBM pode fornecer ferramentas ou utilitários para usar para determinação de problema.

Enviando Informações ao Suporte IBM

Para reduzir o tempo que leva para resolver seu problema, é possível enviar informações de rastreio e diagnóstico ao Suporte IBM.

Procedimento

Para enviar informações de diagnóstico ao Suporte IBM:

1. Abra um problem management record (PMR). É possível usar o IBM Support Assistant (abre na nova janela) ou a ferramenta IBM Service Request (abre na nova janela).
2. Colete os dados diagnósticos necessários. Os dados diagnósticos ajudam a reduzir o tempo que leva para resolver seu PMR. É possível coletar os dados diagnósticos manual ou automaticamente.
3. Compacte os arquivos usando o programa TRSMAIN ou AMATERSE. Faça download do utilitário gratuito da IBM para o sistema IBM Cognos Analytics e, em seguida, instale o utilitário usando o comando TSO RECEIVE.
4. Transfira os arquivos para a IBM. É possível usar um dos seguintes métodos para transferir os arquivos para a IBM:
   - A ferramenta Service Request (abre na nova janela)
   - Métodos de upload de dados padrão: FTP, HTTP
   - Métodos seguros de upload de dados: FTPS, SFTP, HTTPS

- E-mail

Se você estiver usando um produto IBM Cognos e usar ServiceLink / IBMLink para enviar PMRs, poderá enviar dados diagnósticos para o suporte IBM em um e-mail ou usando FTP.

Todos esses métodos de troca de dados são explicados no site de Suporte IBM (abre na nova janela).

Recebendo Informações do Suporte IBM

Ocasionalmente, um representante de suporte técnico da IBM pode pedir que faça download das ferramentas de diagnóstico ou de outros arquivos. É possível usar FTP para fazer download desses arquivos.

Antes de Iniciar

Certifique-se de que seu representante de suporte técnico da IBM tenha fornecido o servidor preferencial para usar para o download dos arquivos e os nomes exatos do diretório e do arquivo para acessar.

Procedimento

Para fazer download desses arquivos a partir do Suporte IBM:

1. Use FTP para conectar ao site que seu representante de suporte técnico da IBM forneceu e efetue login como `anonymous`. Use seu endereço de e-mail como a senha.
2. Altere para o diretório apropriado:
   a. Altere para o diretório `/fromibm`.
      ```
      cd fromibm
      ```
   b. Altere para o diretório que seu representante de suporte técnico da IBM forneceu.
      ```
      cd nameofdirectory
      ```
3. Ative o modo binário para sua sessão.
   ```
   binária
   ```
4. Use o comando **get** para fazer download do arquivo que seu representante de suporte técnico da IBM especificou.
   ```
   get filename.extension
   ```
5. Encerre a sessão FTP.
   ```
   abandonar
   ```

Assinando Atualizações de Suporte

Para se manter informado sobre informações importantes sobre os produtos IBM que usar, é possível assinar as atualizações.

Sobre Esta Tarefa

Ao assinar para receber atualizações, é possível receber informações técnicas importantes e atualizações para ferramentas e recursos específicos do Suporte. É possível assinar atualizações usando uma das duas abordagens:

Alimentações RSS e assinaturas de mídia social

Os seguintes Feeds RSS e assinaturas de mídia social estão disponíveis para o IBM Cognos Analytics:

- Feed RSS para um fórum do developerWorks (abre em nova janela).

- Feed RSS para o site de Suporte do IBM Cognos Analytics (abre em uma nova janela)

Para obter informações gerais sobre RSS, incluindo as etapas de introdução e uma lista de páginas da web da IBM ativadas por RSS, visite o site Feeds RSS de Suporte de Software IBM (abre na nova janela).

Minhas Notificações

Com o My Notifications, é possível assinar atualizações de Suporte para qualquer produto IBM. É possível especificar que deseja receber comunicados por e-mail diária ou semanalmente. É possível especificar que tipo de informações deseja receber, como publicações, dicas e sugestões, atualizações de produtos (também conhecidos como alertas), downloads e drivers. O My Notifications permite customizar e categorizar os produtos sobre os quais deseja ser informado e os métodos de entrega que mais bem se adequam a suas necessidades.

Procedimento

Para assinar atualizações do Suporte:

1. Assine as alimentações RSS do *Product*.
2. Para assinar em Minhas Notificações, inicie acessando o IBM Support Portal (abre na nova janela) e clicando em **Minhas Notificações** no portlet **Notificações**.
3. Se já tiver se registrado no My support, efetue sign in e pule para a próxima etapa. Se ainda não tiver se registrado, clique em **Registrar agora**. Preencha o formulário de registro utilizando seu endereço de e-mail como o IBMid e clique em **Enviar**.
4. Clique em **Editar perfil**.
5. Clique em **Incluir produtos** e escolha uma categoria de produto; por exemplo, **Software**.
6. Na segunda lista, selecione um segmento de produto; por exemplo, **Gerenciamento de Dados & Informações**.
7. Na terceira lista, selecione um subsegmento de produto; por exemplo, **Bancos de Dados**.
8. Selecione os produtos dos quais deseja receber atualizações.
9. Clique em **Incluir produtos**.
10. Após selecionar todos os produtos que sejam do seu interesse, clique em **Assinar por e-mail** na guia **Editar perfil**.
11. Selecione **Enviar estes documentos por e-mail semanalmente**.
12. Atualize seu endereço de e-mail conforme necessário.
13. Na **Lista de documentos**, selecione a categoria do produto; por exemplo, **Software**.
14. Selecione os tipos de documentos dos quais deseja receber informações.
15. Clique em **Atualizar**.

