NOTA TÉCNICA CNMP/STI/BD Nº 01/2014

Em referência ao Processo CNMP 0.00.002.001071/2013-32

Brasília, 22 de Janeiro de 2014.

INTRODUÇÃO

Após análise das evidências documentadas na **Nota Técnica CNMP/STI/BD Nº 03/2013**, integrantes às folhas 347 a 384 deste processo, a equipe técnica identificou fato relevante e superveniente afeto à comprovação de atendimento ao item *10 - Critérios de Qualificação Técnica Exigidos para a Contratada* -, do Termo de Referência OLAP.

FUNDAMENTAÇÃO

Em síntese, licitante **Ewave do Brasil Informática Ltda**, em reunião do dia 26/12/13, fez uso da solução *"Audit Extension"* para atender aos requisitos técnicos dos itens **10.11.1.8, 10.13.5.8** e **10.13.5.14**, do Termo de Referência OLAP. Contudo, de acordo com o artefato *"Audit_Extension_Tool.pdf"* - extraído do sítio www.ibm.com/developerworks/br/data/library/cognos/development/utilities/page574.html e fornecido pela própria Ewave na citada reunião - concluiu-se que a solução é uma contribuição técnica – sem suporte técnico nem garantia de atualização - disponibilizada em um portal gratuito da IBM ("IBM developerWorks"), sendo este considerado um "sítio concentrador recursos técnicos para desenvolvedores, estudantes e profissionais de TI de todo o mundo".

Com vistas ao embasamento da questão, evidencia-se o seguinte excerto do arquivo "Audit_Extension_Tool.pdf" com grifos nossos.

> *(...)*
> *"Uso, suporte e feedback*
> *Recomenda-se que esse aplicativo seja usado como parte de um pacote de serviços IBM para garantir a implementação e interpretação bem-sucedida dos resultados.*
> ***O aplicativo e o modelo são fornecidos estritamente em uma base "no estado em que se encontra" e o IBM Cognos Support não pode oferecer suporte a eles**. Porém, quaisquer feedbacks, relatórios de erros e sugestões são bem-vindos.*
>
> *Detalhes do Aplicativo Arquitetura e visão geral do processo*
> ***O aplicativo é um aplicativo da web e um serviço da web escrito em Java/AXIS.** Ele deve ser instalado em uma máquina IBM Cognos 10 BI, sendo executada em uma instância do IBM Cognos 10 Tomcat ou seu próprio servidor de aplicativos."*
> *(...)*

Desta forma, infere-se:

1) A IBM - fabricante da solução IBM Cognos - disponibiliza o *"Audit Extension"* unicamente no estado como se encontra no sítio "IBM developerWorks". Por conseguinte, não há compromisso de manutenção evolutiva por parte da IBM.

2) O "IBM Cognos Support" declara que não pode oferecer suporte ao "Audit Extension". Consequentemente, as funcionalidades abrangidas por essa solução, apresentadas de forma a suprir parte dos requisitos do Termo de Referência OLAP, estão excluídas de um atendimento com as qualidades de serviço de suporte técnico por parte da fabricante da solução;

3) O *"Audit Extension"* oficialmente não faz parte do pacote IBM Cognos por se tratar de uma contribuição técnica, disponibilizada em um portal gratuito da IBM.

Conforme preceitua o Guia de Boas Práticas em Contratação de Soluções de Tecnologia da Informação – TCU – versão 1.0, *"uma solução de TI engloba todos os elementos necessários que se integram para o alcance dos resultados pretendidos com a contratação, de modo a atender à necessidade que a desencadeou"*. Diferentemente, observou-se que a proposta de solução OLAP apresentada - por si só - não atende integralmente aos requisitos previstos no item *"10. Critérios de Qualificação Técnica Exigidos para a Contratada"* do Termo de Referência OLAP e, mesmo quando a ferramenta "Audit Extension" é utilizada de forma a atender completamente às funcionalidades solicitadas, o atendimento aos requisitos técnicos deixa de ser cumprido pela ausência de cobertura integral de suporte técnico, bem como de atualizações evolutivas.

A fim de obter todos os benefícios da contratação, impende destacar que o suporte técnico e a atualização de versões – integrantes da solução OLAP - devem ser diretamente prestados pela fabricante da tecnologia de modo que correções e evoluções tecnológicas assegurem todos os requisitos técnicos previstos no Edital CNMP 54/2013.

CONCLUSÃO

Ante o exposto, as evidências para atendimento aos itens **10.11.1.8, 10.13.5.8** e **10.13.5.14** estão em desconformidade com as necessidades de negócio evidenciadas em edital. Com efeito, a empresa **não comprova** atendimento ao item *10-Critérios de Qualificação Técnica Exigidos para a Contratada*, do Termo de Referência OLAP.

Dessa forma, solicita-se acolher as razões contidas nesta Nota Técnica, bem como comunicar a licitante interessada acerca do atual entendimento do CNMP, garantindo-lhe o exercício do direito ao contraditório e à ampla defesa, em consonância com os prazos fixados na legislação em vigor e aplicáveis ao caso sob análise, bem como com o disposto no Edital regulatório do certame.

Elaborado por:

Helvecio Silva de Faria Junior
Matricula 24029

Erick Lamartine Leão Joca
Matricula 16371

De acordo:

Waldeck Pinto de Araújo Junior
Secretário de Tecnologia da Informação

Práticas comprovadas do IBM Cognos: Audit Extension do IBM Cognos 10

Natureza do Documento: Prática Comprovada, Produto(s): IBM Cognos 10 BI, Área de Interesse: Segurança, Infraestrutura e Desenvolvimento

Equipe de Práticas Comprovadas do Business Analytics, Business Analytics Proven Practices Team, IBM

Resumo: Um aplicativo do IBM Cognos 10 SDK que fornece auditoria adicional, incluindo a Auditoria de Função, para o IBM Cognos 10 BI. A versão do aplicativo é 1.1.01 e funcionará com as versões 10.1 e posteriores do IBM Cognos 10 BI.

Data: 08/Jul/2013
Nível: Intermediário
Também disponível em : Inglês
Atividade: 287 visualizações
Comentários: 0 (Visualizar | Incluir comentário - Conectar)

Introdução

Propósito

Os recursos de auditoria padrão fornecidos prontos para uso com o IBM Cognos 10 BI abrangem muitos aspectos da operação. Porém, algumas áreas como a auditoria de usuários e as designações de recursos não estão incluídas. O objetivo do aplicativo c10AuditExtension é fornecer a auditoria adicional para essas áreas.

Auditoria de Conta

Uma auditoria de todas as contas de usuário que são encontradas em todos os namespaces configurados e determinadas propriedades dessas contas (detalhes básicos, páginas de portal, datas de criação e modificação, etc.). Isso permite o relatório sobre a base de usuários do IBM Cognos e fornece informações adicionais para acompanhar a auditoria de função/recursos.Esse tipo de auditoria também irá, por padrão, registrar o conteúdo de My Folder dos usuários.

Auditoria de Conteúdo

Uma auditoria de todos os objetos que existem no Content Store principal. Essa auditoria processará a árvore do Content Store e registrará todos os objetos (pastas, relatórios, consultas,etc.) que localizar. Ela irá registrar as informações básicas (como nome, caminho da procura, permissões de objeto, data de criação e de modificação), assim como alguns detalhes mais específicos dos tipos de item (como a especificação XML dos relatórios e consultas, quaisquer valores de parâmetro salvos aplicados aos relatórios salvos e detalhes sobre versões de saída do relatório).

Para também registrar os itens no Content Store que estão localizados dentro de áreas My Folders de usuários individuais, esse tipo de auditoria deve ser uado em conjunto com a Auditoria de Conta (veja acima).

Auditoria de Status

Uma auditoria do estado atual de um servidor e os dispatchers relacionados. Para cada dispatcher registrado no sistema de destino, a configuração e a atividade serão registradas, salvando informações como tempo gasto para se conectar, número de processos ativos e a duração da solicitação.

Auditoria de Função/Recurso

Uma auditoria de todos os recursos (como autoria de relatório) configurada no namespace Cognos e a quais funções, grupos e usuários foi designado o acesso a esses recursos. Onde uma função ou grupo tiver o acesso designado, a auditoria irá registrar todos os usuários individuais que compõem a função ou grupo, para que seja possível determinar de forma precisa que usuários individuais têm acesso a um determinado recurso.

Usage

O aplicativo é gerenciado através de uma interface inicial da web que permite a configuração das informações de namespace e do servidor e pode ser usado para ativar ou desativar tipos de auditoria individuais para um determinado servidor.

As auditorias podem ser iniciadas de três formas:

- através da interface da web de gerenciamento
- através de uma chamada de formulário da web/URL simples
- através da chamada de um serviço da web (isto é, do Event Studio)

Os resultados de cada auditoria são registrados em um banco de dados e um modelo do IBM Cognos Framework Manager é fornecido para ajudar a relatar os dados.

Aplicabilidade

Esse aplicativo foi projetado para o IBM Cognos BI versão 10.1.

Ele também se destina a interagir com qualquer aplicativo de terceiros que possa emitir comandos através dos serviços da web.

Exclusões e Exceções

Esse aplicativo pode não ser compatível com todos os Provedores de Autenticação Customizada, dependendo da implementação do provedor, por exemplo, ele geralmente espera que o provedor/namespace requeira um nome de usuário e senha simples para efetuar o logon, em que o provedor customizado usa alguma outra forma de credencial, a extensão de auditoria pode não ser capaz de realizar a autenticação para tal namespace para realizar a auditoria. Isso não afeta os provedores customizados de tipo de conexão confiável, desde que o provedor subjacente possa ser autenticado da maneira normal.

Esse aplicativo é conhecido por trabalhar com os seguintes bancos de dados:

- DB2 9.x e 10.x
- MS SQL Server 2000, 2005 e 2008
- Oracle 10g & 11g
- MySQL 5
- Apache Derby 10

A Auditoria de Status depende de algumas informações fornecidas pelo servidor IBM Cognos 10 BI que estão sujeitas a alterações e podem ser afetadas pelas atualizações futuras do IBM Cognos 10 BI.

Esse aplicativo funcionará apenas em um JRE versão 1.5 ou superior.

Uso, suporte e feedback

Recomenda-se que esse aplicativo seja usado como parte de um pacote de serviços IBM para garantir a implementação e interpretação bem-sucedida dos resultados.

O aplicativo e o modelo são fornecidos estritamente em uma base "no estado em que se encontra" e o IBM Cognos Support não pode oferecer suporte a eles.Porém, quaisquer feedbacks, relatórios de erros e sugestões são bem-vindos.

Detalhes do Aplicativo

Arquitetura e visão geral do processo

O aplicativo é um aplicativo da web e um serviço da web escrito em Java/AXIS. Ele deve ser instalado em uma máquina IBM Cognos 10 BI, sendo executada em uma instância do IBM Cognos 10 Tomcat ou seu próprio servidor de aplicativos.

Após a instalação, o aplicativo criará suas próprias tabelas de bancos de dados se elas ainda não existirem e apresentará uma interface para permitir que o administrador insira os detalhes dos namespaces e servidores do IBM Cognos 10 BI. Geralmente, apenas uma entrada de servidor deve ser usada para cada grupo de servidores IBM Cognos 10 BI que use o mesmo Content Store. Porém, entradas de servidor separadas são frequentemente usadas para diferentes grupos funcionais, como Produção e Desenvolvimento.

O aplicativo pode ser protegido a partir da interface de gerenciamento ao definir uma senha local que subsequentemente será necessária para acessar a interface ou executar auditorias. O motivo de usar uma senha local em vez de vincular à segurança do IBM Cognos 10 é que o aplicativo pode interagir com várias instalações do IBM Cognos 10 BI, então não há um namespace de segurança do IBM Cognos 10 BI ao qual vinculá-la.

Quando o administrador insere os detalhes de um novo Dispatcher do IBM Cognos 10 BI, o aplicativo irá se conectar a ele e reunir os detalhes dos namespaces de segurança configurados.Esses detalhes serão adicionados à página de propriedades desse Dispatcher e estará pronta para edição.É essencial que exista uma entrada, preenchida com os detalhes de login válidos, para cada namespace que é usado para a segurança de objeto ou designação de recurso no Content Store para que possam ser auditados. Isso ocorre em virtude de o aplicativo precisar ser capaz de realizar a autenticação no namespace para auditar seu conteúdo. Se o aplicativo não puder realizar a autenticação de um namespace que seja usado para usuários ou segurança de objeto, seus objetos não poderão ser auditados. Se vários namespaces forem especificados em uma única entrada de servidor, a autenticação de todos os namespaces deve ser realizada, caso contrário o aplicativo finalizará a execução da auditoria.

Os detalhes de login de namespace serão criptografados e armazenados no banco de dados de aplicativos.

Installation

O aplicativo é implementado como um arquivo WAR (Archive web) que pode ser usado com qualquer contêiner do servlet adequado, como Tomcat ou servidor de aplicativos, como o IBM WebSphere. Primeiro é necessário criar o arquivo WAR em sua instalação do IBM Cognos 10 BI usando os scripts fornecidos e, então, implementar o arquivo WAR em seu servidor.

O procedimento descrito nesse documento abrange a implementação do aplicativo no contêiner do servlet Tomcat que normalmente é instalado com um servidor IBM Cognos 10 BI. Consulte a documentação do contêiner de servlet/servidor de aplicativo específico para obter instruções sobre a implementação do arquivo WAR em destinos alternativos.

Falando de forma geral, é desejável que um ambiente de produção execute esse aplicativo em sua própria instância do Tomcat ou IBM WebSphere. Consulte a documentação do Tomcat, IBM WebSphere ou outro servidor de aplicativos para encontrar detalhes sobre como implementar um aplicativo da web.

O processo de instalação ocorre da seguinte forma:

- Descompacte a instalação em um servidor IBM Cognos 10 BI
- Customize quaisquer arquivos que deseja modificar
- Importe quaisquer drivers JDBC de terceiros que pretende usar
- Crie o arquivo WAR
- Implemente o arquivo WAR em um contêiner do servlet ou servidor de aplicativos
- Configure o aplicativo usando a interface com o usuário da web

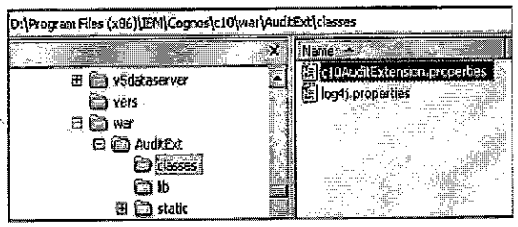
Descompacte a instalação e copie para um servidor IBM Cognos 10 BI

Descompacte o arquivo ZIP contendo o aplicativo Audit Extension para um local temporário adequado. Haverá duas pastas principais,

reporting
Essa pasta contém os materiais para permitir que você crie relatórios na saída do Audit Extension com o IBM Cognos 10 BI. Ela contém um modelo do IBM Cognos Framework Manager e um arquivo de implementação do IBM Cognos 10 BI. Não é necessário fazer nada com ela nesse estágio.

war
Essa pasta contém o aplicativo em si, em um subdiretório chamado AuditExt. É necessário usá-la para criar o arquivo WAR.

Na pasta war, copie o diretório AuditExt e seus subdiretórios para o diretório de instalação do IBM Cognos 10 no diretório <c10install>/war. Nesse momento, é possível customizar o aplicativo antes de criar o arquivo WAR. As configurações padrão devem ser boas na maioria dos casos, mas caso seja necessário fazer alguma alteração nas definições de configuração no arquivo c10AuditExtension.properties (consulte a seção 3.7) ou nas configurações de login no arquivolog4j.properties (consulte a seção 6.1), os arquivos estão localizados no diretório <c10install>/war/AuditExt/classes.



Instale todos os drivers JDBC necessários

Caso esteja usando um banco de dados IBM DB2 ou Apache Derby para armazenar os dados do Audit Extension, não será necessário instalar nenhum driver JDBC adicional, uma vez que o DB2 Universal Driver está incluso na distribuição (o arquivo de licença do DB2 ainda precisará ser fornecido). Caso planeje usar o Microsoft SQL Server, MySQL ou Oracle, será necessário obter o arquivo do driver correto e instalá-lo.

- O arquivo do driver do SQL Server é o sqljdbc4.jar.
- O arquivo do driver do Oracle é o ojdbc5.jar. Também pode ser necessário obter o orai18n.jar caso esteja usando um código de idioma que não seja inglês.
- O arquivo do driver do MySQL driver é o mysql-connector-java-5.1.6-bin.jar.