Resultados

Até que modifique suas preferências de alimentação RSS e do My Notifications, você receberá notificações de atualizações que solicitou. É possível modificar suas preferências quando necessário (por exemplo, se parar de usar um produto e começar a usar outro).

Arquivos de log

Os arquivos de log podem ajudá-lo a resolver problemas registrando as atividades que acontecem ao trabalhar com um produto.

As operações executadas no IBM Cognos Analytics são registradas em vários arquivos de log para propósitos de rastreamento. Por exemplo, se você teve problemas ao instalar o IBM Cognos Analytics, consulte o arquivo de log de transferência para aprender quais atividades o assistente de instalação executou ao transferir os arquivos.

Antes de começar a visualizar os arquivos de log, certifique-se de que eles contêm as informações de que precisa.

Use o IBM Cognos Administration para configurar o nível de detalhes para registrar para cada categoria.

Para obter mais informações, consulte o *IBM Cognos Analytics: Guia de Administração e Segurança*.

Use IBM Cognos Configuration para especificar o tamanho, o número e o local dos arquivos de log e para configurar as propriedades do servidor de log.

Ao solucionar problemas, os seguintes arquivos podem ajudá-lo:

arquivo de log de Transferência

Esse arquivo registra os componentes instalados, a informações de espaço em disco, as seleções realizadas em diálogos de transferência e qualquer erro que o assistente de instalação encontrou ao transferir os componentes. Ele também registra as atividades que o assistente de instalação executou ao transferir arquivos.

O arquivo de log de transferência está localizado no diretório *install_location*\logs. O nome do arquivo inclui o nome do produto e o registro de data e hora. A seguir, um exemplo do formato de nome de arquivo:

```
IBM_Cognos_Analytics_Install_04_21_2016_11_00_59.log
```

Arquivo de log da Configuração de Instalação

Esse arquivo de log registra qualquer atividade de configuração durante a instalação. Por exemplo, ele relata a porta disponível para o dispatcher.

O arquivo de log de erro de resumo de transferência está localizado no diretório *install_location*\logs. Ele é denominado install_configuration.log

Arquivo de configuração da inicialização

Esse arquivo registra as escolha de configuração cada vez que as configurações de propriedades são salvas. O nome de arquivo é cogstartup.xml.

Se não conseguir salvar suas configurações, ou se estiver tendo problemas é possível reverter para um arquivo de configuração previamente salvo. Os arquivos de configuração de backup estão localizados no diretório *install_location*/configuration. A seguir, um exemplo do formato de nome de arquivo para o backup dos arquivos de configuração:

cogstartup_200811231540.xml

Arquivo de bloqueio da configuração da inicialização

Esse arquivo é criado cada vez que você abre o IBM Cognos Configuration. Isso evita que você abra mais de uma janela do IBM Cognos Configuration.

Se você tiver problemas ao abrir o IBM Cognos Configuration, é possível verificar o diretório *install_location*/configuration para o arquivo cogstartup.lock. Se o arquivo existir e o IBM Cognos Configuration não estiver aberto, isso significa que o IBM Cognos Configuration não foi encerrado corretamente na última vez que você o usou. É possível excluir o arquivo de bloqueio e abrir o IBM Cognos Configuration.

O arquivo de configuração de código do idioma

Esse arquivo registra as opções de configuração feitas no IBM Cognos Configuration para códigos do idioma de produto e conteúdo, mapeamento de localidade e suporte à moeda.

Se tiver problemas com o suporte ao idioma na interface com o usuário ou em relatórios, use esses arquivos para controlar as mudanças. Os arquivos de configuração de backup estão localizados no diretório *install_location*/configuration. A seguir, um exemplo do formato de nome de arquivo:

coglocale_200811231540.xml

Arquivo de log de tempo de execução

O arquivo de log padrão do IBM Cognos, denominado arquivo cogaudit.log, ou outros arquivos de log que você configura para receber mensagens de log do servidor de log registram informações após iniciar o serviço do IBM Cognos Analytics. Eles estão localizados no diretório *install_location*/logs. Se foi configurado outro destino para as mensagens de log, verifique o arquivo ou banco de dados adequado.

Algumas mensagens de log indicam problemas. A maioria das mensagens somente fornece informações, mas outras podem ajudá-lo a diagnosticar problemas em seu ambiente de tempo de execução.

Arquivo de log do gateway

Os gateways registram erros no arquivo de log do gateway, localizado no diretório *install_location*/logs.

É possível usar o arquivo de log do gateway para solucionar problemas que evitam que o gateway processe solicitações ou use criptografia. Os sintomas desses problemas são os seguintes:

- IDs e senhas dos usuários não funcionam.
- A conexão única não funciona.
- O dispatcher está em execução, mas os usuários recebem uma mensagem de erro avisando que o servidor do IBM Cognos Analytics não está disponível.

O arquivo de log do gateway usa o seguinte formato de nomenclatura, onde *gateway_interface* é cgi, mod2 (Apache 2.0 module) ou isapi.

gw*gateway_interface*.log (por exemplo, gwcgi.log)

Arquivo de log de desinstalação

O arquivo registra as atividades realizadas pelo assistente de desinstalação ao desinstalar os arquivos. O arquivo de log é chamado de cognos_uninst_log.htm e está localizado no diretório Temp. É possível usar o arquivo de log para solucionar problemas relacionados a desinstalar os componentes do IBM Cognos Analytics.

Arquivo de log do modo silencioso

Esse arquivo registra as atividades que o IBM Cognos Configuration executou durante a execução no modo silencioso. Esse arquivo de log é denominado cogconfig_response.csv e está localizado no diretório *install_location*/logs.