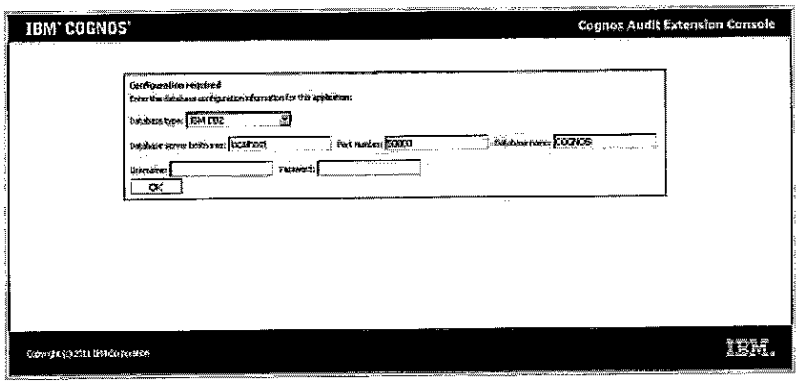
Após obter o(s) arquivo(s) de licença e/ou JAR corretos para seu banco de dados, coloque-os no diretório <c10install>/war/AuditExt/lib. Caso não instale o driver correto nesse estágio, o aplicativo irá alertá-lo ao tentar configurar o banco de dados pela primeira vez.

Desenvolva e implemente o arquivo WAR

Crie o arquivo WAR executando o script <c10install>/war/AuditExt/build.bat (Windows) ou o <c10install>/war/AuditExt/build.sh (UNIX/Linux). Isso criará o arquivo WAR <c10install>/war/AuditExt/AuditExt.war. Coloque esse arquivo no diretório <c10install>/webapps. Após um breve período, o servidor IBM Cognos 10 Tomcat irá descompactar o arquivo WAR automaticamente. Agora o aplicativo está pronto para ser configurado.

Configure via UI

Acesse a URL de administração da web em http://servername:9300/AuditExt/. Uma tela solicitando os detalhes de conexão com o banco de dados será exibida. A solicitação inclui o tipo de banco de dados, o número da porta e o nome do servidor do banco de dados do host, o nome do banco de dados e o id de usuário/senha usados para se conectar ao banco de dados.



O aplicativo c10AuditExtension pode usar um banco de dados de auditoria do IBM Cognos 10 BI existente ou um banco de dados separado criado

especificamente para esse aplicativo. É altamente recomendado não usar um banco de dados que já esteja sendo usado por um IBM Cognos 10 Content Store.

IMPORTANTE: O banco de dados especificado no campo **Database name** já deve existir antes da conexão. O aplicativo criará as tabelas necessárias nesse banco de dados.

O processo de criar e preencher as tabelas de banco de dados pode ser um pouco demorado, dependendo da velocidade do servidor. Após clicar em OK, espere que a tela seja atualizada antes e continuar. Não clique em OK mais de uma vez.

Preparação do banco de dados

Para preparar o banco de dados para ser usado por esse aplicativo, é necessário configurá-lo da mesma forma descrita no Guia de instalação e configuração do IBM Cognos 10 como se ele estivesse sendo usado para um Content Store. Também é possível usar um banco de dados de criação de log de auditoria do IBM Cognos 10 BI padrão, que também deve ter sido configurado dessa forma.

IMPORTANTE: Para o IBM DB2, é necessário criar um espaço de tabela de usuário regular adicional com um tamanho de página de 16 KB. Caso esteja usando um banco de dados que já foi configurado para a criação de log de auditoria do IBM Cognos 10 BI, talvez isso já tenha sido feito.

IMPORTANTE: Para o Oracle pode ser necessário aumentar o número máximo de cursores abertos suportados pelo bando de dados. O padrão é 50, que provavelmente será insuficiente para esse aplicativo. Um valor mais adequado seria 500. Para obter mais informações, consulte http://www.orafaq.com/node/758 .

Reconfiguração

Para reconfigurar a conexão com o banco de dados principal, clique no link Reset configuration na página Manage Servers. Isso permite a reinserção dos detalhes de conexão com o banco de dados. De maneira alternativa, a conexão com o banco de dados principal pode ser reconfigurada manualmente através das seguintes etapas:

- Pare o serviço do IBM Cognos 10 BI
- Edite o arquivo <c10install>/webapps/AuditExt/WEB-INF/classes/c10AuditExtension.properties
- Reconfigure os detalhes de conexão do JDBC da seguinte forma:

```
# JDBC connection details:
jdbc.url=
jdbc.user=
jdbc.password=
```

- Reinicie o IBM Cognos 10 BI

Quando o IBM Cognos 10 BI for reiniciado e a URL de administração for acessada novamente, a tela solicitando os detalhes da conexão JDBC será exibida.

Referência do arquivo de configuração

O arquivo de configuração principal é chamado c10AuditExtension.properties e pode ser encontrado em <c10install>/webapps/AuditExt/WEB-INF/classes. Esse arquivo de configuração contém os seguintes parâmetros:

jdbc.url
jdbc.user
jdbc.password
Detalhes de conexão com o banco de dados usados pelo aplicativo Audit Extension. Eles são gerados pela interface de configuração do aplicativo e não devem ser editados manualmente, exceto para redefinir os valores vazios para reconfiguração. Observe que a senha é armazenada em um formato criptografado.

option.ra.recurse.everyone
Uma opção de Auditoria de Função que determina se a auditoria deve realizar uma recursão integral do(s) namespace(s) quando o grupo Everyone é encontrado em um recurso ou associação. Isso fará com que os usuários que têm acesso através de Everyone sejam explicitamente auditados, mas aumentará o espaço de banco de dados e tempo de processamento necessários. Os valores possíveis são verdadeiro e falso. O valor padrão é falso.

option.ra.recurse.auth
Uma opção de Auditoria de Função que especifica se a auditoria deve realizar uma recursão integral do(s) namespace(s) quando o grupo Authenticated Users é encontrado em um recurso ou associação. Isso fará com que os usuários que têm acesso através de Authenticated Users sejam explicitamente auditados, mas aumentará o espaço de banco de dados e tempo de processamento necessários. Os valores possíveis são verdadeiro e falso. O valor padrão é verdadeiro.

option.ra.recurse.anon
Uma opção de Auditoria de Função que determina se a auditoria deve realizar uma recursão integral do(s) namespace(s) quando o grupo Anonymous Users é encontrado em um recurso ou associação. Isso fará com que os usuários que têm acesso através de Anonymous Users sejam explicitamente auditados, mas aumentará o espaço de banco de dados e tempo de processamento necessários. Os valores possíveis são verdadeiro e falso. O valor padrão é falso.

option.ra.max.items
Uma opção de Auditoria de Função que limita o número máximo de itens que será processado pela auditoria. Se o número for excedido, a auditoria é finalizada e registrada como uma falha. Se ele for configurado para um valor zero, nenhum limite será aplicado. O valor padrão é 20000.

option.ra.max.duration
Uma opção de Auditoria de Função que limita o período de tempo máximo, em segundos, pelo qual a auditoria deve ser executada. Se esse período for excedido, a auditoria é finalizada e registrada como uma falha. Se ele for configurado para um valor zero, nenhum limite de tempo será aplicado. O valor padrão é 900 (15 minutos).

option.ca.include.specifications
Uma opção de Auditoria de Conteúdo que determina se a auditoria deve registrar o XML de especificação de quaisquer relatórios/consultas/análises que ela localizar. Os valores possíveis são verdadeiro e falso. O valor padrão é verdadeiro. Se esse parâmetro for definido como falso, será usado menos espaço de banco de dados.

option.ca.include.output
Uma opção de Auditoria de Conteúdo que determina se a auditoria deve registrar detalhes de versões de relatório e saídas para objetos de relatório que ela encontrar. Os valores possíveis são verdadeiro e falso. O valor padrão é verdadeiro. Se esse parâmetro for definido como falso, será usado menos espaço de banco de dados e a auditoria pode ser executada mais rápido.

option.ca.max.items
Uma opção de Auditoria de Conteúdo que limita o número máximo de itens que será processado pela auditoria. Se o número for excedido, a auditoria é finalizada e registrada como uma falha. O valor padrão é 0 (zero), o que significa que nenhum limite será aplicado.

option.ca.max.duration
Uma opção de Auditoria de Conteúdo que limita o período de tempo máximo, em segundos, pelo qual a auditoria deve ser executada. Se esse período for excedido, a auditoria é finalizada e registrada como uma falha. Se ele for definido como 0 (zero), nenhum limite de tempo será aplicado. O valor padrão é 900 (15 minutos).

option.ca.policy.calculation
Uma opção de Auditoria de Conteúdo que determina se o cálculo de política de segurança deve ser feito no FM. Os valores possíveis são verdadeiro e falso. Se for configurado para falso, o cálculo será realizado no tempo de execução. O valor padrão é verdadeiro, significando que não haverá cálculos sendo feitos no tempo de execução.

option.aa.flatsearch
Uma opção de Auditoria de Conta que altera o método de varredura do namespace da abordagem recursiva padrão para uma procura simples. Essa opção pode ser usada para namespaces muito grandes. Se essa opção for configurada, em vez de processar recursivamente todo o namespace, o aplicativo executará uma procura simples apenas de usuários que fizeram o login anteriormente no IBM Cognos 10 BI e registrará apenas esses usuários. Os usuários que existirem no namespace de origem, mas nunca tiverem efetuado o login serão ignorados. Essa abordagem pode melhorar muito os tempos de processamento em casos em que o namespace de origem é grande, mas apenas uma pequena fração de seus membros é composta por usuários do Cognos 10 BI. O valor padrão é falso, significando que uma procura recursiva tradicional de todos os usuários será realizada.

option.aa.max.items
Uma opção de Auditoria de Conta que limita o número máximo de itens que será processado pela auditoria. Se o número for excedido, a auditoria é finalizada e registrada como uma falha. Se ele for configurado para um valor zero, nenhum limite será aplicado. O valor padrão é 10000.

option.aa.max.duration
Uma opção de Auditoria de Conta que limita o período de tempo máximo, em segundos, pelo qual a auditoria deve ser executada. Se esse período for excedido, a auditoria é finalizada e registrada como uma falha. Se ele for definido como 0 (zero), nenhum limite de tempo será aplicado. O valor padrão é 900 (15 minutos).

option.aa.include.content
Uma opção de Auditoria de Conta que determina se a auditoria deve processar o conteúdo de My Folders dos usuários. Se configurado, isso fará com que uma mini Auditoria de Conteúdo seja executada para o conteúdo de cada usuário onde ele existir. Os valores possíveis são verdadeiro e falso. O valor padrão é verdadeiro.

option.sa.include.configuration
Uma opção de Auditoria de Status que determina se a auditoria deve registrar as informações de configuração dos dispatchers. Ela inclui informações como o número máximo de processos. Os valores possíveis são verdadeiro e falso. O valor padrão é verdadeiro. Se esse parâmetro for definido como falso, será usado menos espaço de banco de dados.

option.sa.include.rawstatus
Uma opção de Auditoria de Status que especifica se a auditoria deve registrar o XML status não processado dos serviços que a auditoria localizar. Os valores possíveis são verdadeiro e falso. O valor padrão é verdadeiro. Se esse parâmetro for definido como falso, será usado menos espaço de banco de dados.

option.sa.include.ping
Uma opção de Auditoria de Status que especifica se a auditoria deve executar testes de rede básicos adicionais nos dispatchers registrados em um servidor. Os valores possíveis são verdadeiro e falso. O valor padrão é verdadeiro.

security.keystore.filename
O local do arquivo keystore que é usado para segurança. Se o arquivo não existir nesse local, um novo será gerado. Observe que esse deve ser um local gravável, caso contrário o aplicativo falhará. O valor padrão colocará o keystone no diretório ./configuration da instalação do IBM Cognos 10 BI usando um caminho de arquivo relativo. Se esse aplicativo foi implementado em outro lugar que não o contêiner do servlet Tomcat que foi instalado com o IBM Cognos 10 BI, esse valor precisará ser editado.

option.db.setdefault.audittypes
Uma opção de banco de dados que determina se o aplicativo deve reconfigurar as descrições de tipo de auditoria no banco de dados para seus valores padrão caso eles tenham mudado. Os valores possíveis são verdadeiro e falso. O valor padrão é falso.

option.db.setdefault.statusresulttypes
Uma opção de banco de dados que determina se o aplicativo deve reconfigurar as descrições de tipo de resultado de status no banco de dados para seus valores padrão caso eles tenham mudado. Os valores possíveis são verdadeiro e falso. O valor padrão é falso.

option.db.setdefault.serverversiondesc
Uma opção de banco de dados que determina se o aplicativo deve reconfigurar as descrições de versão do servidor no banco de dados para seus valores padrão caso eles tenham mudado. Os valores possíveis são verdadeiro e falso. O valor padrão é falso.

option.db.setdefault.pingtype
Uma opção de banco de dados que determina se o aplicativo deve reconfigurar as descrições de tipo de teste de ping no banco de dados para seus valores padrão caso eles tenham mudado. Os valores possíveis são verdadeiro e falso. O valor padrão é falso.

option.db.setdefault.pingresult
Uma opção de banco de dados que determina se o aplicativo deve reconfigurar as descrições de resultado de teste de ping no banco de dados para seus valores padrão caso eles tenham mudado. Os valores possíveis são verdadeiro e falso. O valor padrão é falso.

option.db.dimension.time.populate
Uma opção de banco de dados que determina se o aplicativo deve preencher totalmente a tabela de dimensão de tempo quando ela for criada na primeira inicialização. Observe que quaisquer tempos ausentes serão adicionados quando a auditoria para eles for executada, então o pré-preenchimento não é necessário, embora seja considerado melhor para fins de relatório. Os valores possíveis são verdadeiro e falso. O valor padrão é verdadeiro.

option.db.dimension.date.initdays
Uma opção de banco de banco de dados que especifica o número de dias (a partir da data atual) para preencher previamente a tabela de dimensão de data quando ela é criada na primeira inicialização. Observe que quaisquer datas ausentes serão adicionadas quando a auditoria para elas for executada, então o pré-preenchimento integral não é necessário, embora seja considerado melhor para fins de relatório. O valor padrão é 730 (2 anos).

option.db.maxbatch
Uma opção que especifica o número máximo de itens que devem ser processados antes de um banco de dados ser gravado. Ela se aplica a todos os tipos de auditoria e foi projetado para reduzir o consumo de memória geral para auditorias muito grandes. O valor padrão é 2000.

option.db.random-audit-id
Uma opção que controla se o ID do banco de dados gerado para cada auditoria deve ser um número pseudoaleatório (um valor de verdadeiro) ou sequencial (um valor de falso). O valor padrão é falso.

Considerações sobre a implementação em outro servidor de aplicativos

Conforme observado acima, se instalado em um ambiente de produção bastante usado, deve-se considerar a instalação em outro contêiner do servlet. Ele pode ser uma instância Tomcat independente (http://tomcat.apache.org/download-55.cgi) ou um servidor de aplicativos integral como o IBM WebSphere Application Server.

Geralmente, o procedimento é tão simples quanto implementar qualquer aplicativo da web, no caso do Tomcat, é possível apenas colocar o arquivo WAR no diretório de aplicativos da web da mesma forma que seria feito com o IBM Cognos 10 BI. Entretanto, há duas considerações a serem feitas sobre o caminho do arquivo,

1. Em WEB-INF/classes/log4j.properties, o nome do arquivo de log é especificado usando um caminho relativo, ../logs/c10AuditExtension.log. Embora isso funcione com o IBM Cognos 10, pode ser necessário alterá-lo para um caminho relativo diferente ou um caminho completo como C:/logs/c10AuditExtension.log.
2. O arquivo WEB-INF/classes/lc10AuditExtension.properties contém um caminho relativo na propriedade security.keystore.filename(../configuration/c10AuditExtension.keystore). Verifique se esse caminho funciona em seu ambiente e, caso seja necessário, atualize-o. Lembre-se de usar barras para o nome do caminho.

Outra configuração alternativa é instalar em uma instalação dedicada do IBM Cognos 10 BI. Como o Audit Extension pode se comunicar com vários servidores IBM Cognos 10 BI e não apenas com o servidor em que está instalado, é possível ter uma instância dedicada do IBM Cognos 10 BI para executar essa auditoria e relatá-lo. Verifique seu licenciamento para determinar se essa é uma alternativa viável.

Remoção e reinstalação

Para desinstalar o aplicativo, pare o IBM Cognos 10 BI e exclua os seguintes itens:

- o arquivo <c10install>/webapps/AuditExt.war
- o diretório <c10install>/webapps/AuditExt

Opcionalmente, o arquivo keystore também pode ser excluído. Por padrão, o arquivo keystore está localizado em<c10install>/configuration/c10AuditExtension.keystore, mas esse local será diferente se o aplicativo tiver sido implementado fora do contêiner do servlet Tomcat instalado com o IBM Cognos 10 BI.