Apêndice C. Avisos de descontinuação

Este tópico lista os recursos descontinuados em liberações futuras do IBM Cognos Analytics.

- O uso de *install_location*\webapps\p2pd\WEB-INF\lib para localizar drivers JDBC foi descontinuado para liberações futuras. Ele foi substituído pelo diretório *install_location*\drivers.

Apêndice D. Sobre este Manual

Este documento foi criado para usar com o IBM Cognos Analytics. O IBM Cognos Analytics é um produto da web com recursos integrados de relatório, painéis, análises e gerenciamento de eventos.

Este guia contém instruções para instalar, fazer upgrade, configurar e testar o IBM Cognos Analytics.

Público-alvo

Para utilizar esse guia, é preciso estar familiarizado com

- Conceitos de relatórios.
- conceitos sobre banco de dados e armazém de dados
- problemas de segurança
- qualificações de administração básicas do Windows ou UNIX
- ambiente do servidor e infraestrutura de segurança existentes em sua organização

Localizando Informações

Para localizar a documentação do produto na web, incluindo toda a documentação traduzida, acesse IBM Knowledge Center(http://www.ibm.com/support/knowledgecenter). As Notas sobre a Liberação são publicadas diretamente no IBM Knowledge Center e incluem links para as notas técnicas e APARs mais recentes.

Também é possível ler as versões em PDF dos arquivos de ajuda on-line do produto clicando nos links de PDF na parte superior de cada página HTML ou acessar os PDFs na página da web da documentação do produto IBM Cognos (www.ibm.com/support/docview.wss?uid=swg27047187).

Instruções para Procura de Versões Futuras

Esta documentação descreve a funcionalidade atual do produto. Referências a itens que não estão disponíveis atualmente podem estar incluídas. Não se deve inferir implicações de qualquer disponibilidade futura. Tais referências não representam um compromisso, uma promessa ou uma obrigação legal de entrega de qualquer material, código ou funcionalidade. O desenvolvimento, a liberação e a sincronização de recursos ou funcionalidade ficam ao arbítrio exclusivo da IBM.

Termo de responsabilidade das amostras

A Companhia de Aventuras de Amostra, a Companhia das Grandes Aventuras, a Vendas GA, qualquer variação dos nomes Aventuras ou Grandes Aventuras e a Amostra de Planejamento representam operações de negócios fictícias com dados de amostra usados para desenvolver aplicativos de amostra para a IBM e para os clientes IBM. Estes registros fictícios incluem dados de amostra para transações de vendas, distribuição de produtos, finanças e recursos humanos. Qualquer semelhança com nomes, endereços, números de contato ou valores de transação é coincidência. Outros arquivos de amostra podem conter dados fictícios gerados manualmente ou por máquina, dados reais compilados de origens acadêmicas ou públicas ou dados usados com permissão do portador do copyright, para serem

usados como dados de amostra para o desenvolvimento de aplicativos de amostra. Os nomes de produtos referidos podem ser marcas registradas de seus respectivos proprietários. A cópia não autorizada é proibida.

Índice Remissivo

Numéricos

64 bits
  servidor de relatório 91

A

AIX
  variáveis de ambiente 60, 64, 83, 96
ajuste
  Armazenamento de conteúdo do Db2 279
algoritmo de confidencialidade 157
alias da web
  IBM Cognos Analytics 97
aliases
  configurando nos servidores da web 97
alimentações RSS
  resolução de problemas 318
alterando
  codificação para e-mail 217
  definições de configuração padrão 149
  modelo de configuração 280
  URIs 149
  versões Java 147
ambientes suportados 2
amostras
  IBM Cognos Workspace 230
áreas de trabalho
  estilos de relatórios 230
armazenamento de conteúdo
  criando áreas de tabela 68
  criando no Oracle 12
  descrição do componente 24
  diversas versões do IBM Cognos BI 43
  e outros locais para armazenar saída de relatório 168
  gerenciamento de conexão 74
  utilizando SSL 188
Armazenamento de conteúdo do Db2 279
  script 67
armazenamento de objeto externo
  para saída de relatório 172
  testando conexão 173
arquitetura 24
arquivando
  Conteúdo do IBM Cognos 303
  saída de relatório 169
arquivo apache_mod
  configurando para gateways 132
arquivo cogstartup.lock 321
arquivo cogstartup.xml 284, 288
  alterando propriedades manualmente 286
arquivo de especificação de transferência (.ats)
  configuração 291
arquivo de instalação
  fazendo o download de modeladores do Transformer 143
arquivo de instalação do Transformer 143
arquivos chase_referral 246
arquivos de biblioteca 9
arquivos de configuração
  coglocale.xml 286
  cogstartup.xml 284
arquivos de configuração *(continuação)*
  exportação 296
arquivos de implementação
  em movimento 49
  importando 50
arquivos de log 320
  configuração de inicialização 320
  configuração de instalação 320
  configuração do código do idioma 321
  desinstalação 322
  erros do gateway 321
  modo silencioso 322
  tempo de execução 321
  transferência 320
Arquivos JRE
  atualização 6
ativação
  IBM Cognos Application Firewall 160
ativando
  serviços 163
atualização 37
  ambiente java 6
  armazenamento de conteúdo 47
  comparando relatórios de versões diferentes 51
  de outros produtos IBM Cognos para o IBM Cognos Analytics 34
  especificações do relatório 51
  ferramentas que suportam atualização do IBM Cognos ReportNet 36
  movendo conteúdo 46
  processo 37
  recursos 39
  tarefas 42
auditoria
  logs 200
autenticação
  árvores de domínio para Active Directory Server 246
  CA SiteMinder 267
  conexão única usando LDAP 266
  conexão única usando o Active Directory Server 246
  conexão única usando o namespace do IBM Cognos Series 7 252
  conexão única usando SAP 273
  configurando namespace do IBM Cognos Series 7 251
  desativando logon anônimo 234
  excluindo namespaces 273
  função SaferAPIGetTrustedSignon 253
  LDAP 257, 258
  LDAP usando Active Directory Server 259
  LDAP usando IBM Directory Server 260
  LDAP usando Novell Directory Server 261
  LDAP usando Oracle Directory Server 263
  plug-ins de conexão confiável para IBM Cognos Series 7 253
  propriedades customizadas para Active Directory Server 244
  propriedades de usuário customizadas para LDAP 264
  provedores de autenticação customizada 255
  requisitos para conexão única com Microsoft Analysis Server ou Microsoft SQL Server 243
  SAP 271

autenticação *(continuação)*
Servidor Active Directory 243
SiteMinder 269
SSL usando LDAP 265
usando namespaces 233
autenticação do Kerberos 248
delegação restrita 249
autenticação do Windows 246
autoridade de certificação
configurando 179
configurando o serviço 179

B

balanceamento de carga 14, 107, 108
ativando e desativando serviços 163
configurações do servidor de e-mail 80
configurando 26
banco de dados de criação de log
criando usando Microsoft SQL Server 13
criando usando Oracle 12
criando usando servidor de banco de dados Informix 14
Db2 9
diretrizes de criação 201
espaços de tabela para o Db2 on z/OS 202
utilizando SSL 188
banco de dados de notificação
configurações para o Db2 on z/OS 175
configurando 177
criação 174
criando áreas de tabela 68
espaços de tabela para o Db2 for z/OS 176
utilizando SSL 188
banco de dados de tarefa manual e de anotações
espaços de tabela no Db2 on z/OS 224
banco de dados do Cognos Mobile
configurando 92
criando tabelas manualmente 92
bancos de dados
cliente do banco de dados de criação de log 203
criação de log 205
notificação 80
bancos de dados de consulta 24

C

CA,
Veja autoridade de certificação
CA SiteMinder 267
verificação de script cruzado no IBM Cognos Application Firewall 160
camada de dados
Content Manager 20
camada do aplicativo
componentes 20
caminhos
configuração para cookies 219
caracteres especiais
nas propriedades do namespace LDAP 257
Certificados 1024-bit 177, 178
certificados CA 177, 178
Certificados SHA1 177, 178
chave simétrica comum 155
Chinês simplificado
configurando fontes 163, 166
cliente de banco de dados
configurando para um banco de dados de criação de log 203
requisitos para modeladores do Transformer 143
requisitos para Transformer 32
codificação de e-mail em tailandês
requisitos do JRE 217
código do idioma do usuário
mapeando para o código do idioma do conteúdo 214
códigos de idioma do produto
exibindo códigos do idioma suportados 212
mapeando para a interface com o usuário 216
códigos de página para origens de dados 134, 140
códigos do idioma
exibindo códigos de idioma do produto suportados 212
exibindo códigos do idioma de conteúdo suportados 213
códigos do idioma do conteúdo
customizando 213
exibindo códigos do idioma suportados 213
mapeando para o código do idioma do usuário 214
Coexistência 43
cogconfig.sh
opções da linha de comandos 311
Cognos Workspace domínios aprovados 160
colaboração
usando o IBM Connections 160
componentes 19
armazenamento de conteúdo 24
componentes de camadas de aplicativos 26, 28
Content Manager 20, 26
distribuindo 32
Event Studio 22
Framework Manager 23
gateways 22
IBM Cognos Administration 21
IBM Cognos Configuration 20
IBM Cognos Workspace 22
Map Manager 24
origens de dados 24
Portal do Cognos Analytics 20
Query Studio 22
Relatórios 20
Transformer 23
Componentes da camada de aplicativos
servidor de log 200
componentes de camadas de aplicativos
instalando no computador separado 26
requisitos de configuração 28
Componentes de modelagem 23
arquivo de instalação para modeladores do Transformer 143
opções de instalação 28
componentes do Cognos Mobile 24
componentes do servidor 19
opções de instalação 28
sequência de instalação 57
comunicação LDAP segura 265
conectividade do banco de dados
banco de dados de relatório 85
conexão única
usando o namespace do IBM Cognos Series 7 252
Conexão única Kerberos
JDBC 195, 196, 198
conexões de origens de dados
configurando 74
conexões do banco de dados 74
MS SQL Server e SSL 189