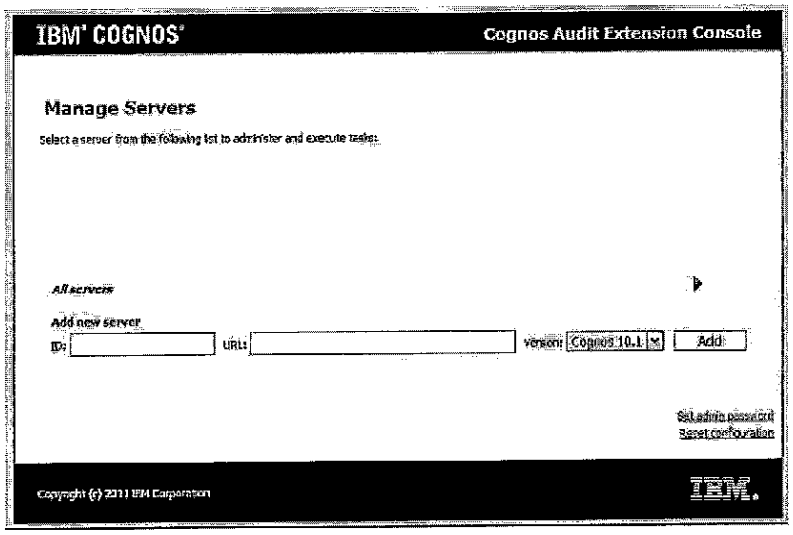
IMPORTANTE: Se o arquivo keystore for excluído ou o aplicativo for instalado em outra máquina sem copiar o arquivo keystore para a nova máquina, não será mais possível acessar as senhas salvas e podem ocorrer erros ao executar e administrar auditorias.

Opcionalmente, as tabelas de banco de dados criadas pelo aplicativo podem ser excluídas. As tabelas de bancos de dados recebem o prefixo "AE_".

Usando o Aplicativo

Manage servers

Após o aplicativo ser configurado, a interface principal é a página Manage Servers, que é acessada através de http://servername:9300/AuditExt/. A página Manage Servers inicial não conterá servidores.



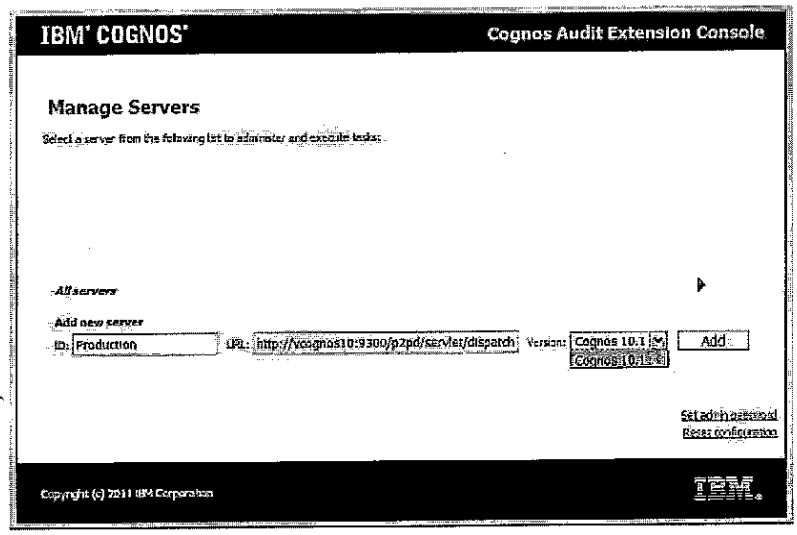
Adicionar um servidor

A partir da página Manage Servers, adicione uma nova entrada de servidor ao preencher os campos abaixo do rótulo Add new server e clicar no botão Add. Os campos a serem preenchidos são:

ID: Um identificador de texto para o servidor IBM Cognos 10 BI a ser auditado. Pode ser um nome do host ou um identificador simples, como "Production". Como o valor desse identificador pode ser usado para se referir ao servidor para comandos, sugere-se que esse valor seja uma cadeia de caracteres curta e simples, apenas com os caracteres padrão.

URL: A URL que o aplicativo irá usar para se conectar ao servidor IBM Cognos 10 BI a ser auditado. Essa URL pode ser diretamente para um dispatcher do IBM Cognos 10 BI ou para um gateway dedicado para os aplicativos do IBM Cognos 10 SDK.

Version: A partir da lista suspensa, selecione a versão do IBM Cognos 10 BI que está sendo executada no servidor a ser auditado.



Assim que um novo servidor for adicionado com sucesso, a página **Edit Server** que contém as diversas propriedades que se aplicam ao servidor IBM Cognos 10 BI recém-adicionado será automaticamente exibida. Há vários campos nessa página e eles são agrupados em três seções, a seção **Set properties** , a seção **Saved namespace logins** e a seção **Add new namespace login** .

Set properties

URL: A URL do servidor IBM Cognos 10 BI a ser auditado.

Version: A versão do servidor IBM Cognos 10 BI atrás da URL especificada.

Description: Uma descrição opcional geralmente usada para descrever a auditoria que ocorrerá no servidor IBM Cognos 10 BI atrás da URL especificada.

Filter (Content Audit): Um campo de texto usado para definir um filtro que será usado em uma Auditoria de Conteúdo. O filtro da Auditoria de Conteúdo será descrita em breve.

Filter (Account Audit): Um campo de texto usado para definir um filtro que será usado em uma Auditoria de Conta. O filtro de Auditoria de Conta será descrito em breve.

Role audit active: Quando marcado, a Auditoria de Função será executada. Esse item é marcado por padrão.

Content audit active: Quando marcado, a Auditoria de Conteúdo será executada. Esse item é marcado por padrão.

Account audit active: Quando marcado, a Auditoria de Conta será executada. Esse item é marcado por padrão.

Status audit active: Quando marcado, a Auditoria de Status será executada. Esse item é marcado por padrão.

Saved namespace logins :

User: O ID do usuário para o namespace de segurança associado que será usado pelo aplicativo para efetuar o logon no servidor IBM Cognos 10 BI sendo auditado.

A senha: A senha associada ao ID do usuário.

Password (verify): Para verificar o valor no campo Password.

Ícone Save: Salva as informações de login para o namespace associado.

Ícone Delete Login: Exclui as informações de login para o namespace associado.

Add new namespace login :

Namespace ID: O ID do namespace de segurança com o qual efetuar o login. Ele precisa ser o mesmo valor contido no campo NameSpace ID da definição de namespace de segurança na configuração do IBM Cognos Configuration.

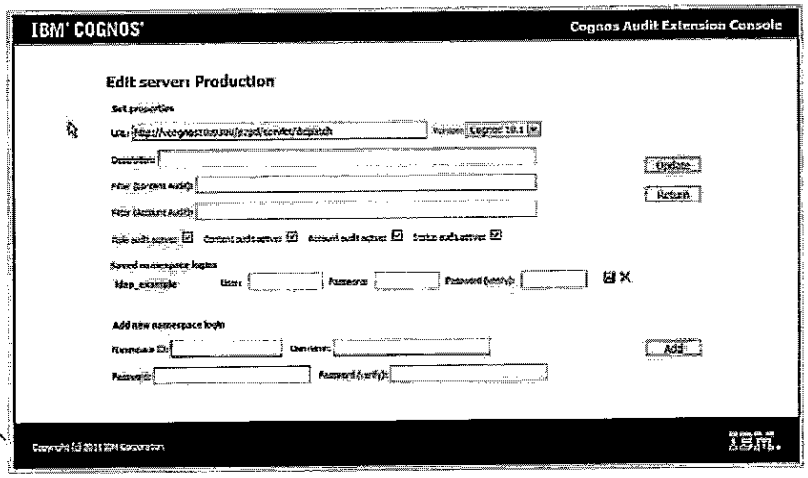
Nome de usuário: O ID do usuário para o namespace de segurança especificado que será usado pelo aplicativo para efetuar o logon no servidor IBM Cognos 10 BI sendo auditado.

A senha: A senha associada ao ID do usuário.

Password (verify): Para verificar o valor no campo Password.

Botão Add: Adiciona as informações de login para esse namespace à seção **Saved namespace logins** .

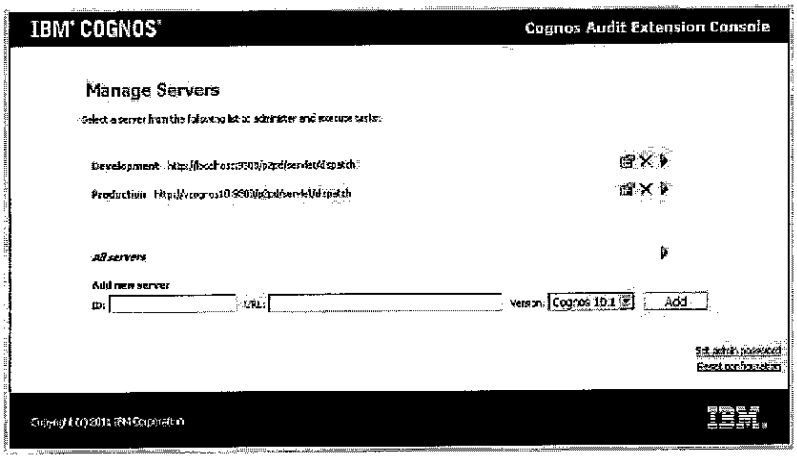
Clique no botão Update para salvar as alterações, clique no botão Return para retornar à página Manage Servers.