conexões do banco de dados *(continuação)*
SSL 189
conexões ODBC para origens de dados 86
confiança compartilhada
configurando entre o IBM Cognos Analytics e outros servidores 186
configuração
alterando configurações padrão 149
alterando o modelo 280
arquivo de bloqueio 321
automatizando 291
configurações globais 211
configurações para o Cognos Analytics 7
Content Manager 26
executando a partir da linha de comandos 288
grupo de configurações 152, 154
incluindo recursos 284
não assistida 291, 296
não é possível abrir o IBM Cognos Configuration 321
requisitos para conexão única com Microsoft Analysis Server ou Microsoft SQL Server 243
várias versões do IBM Cognos Analytics 43
configuração de cliente
bancos de dados Db2 67
configuração não assistida
alterando propriedades 286
configurando 291
configuração silenciosa 291
configurações de memória 4
configurações de ulimit 5
configurando 311
apache_mod para o gateway 132
arquivo de especificação de transferência (.ats) 291
bancos de dados de notificação 177
confiança compartilhada com outros servidores 186
Content Manager em espera 78
destino para mensagens de log 200
fontes 163
Framework Manager 30
fuso horário padrão 217
gateways 99
gráficos de mapa do Relatórios 170
IBM Cognos Analytics 14
IBM Cognos Analytics para trabalhar com outros produtos IBM Cognos 231
IBM Cognos Workspace 222
Infraestrutura de Segurança do Entrust 158
ISAPI para o gateway 132
local de arquivos temporários 162
namespace do Active Directory 243
namespace LDAP 258
namespace LDAP para Active Directory Server 259
namespace LDAP para IBM Directory Server 260
namespace SAP 272
namespace SiteMinder 269
não assistida 296
Navegadores da web 15
propriedades de ambiente para componentes de serviço de aplicativo 89
propriedades em uma configuração não assistida 286
protocolo SSL 184
provedor de criptografia padrão 157
provedores de autenticação customizada 255
roteadores 230
serviço de autoridade de certificação 179
serviço do IBM Cognos 280
servidor da web 97
configurando *(continuação)*
Transformer 31
conjuntos de códigos
configurando uma prioridade para conexões SSL 187
conta do usuário
requisitos para execução do serviço do IBM Cognos 73, 88
Content Manager
alterando fusos horários 217
ativo e em espera 63, 172
componente 26
configuração 26
configurando em diversos computadores 78
descrição do componente 20
espera 26
opções de instalação 26
proteção contra failover 26
replicação 172
requisitos em caso de uso do IBM Cognos Transformer com namespace Series 7 135, 251
salvando saída de relatório externamente 172
servidor de log 200
Content Manager 8
desligando o arquivamento de especificação de relatório 310
Content Manager ativo 63
Content Manager em espera 26, 63
configurando 78
Cookies
ativando em navegadores da Web 15
configurações 219
customizando 219
cookies HTML,
Veja Cookies
credenciais do usuário
alterando na configuração não assistida 286
criação de log
banco de dados 205
cliente de banco de dados 203
configurando 205
servidores remotos de log 204
usando arquivos 205
criação de log de diagnóstico
resolução de problemas de namespaces do OpenID Connect 241
criptografia
alterando definições na configuração não assistida 286
criptografia de propriedades de arquivo temporário 162

D

Db2
conectividade do banco de dados 85
configuração de cliente 67
drivers de banco de dados 67
especificando como um repositório de mensagem de log 205
páginas de códigos 134, 140
desempenho
calculando a largura da banda 280
calculando servidores 280
estimando 280
desinstalação
Cognos Analytics 300
Framework Manager 300
IBM Cognos Analytics 299
Transformer 300
desinstalação autônoma 297

desinstalação no modo silencioso 297
Desinstalar
  malsucedido 301
destinos de log
  tipos de 200
determinação de problema
  trocando informações com o suporte IBM 317
diagnósticos
  Veja resolução de problemas
Diretório Ativo
  LTPA 238
diretório-raiz
  para salvar a saída de relatório fora do IBM Cognos Analytics 168
diretórios JDBC
  configurando bancos de dados Oracle 204
diretórios virtuais
  IBM Cognos Analytics 97
dispatchers
  excluindo 48
  importação 50
  métricas do sistema 275
distribuição de relatório
  em uma rede 281
domínios
  aprovados para o Cognos Workspace 160
  árvores de domínio do Active Directory Server 246
  configuração para cookies 219
drivers de banco de dados
  Db2 67
  Informix 72, 204
  Oracle 72

E

e-mails
  alterando a codificação 217
efetuando login
  configurando segurança 81
  ocultando namespaces durante 256
entrega
  diminuindo o tempo para abrir relatórios 281
espaços de nome
  configurando para um gateway 162
  configurando provedores de autenticação customizada 255
  ocultando durante o login 256
  OpenID Connect 239
  requisitos para Content Manager em caso de uso do Transformer com namespace Series 7 251
especificações do relatório
  atualização 51
  desligando o arquivamento 310
estilos de análise
  em áreas de trabalho 230
estilos de consulta
  em áreas de trabalho 230
estilos de relatórios
  em áreas de trabalho 230
Event Studio
  descrição do componente 22
excluindo
  dispatchers 48
exportação
  arquivos de configuração 296

F

FileNet
  desligando o arquivamento de especificação de relatório 310
  importando classes customizadas 306
Firefox
  configurações 15
firewalls
  acesso entre o Transformer e o Cognos Analytics 139
  considerações de instalação 29
fontes
  alterando o padrão 166
  alterando para relatórios PDF 166
  configurando 163
  lista de fontes integradas para relatórios PDF 167
  usando fontes do sistema no Cognos Configuration 166
fontes integradas 167
fontes PDF
  mapeando para fontes PDF integradas para impressão de relatório mais rápida 165
formatos de saída
  restringindo 309
Framework Manager
  Veja também Cognos Framework Manager
  configurando 30
  configurando origens de dados 134
  dentro do firewall de rede 132
  descrição do componente 23
  desinstalação 300
  fora de um firewall 132
  instalando 129, 130
  opções de instalação 30
  requisitos do sistema 130
  testando a instalação e a configuração 135
função SaferAPIGetTrustedSignon
  usando para autenticação 253
fusos horários
  alterando 217
fusos horários do servidor
  alterando 217

G

gateway
  configurando para o Transformer 139
  instalando 96
  usando os gateways de 32 bits 98
gateway ISAPI 121
gateways
  Arquivo de log 321
  configurando 99
  configurando apache_mod 132
  configurando ISAPI 132
  configurando para usar um namespace 162
  descrição do componente 22
  incluindo em uma rede para diminuir tempos de entrega 281
gateways de 32 bits 98
GB18030 163, 166
Google Chrome
  configurações 15
gráficos de mapas 170
grupo de configurações 152, 154

H

httpEndpoint
  grupo de configurações 152

I

IBM Cognos Administration
  descrição do componente 21
IBM Cognos Analytics
  configurando 14
  desinstalação 299
  dispatchers 279
  efetuando login 81
  resolução de problemas das instalações 313
  serviços 279
IBM Cognos Analytics for Microsoft Office 22
IBM Cognos Application Firewall
  configurando 160
IBM Cognos Configuration
  descrição do componente 20
  modo autônomo 296
  opções da linha de comandos 311
  problemas ao abrir 321
  usando fontes do sistema 166
IBM Cognos Content Archival
  repositório externo 303
IBM Cognos Controller
  acesso a dados no IBM Cognos Analytics 35
IBM Cognos Planning - Analyst
  acesso a dados no IBM Cognos Analytics 34
IBM Cognos Planning - Contributor
  acesso a dados no IBM Cognos BI 34
  ativando agentes e relatórios programados 231
IBM Cognos Series 7
  ativando a conexão única 252
  ativando SSL 252
  plug-ins de conexão confiável 253
  usando para autenticação 251
IBM Cognos Series 7 PowerCubes
  requisitos para conversão de idioma bem-sucedida 35
IBM Cognos Transformer
  configurando origens de dados 140
IBM Cognos Workspace 22
  amostras 230
  configurando 222
  estilos de relatórios 230
  requisitos para carregar o Microsoft IIS 223
IBM Connections 160
  configurar colaboração 221
IBM Content Manager 8
  importando classes customizadas 307
  importar
    classes customizadas para IBM Content Manager 8 307
IBM Db2
  criando sequências de conexões 74
IBM Directory Server
  com um namespace LDAP 260
IBM FileNet Content Manager 303
IBM Java Software Development Kit 210
IBMid 241
idioma
  configurando para a interface com o usuário do Transformer 136
  customizando para a interface com o usuário 212
  customizando suporte ao conteúdo do código do idioma 213
IIS
  configurando 116
  configurando SSO 116
imagens
  carregando no Relatórios 97
  validade do conteúdo 97
implementando
  objetos de configuração 50
  Transformer para modeladores 145
importando
  arquivos de implementação 50
  configurações 50
importar
  classes customizadas para o FileNet 306
impressão de relatórios
  customizando para servidores de impressão UNIX e Linux 174
Informix
  criando o armazenamento de conteúdo 14
  criando um banco de dados de criação de log 14
  drivers de banco de dados 72, 204
  especificando como um repositório de mensagem de log 205
Infraestrutura de Segurança do Entrust 158
inicialização
  arquivo de bloqueio de configuração 321
iniciando o Cognos Analytics 127
iniciando o serviço do Cognos
  a partir da linha de comandos 288
inscrevendo
  modelos de resolução de problemas 318
instalação 61
  básica para diversos locais 58
  modos 59
  não assistida 291
  opções do componente do servidor 28
  opções para Framework Manager 30
  opções para o Content Manager 26
  opções para Transformer 31
  testando o Framework Manager 135
  testando o Transformer 142
  UNIX, Linux 60
instalação em Windows 61
instalação não assistida
  configurando 291
  modelos de arquivo de resposta 293
instalações básicas
  diversos locais 58
instalações distribuídas
  cenários 25
  opções 32
instalações silenciosas 291
instalando
  distribuindo componentes 32
  Framework Manager 129
  IBM Cognos Analytics 291
  instalação não assistida 291
  opções 32
  sequência para componentes do servidor 57
  teste 82, 92, 127
  Transformer 135
Integrated Facility for Linux (IFL) 28
interface
  customizando suporte ao idioma 212
interface com o usuário
  customizando suporte ao idioma 212
  mapeando para o código de idioma do produto 216

Internet Explorer
configurações 15
IPv4 219
IPv6 219
ISAPI
configurando para o gateway 132

J

Java
alterando versões 147
atualizando ambientes de tempo de execução 6
Java Management Extensions
com logs de usuário 210
configurando propriedades JMX para monitoramento remoto de métricas do sistema 275
Java Software Development Kit da IBM 275
Javascripts
ativando em navegadores da Web 15
JDBC
Conexão única Kerberos 195, 196, 198
JVM
alterando 147

L

largura da banda
estimando 280
latência
melhorando 281
LDAP
Active Directory Server 259
ativando a conexão única 266
ativando SSL 265
configurando um namespace 258
editando a propriedade de mapeamento de identidade externa 267
IBM Directory Server 260
LTPA 236
Novell Directory Server 261
Oracle Directory Server 263
propriedades customizadas 264
usando para autenticação 257
Lifecycle Manager 36, 51
lightweight third-party authentication (LTPA) 236
Diretório Ativo 238
namespace LDAP 236
limite de tempo assíncrono 281
Linux
conexões ODBC com origens de dados 86
configurações de ulimit 5
iniciando e parando o serviço do Cognos 288
mensagens de log 205
variáveis de ambiente 60, 64, 83, 96
listas de incorporação de fontes 167
locais
gráficos de mapas 170
local de arquivos temporários 162
configurando 162
log de eventos do Windows
destino para mensagens de log 205
logon anônimo
desativando 234
logs
processamento de mensagens 200
serviço 278
logs de auditoria
Veja também mensagens de log
Veja também resolução de problemas
destinos de log 200
logs de eventos 205
logs de usuário 210