Quando um novo servidor for adicionado, todos os namespaces que foram configurados no servidor IBM Cognos 10 BI para serem auditados serão automaticamente adicionados à página de propriedades sem IDs de usuário e senhas.

OBSERVAÇÃO: Caso esteja usando esse aplicativo em um ambiente de teste ou desenvolvimento e o acesso Anônimo tiver sido ativado na instância do IBM Cognos 10 BI, os namespaces configurados não serão exibidos automaticamente. Os namespaces configurados podem ser incluídos manualmente ao preencher os campos na seção **Add new namespace login** .

Quando um novo servidor é incluído, a página Manage Servers irá conter uma lista de todos os servidores que podem ser auditados por esse aplicativo.



Excluir um servidor

É possível excluir um servidor a partir da página Manage Servers. Para excluir um servidor, clique no ícone **Delete Server** próximo à entrada do servidor. Será exibida uma página solicitando ao usuário para confirmar ou cancelar a exclusão. Se for confirmada, a tela Manage Servers será reexibida com o servidor excluído removido da lista.

Gerenciar os namespaces de servidor

É possível gerenciar os namespaces de cada servidor a partir da página de propriedades do servidor especificado. Se um novo servidor acaba de ser adicionado, a página de propriedades será exibida automaticamente. Para acessar e editar a página de propriedades de qualquer servidor exibido na lista da página Manage Servers, clique no ícone **Set Properties** ao lado do servidor de destino e a página Edit Servers será exibida. Os campos na página Edit Servers foram descritos anteriormente na seção chamada **Adicionar um servidor**.

Antes de um namespace poder ser incluído em uma auditoria, as credenciais de login que o aplicativo deve usar devem ser fornecidas. Insira os nomes de usuário e senhas de um namespace de cada vez clicando no ícone **Salvar** próximo à entrada de tal namespace um após o outro. Caso seja feita uma tentativa de salvar várias credenciais de namespace simultaneamente, apenas as credenciais que correspondem ao ícone Save que foi clicado serão salvas. Observe que os namespaces salvos exibirão o usuário salvo, mas nunca exibirão a senha salva.

Para quaisquer namespaces indesejados ou não usados, eles devem ser excluídos ao clicar o ícone **Delete Login** . Se eles não forem excluídos, o aplicativo irá tentar efetuar o login no namespace e a auditoria pode falhar, caso não consiga efetuá-lo. Um exemplo de tal namespace é um que é usado apenas para a conexão única.

Para adicionar um novo namespace, insira os detalhes na seção chamada **Add new namespace login** na parte inferior da tela. Os campos dessa seção foram descritos anteriormente na seção chamada **Adicionar um servidor**.

Quando concluir as ações na página de propriedades do servidor, clique no botão Return para voltar à página Manage Servers.

Configurar as propriedades do servidor e tipos de auditoria

Como mencionado anteriormente, é possível configurar propriedades adicionais para o servidor na página Manage Servers. As propriedades que podem ser configuradas são:

- Atualizar a URL do dispatcher
- Adicionar ou modificar uma descrição para o servidor
- Configurar que tipos de auditoria devem ser executados para esse servidor
- Aplicar filtros às auditorias

Configurar filtros de auditoria

Para auditorias de Conta e Conteúdo, é possível especificar um filtro para limitar o escopo da auditoria a uma subseção do namespace ou do Content Store. Esses filtros são especificados em um dos campos de filtro da página Edit Server. Se nenhum filtro for ser aplicado (o padrão), deixe os valores de filtro vazios.

Um filtro assume a forma de várias expressões regulares, separadas por barras para simbolizar as pastas. O uso é um pouco diferente dependendo de se tratar de uma auditoria de conteúdo ou conta. É possível encontrar mais informações sobre as expressões regulares em http://www.regular-expressions.info/ .

Filtro de auditoria de conta

Assume-se que o filtro deve ser iniciado no nível do namespace, então o primeiro item no filtro irá se referir ao namespace. Por exemplo, para restringir a auditoria a membros da pasta Users na pasta Accounts para todos os namespaces configurados, o filtro deve ser:

```
*/Accounts/Users
```

O asterisco no primeiro item indica que todos os namespaces serão correspondidos. De maneira alternativa, para restringir a auditoria ao mesmo conjunto de pastas, mas também restringir apenas ao namespace com ID "ADNamespace", o filtro deve ser:

```
ADNamespace/Accounts/Users
```

O filtro a seguir seria um pouco menos restritivo e selecionaria todos os itens em Accounts para todos os namespaces:

```
*/Accounts
```

É possível usar qualquer expressão regular. Porém, é importante lembrar que o caractere '/' é um caso especial e será tratado como um separador de pastas.

Auditoria de conteúdo

Assume-se que o filtro deve iniciar no nível de conteúdo (pacote) superior. Por exemplo, o filtro a seguir restringiria o conteúdo a tudo no pacote "GO Sales and Retailers":

```
GO Sales and Retailers
```

Para restringi-lo ainda mais para a pasta "Report Studio Report Samples" nesse pacote, o filtro deveria ser:

```
GO Sales and Retailers/Report Studio Report Samples
```

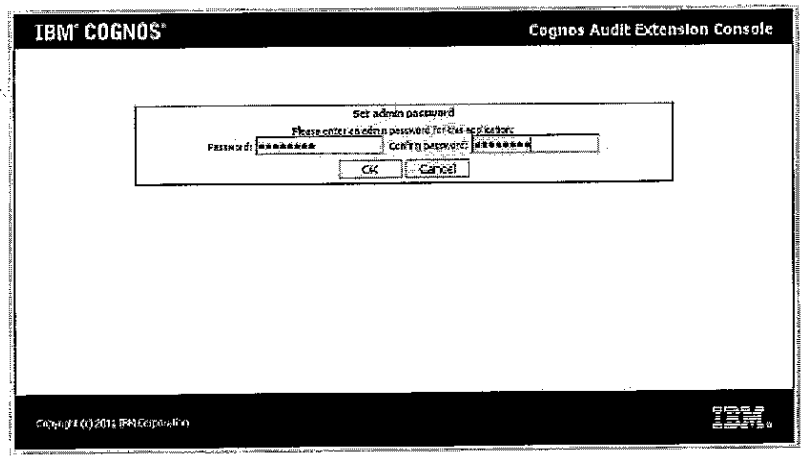
Para limitar a auditoria de conteúdo para todos os pacotes que comecem com "GO", use o seguinte:

```
GO*
```

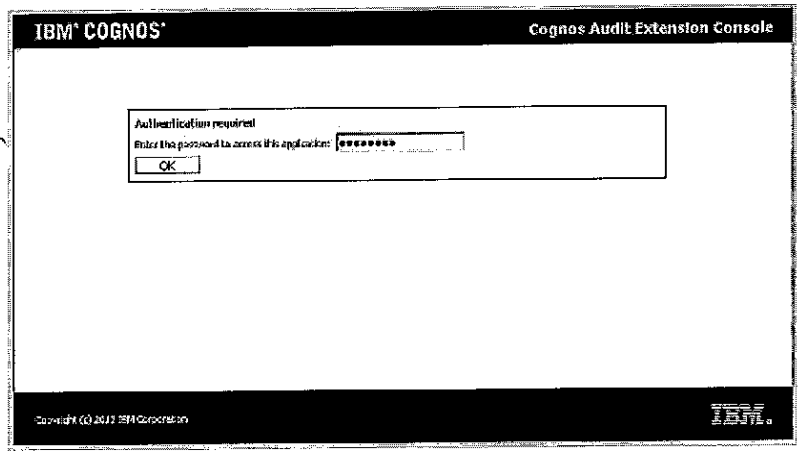
Observe que o filtro faz distinção entre maiúsculas e minúsculas.

Configurar a segurança

Como dito anteriormente, o aplicativo usa seu próprio mecanismo de segurança. Clique no link chamado **Set admin password** na página Manage Servers principal para especificar a senha necessária para executar o aplicativo. Uma tela com os campos Password e Confirm Password será exibida. Especifique a senha em ambos os campos e clique no botão OK para configurar a senha de administrador.



Após a senha ter sido configurada, uma tela de prompt solicitando a inserção da senha necessária para acessar o aplicativo será exibida para os usuários.



Executar auditorias através da interface da web

Para executar uma auditoria através da interface da web, acesse a página Manage Servers. Cada entrada de servidor tem um botão Run que fará com que as auditorias configuradas sejam executadas para esse servidor. Para executar a auditoria para todos os servidores configurados, clique no botão Execute próximo ao campo **All servers** .