M

manutenção
melhorando o desempenho do sistema 275
Map Manager
descrição do componente 24
mensagens de log
Veja também logs de auditoria
Veja também resolução de problemas
ativação para o IBM Cognos Application Firewall 160
destinos de log 200
Servidor de log remoto. 200
métricas
para servidores, dispatchers e serviços 275
métricas do sistema
monitoramento remoto 275
Microsoft Analysis Server
requisito de namespace 243
Microsoft Analysis Services
conexão única com origens de dados MSAS 246
configurando o ambiente de origem de dados 134, 140
Microsoft IIS
configurando SSL no 115
requisitos para carregar o IBM Cognos Workspace 223
Microsoft Office
serviço de dados de relatório 279
Microsoft SQL Server
conectividade do banco de dados 85
criando sequências de conexões 74
especificando como um repositório de mensagem de log 205
requisito de namespace 243
SSL 189
modeladores
implementando Transformer 145
modelagem 23
modelos
alterando o tamanho do modelo 280
modo autônomo 291
modo de consulta compatível
configurações de memória 4
origens de dados de 64 bits 85
modo de consulta dinâmica 85
conectividade do banco de dados 85
configurações de memória 4
modo silencioso 291
Módulos do Apache 111
moeda
customizando suporte 212
MSAS,
Veja Microsoft Analysis Services
multi_domain_tree 246

N

namespaces
autenticação 233
exclusão 273
não é possível abrir o IBM Cognos Configuration 321

Navegadores da web
configurações de segurança 2
configurando 15
Netezza
conectividade da origem de dados 85
configurando conexões ODBC 86
NIST SP800-131a 177, 178
notas sobre a liberação
revisando 1
Novell Directory Server
com um namespace LDAP 261

O

opções da linha de comandos 311
opções de inicialização 311
opções de instalação 25
Componentes de modelagem 28
OpenID Connect
configurando um namespace 241
criação de log de diagnóstico 241
provedores de identidade 241
provedores de identidade suportados 239
Oracle
conectividade do banco de dados 85
criando sequências de conexões 74
drivers de banco de dados 72
drivers JDBC de banco de dados 204
especificando como um repositório de mensagem de log 205
suporte multilíngue 134, 140
Oracle Directory Server
com um namespace LDAP 263
Oracle Essbase
configurando 87
Microsoft Windows de 64 bits 88
UNIX 88
Oracle ESSBASE
conectividade da origem de dados 85
Oracle Java SE Development Kit 210, 275
origens de dados
conexões ODBC 86
descrição do componente 24
para Framework Manager 134
para IBM Cognos Transformer 140
outros componentes 24

P

parando o serviço do Cognos
a partir da linha de comandos 288
períodos de blecaute
especificando 308
permissões
desvio 222
execução 222
para a conta do usuário que é usada para o serviço do IBM Cognos 73, 88
para modeladores do Transformer 143
política de configuração 222
Planning Analytics 36
pools de aplicativos 97
porta de serviço do conjunto de dados
alterando 151
Portal do Cognos Analytics 20
portas
alterando 149, 151
definições de configuração padrão 7
porta de serviço do conjunto de dados 151
várias versões do IBM Cognos Analytics 43
PowerCubes
acesso no IBM Cognos Analytics 35
requisitos para conversão de idioma bem-sucedida 35
processamento de mensagens de log 200
produtos
versões suportadas 2
propriedade Consulta de usuário
caracteres especiais para namespace LDAP 257
propriedade de mapeamento de identidade externa
caracteres especiais para namespace LDAP 257
editando para um namespace LDAP 267
propriedade Senha e DN do usuário de ligação
caracteres especiais para namespace LDAP 257
propriedades
alterando na configuração não assistida 286
local de arquivos temporários 162
propriedades customizadas de usuário
LDAP 264
Servidor Active Directory 244
proteção contra failover 26
protocolo
endereço IP 219
provedor de autenticação
configurando IBM Cognos BI para usar segurança 81
provedor de criptografia
configurações 157
solicitação de assinatura de certificado 181
provedor de identidade para OpenID Connect 239
provedores de autenticação customizada 255
provedores de identidade para OpenID Connect 241
público-alvo do documento 325

Q

qualidade de proteção em conexões SSL 187
Query Studio
descrição do componente 22

R

recuperando-se de uma desinstalação malsucedida 301
recursos
incluindo 284
relatórios
alterando a fonte padrão 166
customizando suporte ao idioma 213
diminuindo o tempo de entrega 281
Relatórios
carregando imagens 97
descrição do componente 20
mudança do local dos gráficos de mapa 170
removendo o registro
dispatchers 48
reportando necessidades
para usuários do Transformer 32
repositório externo
arquivando conteúdo 303
requisitos de software
versões do produto suportadas 2
requisitos do sistema 2
Framework Manager 130

requisitos do sistema *(continuação)*
Transformer 136
resolução de problemas 313
assinando o suporte 318
bases de conhecimento
procurando soluções de resolução de problemas 315
correções
obtendo 316
criação de log 200
entrando em contato com o Suporte IBM 316
identificando problemas 313
obtendo correções 316
para um usuário específico 210
procurando em bases de conhecimento 315
trocando informações com o suporte IBM 317
roteadores
configurando 230