Executar auditorias através de uma URL

Para executar uma auditoria para um ID de servidor usando uma URL, use a sintaxe a seguir:

http://servername:9300/AuditExt/AuditServlet?action=run_audit&server_id=serverId

Para executar uma auditoria para todos os servidores especificados na página Manage Servers usando uma URL, use a sintaxe a seguir:

http://servername:9300/AuditExt/AuditServlet?action=run_audit&server_id=all

Executar auditorias através da chamada de serviço da web

O WSDL para a interface de serviço da web pode ser encontrado na URL:

http://servername:9300/AuditExt/services/AuditService?wsdl

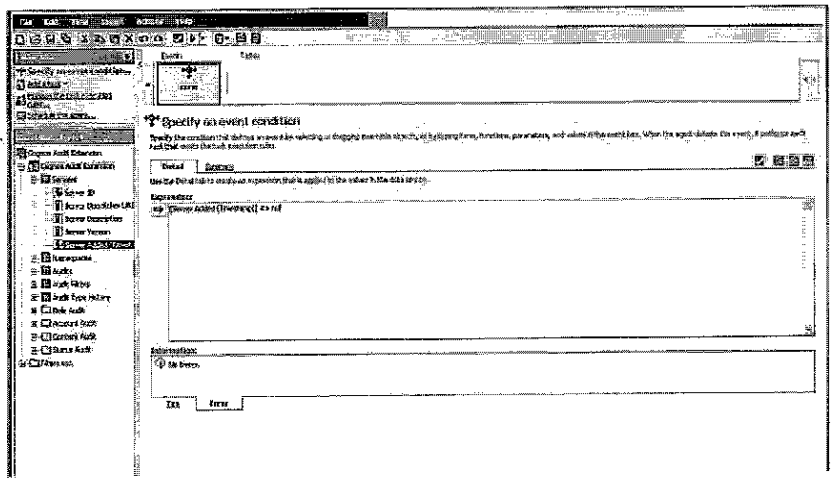
Há dois métodos disponíveis na interface de serviços da web:

- **runAudit** – Toma um parâmetro, o ID do servidor, e executa as auditorias configuradas para esse servidor.
- **runAuditAll** – Não toma nenhum parâmetro e executa as auditorias configuradas para todos os servidores.

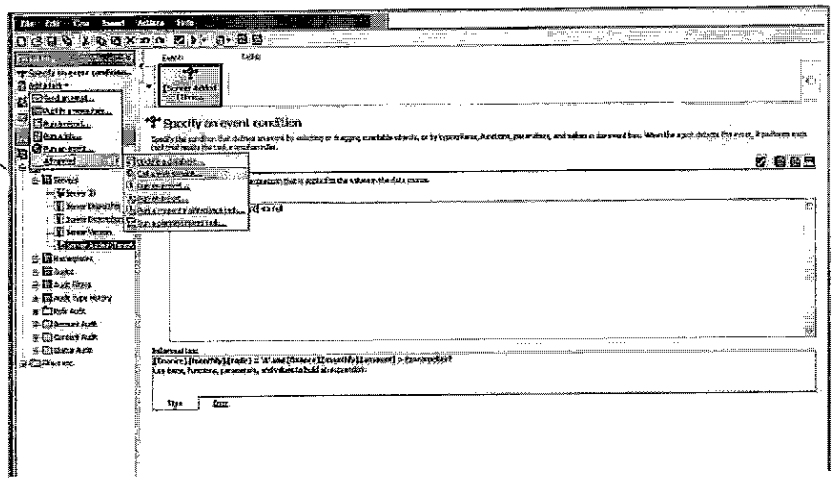
Esse serviço da web pode ser chamado a partir de qualquer aplicativo, mas aqui será apresentado um exemplo que usa o Event Studio para criar um agente do IBM Cognos 10 BI que irá chamar a interface de serviço da web para executar uma auditoria. O exemplo irá usar o pacote de amostras que acompanha esse aplicativo.

Quando o Event Studio é chamado para criar um novo agente, a primeira tela exibida é **Specify an event condition...** Use uma medida no modelo que sabidamente seja maior que zero ou não nula. Isso forçará a condição do evento a ser verdadeira e a execução do agente será garantida sob demanda ou conforme planejado. Nessa instância a condição será configurada para:

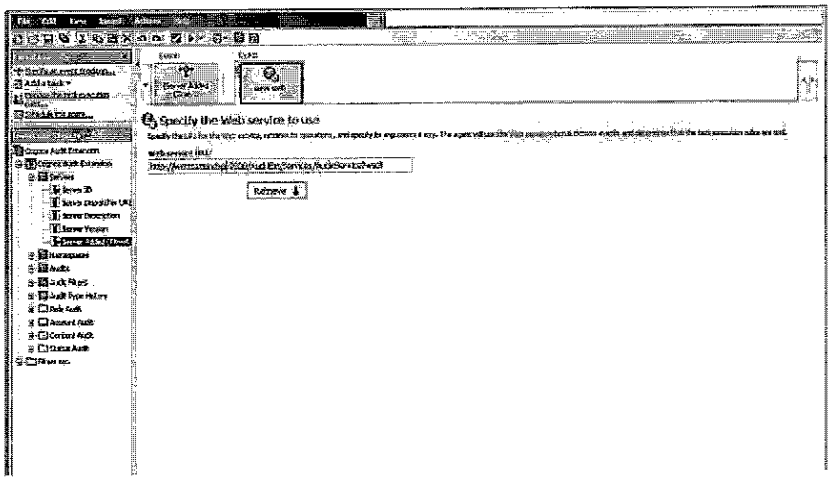
```
[Server Added(Timestamp)] <> null
```



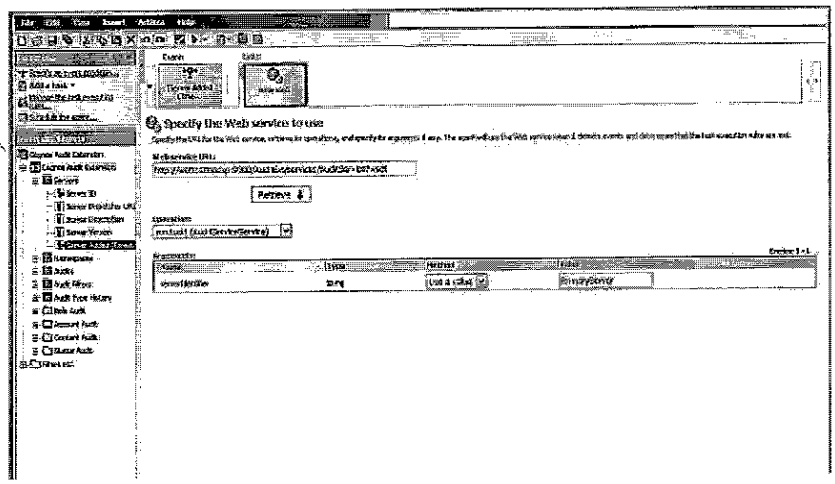
Na guia **Add a Task** , selecione **Advanced > Call a Web service...**



Insira a URL para o WSDL no campo **Web service URL:** e clique no botão Retrieve para obter os métodos disponíveis.



Após o WSDL ser recuperado, as operações que podem ser realizadas serão armazenadas na lista suspensa chamada **Operation:** e uma caixa chamada **Arguments**: permitirá a configuração do valor para cada argumento associado a cada operação. Nessa instância, o método **runAudit** foi selecionado na lista suspensa e o ID do servidor **PrimaryServer** configurado anteriormente foi fornecido como o **serverIdentifier** .



Salve o agente. Agora o agente pode ser planejado através do IBM Cognos Connection.

Implementação de amostra

Um arquivo de implementação do IBM Cognos 10 BI consistindo em um pacote contendo alguns agentes e relatórios de amostra criados com relação ao modelo de amostra do IBM Cognos Framework Manager é fornecido com esse aplicativo. O modelo e a implementação de amostra estão contidos no arquivo AuditExt_reporting_*ver_yyyymmdd*.zip, em que a porção *ver* do nome indica a(s) versão(ões) do IBM Cognos 10 BI a ser usado e a porção *yyyymmdd* do nome representa a data em que o pacote de relatórios foi liberado.