S

Safari 5
configurações 15
saída de relatório
compartilhando com usuários fora do IBM Cognos Analytics 168
reutilizando 169
salvando em um sistema de arquivos 168
sAMAccountName
utilizando Autenticação do Kerberos 249
SAP
ativando a conexão única 273
usando para autenticação 271
SAP BW
conectividade 272
conectividade da origem de dados 85
configurações de autorização para administradores do IBM Cognos BI 272
configurações de autorização para usuários do IBM Cognos BI 271
script ativo
ativando em navegadores da Web 15
scripts
criando um armazenamento de conteúdo no Db2 67
Secure Sockets Layer,
Veja SSL
segurança.
ativando 81
configurações para navegadores da Web 2
senhas
alterando na configuração não assistida 286
sequências de conexões de banco de dados
IBM Db2 74
Microsoft SQL Server 74
Oracle 74
Series 7 IQD Bridge
instalando 135
Series 7 PowerCubes
requisitos para conversão de idioma bem-sucedida 35
serviço
gráficos 277
tarefa manual 277
Serviço Content Manager 277
serviço de anotação 277
serviço de apresentação 279
Serviço de apresentação
requisitos 276
serviço de consulta 279
serviço de dados de relatório 279
serviço de entrega 277
serviço de gerenciamento de eventos 277
serviço de gráficos 277
Serviço de metadados 278
serviço de metadados relacionais 279
Serviço de migração 278
serviço de monitor 279
Serviço de Relatório
lista de fontes integradas para relatórios PDF 167
requisitos 276
serviço de relatórios em lote 277
Serviço de relatórios em lote
lista de fontes integradas para relatórios PDF 167
serviço de tarefa 277
serviço de tarefa realizada por usuários 277
serviço do agente 276
serviço do Cognos
iniciando a partir da linha de comandos 288
serviço do IBM Cognos
configurando 280
parando a partir da linha de comandos 288
requisitos para a conta do usuário que é usada para o serviço 73, 88
serviço Interactive Discovery Visualization 277
serviço móvel 278
serviços
agente 276
ajustando para melhorar o desempenho 276
anotação 277
apresentação 276, 279
ativando e desativando 163
consulta 279
Content Manager 277
dados do relatório 279
desinstalação 299
entrega 277
gerenciamento de eventos 277
IBM Cognos Analytics 279
iniciando a partir da linha de comandos 288
Interactive Discovery Visualization 277
log 278
Metadados 278
metadados relacionais 279
métricas do sistema 275
Migração 278
monitor 279
móvel 278
parando a partir da linha de comandos 288
relatório 279
Relatório 276
relatório em lote 277
repositório 279
tarefa 277
serviços de relatório 279
serviços de repositório 279
Servidor Active Directory
ativando a conexão única 246
ativando SSL 245
autenticando em diversos domínios 246
com um namespace LDAP 259
propriedades avançadas 246
usando para autenticação 243
servidor de e-mail
configurando 80
servidor de relatório
ativar 64 bits 91

Servidor HTTP Apache
configurando para o Cognos Analytics 11.0.4 108
Servidor HTTP Appache
configurando para o Cognos Analytics 11.0.5+ 107
Servidor IBM HTTP
configurando para o Cognos Analytics 11.0.4 108
configurando para o Cognos Analytics 11.0.5+ 107
servidores
calculando números 280
métricas do sistema 275
servidores baseados em função
considerações para Transformer 31
servidores da web
ativando SSL 105
configurando 97
configurando o tempo de carregamento do Relatórios 97
servidores da Web
conexão única usando Active Directory e servidor da Web IIS 246
servidores da web Apache
configurando alias 97
servidores da Web IIS
conexão única usando Active Directory 246
servidores remotos de log 204
configurando 205
sinalizador seguro
configuração para cookies 219
sistema de arquivos
para salvar cópias da saída de relatório 168
sistema operacional
configurações de memória 4
sistemas operacionais
versões suportadas 2
SiteMinder
configurando namespaces 269
Solaris
variáveis de ambiente 60, 64, 83, 96
solicitação de assinatura de certificado 181
SSL
ativando em servidores da web 105
configurando 115, 184
configurando confiança compartilhada com outros servidores 186
Microsoft SQL Server 189
namespace LDAP 265
para o banco de dados de armazenamento de conteúdo 188
para o banco de dados de criação de log 188
para o banco de dados de notificação 188
qualidade de proteção 187
Servidor Active Directory 245
usando o namespace do IBM Cognos Series 7 252
SSO 107, 108
Suporte IBM
entrando em contato 316
enviando e recebendo informações 317
syslog
destino para mensagens de log 205

T

tablespaces 279
Db2 for z/OS 176
Db2 on z/OS 202, 224
scripts de armazenamento de conteúdo 68
tempos de arquivamento
especificando 308
tempos de execução de encadeamento
especificando 308
Teradata
conectividade da origem de dados 85
teste
Framework Manager 135
instalação do Transformer 142
teste da instalação 82, 92, 127
tipos MIME
deve ser especificado no Microsoft IIS para carregar o IBM Cognos Workspace 223
TM1
conectividade da origem de dados 85
Transformer
acessando o Cognos Analytics fora de um firewall 139
acesso a dados no IBM Cognos Analytics 35
configurando 31
descrição do componente 23
desinstalação 300
etapas para testar a instalação 142
implementando para modeladores 145
instalando 129, 135, 136
instalando em Linux e UNIX 137
instalando no Windows 138
opções de instalação 31
requisitos do sistema 136
requisitos para o Content Manager em caso de uso do namespace Series 7 135, 251

U

único signon
namespace do Active Directory 246
namespace LDAP 266
namespace SAP 273
UNIX
conexões ODBC com origens de dados 86
configurações de ulimit 5
iniciando e parando o serviço do Cognos 288
mensagens de log 205
variáveis de ambiente 60, 64, 83, 96
URI
definições de configuração padrão 7
URI de descoberta de colaboração
configurando 221
URIs
alterando 149, 151
URIs do Content Manager 78, 89
UTF-8
codificação para e-mails 217

V

validade do conteúdo
diretório de imagens 97
variáveis de ambiente
configurando para componentes de serviço de aplicativo 89
instalação no UNIX ou no Linux 60, 64, 83, 96
variável de ambiente ARBORPATH 88
variável de ambiente ESSBASEPATH 88
verificação de script cruzado
configurando no IBM Cognos Application Firewall 160
versão de endereço IP 219
virtualização
ambientes suportados 2

W

Windows 61