Para importar a implementação de amostra para que ela possa ser usada pelos Studios do IBM Cognos 10 BI:

- Copie o arquivo *AuditExt_deployment_ver_yyyymmdd.zip* para o diretório da implementação do IBM Cognos 10 BI, normalmente <c10install>/deployment.
- No IBM Cognos Administration, clique na guia Configuration, selecione Content Administration e clique no ícone New Import. Selecione o arquivo de implementação chamado *AuditExt_deployment_ver yyyymmdd*. A partir desse ponto, siga as instruções e opções apresentadas no New Import wizard. Na maioria das instâncias, as configurações padrão serão suficientes. Observe que o nome da implementação interna é *Cognos_Audit_Extension.*

Antes de o pacote poder ser usado, é necessário criar uma nova origem de dados no IBM Cognos Content Store que irá interagir com o banco de dados de auditoria especificado quando esse aplicativo foi instalado inicialmente. No IBM Cognos Administration, clique na guia Configuration e selecione Data Source Connection. Clique no ícone New Data Source e nomeie a nova origem de dados como **audit_ext**. A partir desse ponto, siga as instruções e opções apresentadas pelo New Data Source wizard para criar a origem de dados.

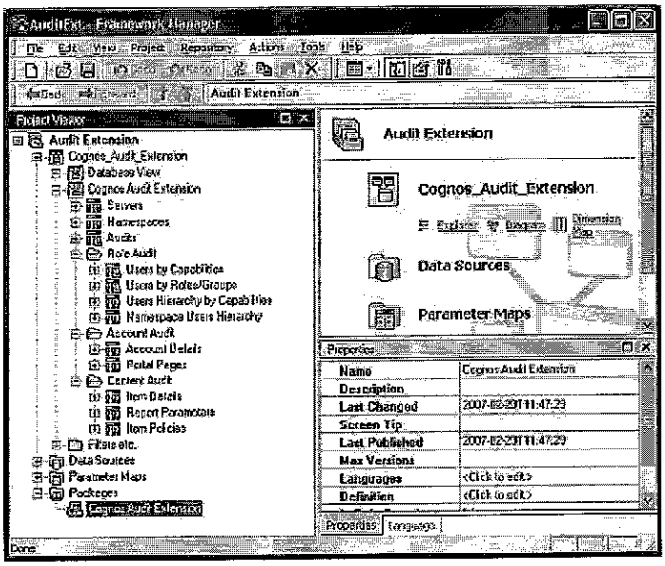
Agora o pacote pode ser usado pelos Studios do IBM Cognos 10 BI.

Modelo de amostra

Um modelo de amostra do IBM Cognos Framework Manager também é fornecido com o aplicativo como base para desenvolvimentos adicionais. O modelo de amostra é fornecido com o arquivo *AuditExt_model_yyyymmdd.zip* em que a porção yyyymmdd representa a data em que o modelo foi liberado.

Antes de esse modelo poder ser usado, uma origem de dados chamada **audit_ext** deve existir no IBM Cognos 10 Content Store. Essa origem de dados é a mesma origem descrita na seção chamada *Implementação de amostra.*

Descompacte o modelo de amostra em um diretório adequado e, no IBM Cognos Framework Manager, abra o arquivo de projeto *AuditExt.cpf.*



Reconhecendo o c8AuditExtension

O aplicativo c10AuditExtension reconhece a existência do aplicativo c8AuditExtension.

Recomenda=se que o aplicativo c10AuditExtension use um banco de dados separado do aplicativo c8AuditExtension. Porém, é possível para o c10AuditExtension usar o banco de dados que foi estabelecido com o c8AuditExtension. Se o aplicativo c10AuditExtension for configurado para usar um banco de dados existente que será compartilhado com o c8AuditExtension, então, o seguinte se aplica:

- Os servidores IBM Cognos 8 que foram definidos no c8AuditExtension aparecerão na página Manage Servers e podem ser editados na página Edit Server.
- As auditorias para os servidores IBM Cognos 8 não serão executados a partir do aplicativo c10AuditExtension.
- A criação de relatórios deve ser feita usando o pacote de relatórios fornecido com o c10AuditExtension.

Consulte http://www.ibm.com/developerworks/data/library/cognos/development/utilities/page509.html para obter mais informações sobre o aplicativo c8AuditExtension.

Outro

Logging

Esse aplicativo usa o log4j para fornecer serviços de criação de log. Para alterar as configurações de criação de log, edite o arquivo <c10install>/webapps/c10AuditExtension/WEB-INF/classes/log4j.properties. O arquivo de log é predeterminado como <c10install>/logs/c10AuditExtension.log.

Consulte a documentação do log4j em http://logging.apache.org/log4j/1.2/index.html para obter mais informações sobre como configurar o log4j.

Tabelas de banco de dados

O aplicativo cria/usa as seguintes tabelas:

Configuração geral

AE_CONFIG_MAIN
Configuração principal do aplicativo contendo os servidores configurados.

AE_CONFIG_NS
Os namespaces salvos configurados para cada servidor.

AE_AUDIT_TYPES
Lista dos tipos de auditoria possíveis.

AE_SERVER_VERSIONS
Lista das versões de servidor Cognos suportadas.

AE_CONFIG_AUDIT_TYPES
Que tipos de auditoria estão configurados para cada servidor.

AE_SECURITY
Tabela contendo a senha de administrador criptografada.

Auditoria de conta

AE_ACCOUNTAUDIT_MAIN
Tabela de detalhes principal

AE_ACCOUNTAUDIT_PORTALPAGES

Registros de quaisquer páginas de portal do usuário.

Auditoria de conteúdo

AE_CONTENTAUDIT_MAIN
Tabela de detalhes principal.

AE_CONTENTAUDIT_PARAMS
Registro dos parâmetros salvos para as visualizações e relatórios.

AE_CONTENTAUDIT_POLICIES
Registro de todas as políticas de segurança aplicadas a todos os objetos.

AE_CONTENTAUDIT_SPEC
Registro de especificações de análise, consulta e relatório.

AE_CONTENTAUDIT_REPORT_VERSIONS
Registro das versões de saída do relatório salvas no Content Store.

AE_CONTENTAUDIT_REPORT_OUTPUTS
Registro das saídas de relatório salvas no Content Store.

Auditoria de função

AE_ROLEAUDIT_HEIR
Uma versão nivelada da hierarquia das pastas Capabilities e Namespace.

AE_ROLEAUDIT_DETAIL
Tabela de detalhes principal.

Auditoria de status

AE_STATUSAUDIT_MAIN
Tabela de detalhes principal.

AE_STATUSAUDIT_RESULT_TYPES
Tabela de consulta para os códigos de tipo de resultado.

AE_STATUSAUDIT_DISP
Detalhes de auditoria principais para cada dispatcher registrado no Content Store.

AE_STATUSAUDIT_DISP_CONFIG
Detalhes de configuração adicionais para cada dispatcher registrado no Content Store.

AE_STATUSAUDIT_DISP_SERVICES
Detalhes dos serviços em execução para cada dispatcher registrado no Content Store.

AE_STATUSAUDIT_DISP_PING
Resultados de testes de rede simples nos dispatchers.

AE_STATUSAUDIT_PING_TEST_TYPES
Possíveis tipos de testes de rede simples que podem ser realizados nos dispatchers.

AE_STATUSAUDIT_PING_RESULT_TYPES
Possíveis códigos de resultado e descrições dos testes de rede simples do dispatcher.

Dados de auditoria geral

AE_STATUS
Histórico e status das execuções de auditoria.

AE_AUDIT_TYPE_LOG
O log dos tipos de auditoria executados para cada auditoria.

AE_ITEM_LOOKUP
Tabela de consulta correlacionando os IDs de armazenamento de item com os nomes.

AE_ITEM_LOOKUP_FAILURES
Registro de todos os itens que não puderam ser consultados (por exemplo, pelo fato de terem sido removidos do Content Store, mas terem sido encontrados nas auditorias como proprietários de outros itens, etc.)

AE_MAP_DATETIME
Tabela para o mapeamento de registros de data e hora (como os horários de início e conclusão da auditoria) para as chaves da tabela de dimensão de tempo e data.

AE_DIM_DATE
Tabela de dimensão de data. A granularidade é de dias.

AE_DIM_TIME
Tabela de dimensão de tempo. A granularidade é de minutos.

AE_SECURITY_MEMBERS
Dados opcionais sobre as políticas de segurança geradas durante uma Auditoria de Conta ou Conteúdo quando a opção option.c8.policy.deviation está configurada para falso.

Histórico de Mudanças

Versão 1.0

Release inicial, com base no c8AuditExtension versão 1.5.

Download

Descrição	Nome	Tamanho	Método de download
Sample scripts for this article	c10AuditExtensionPublicPackage.zip	2424KB	HTTP

Informações sobre métodos de download

Sobre o autor

Equipe de Práticas Comprovadas do Business Analytics

Fechar [x]

developerWorks: Registre-se

IBM ID: jhanssen.oliveira@ewave.com.t
Precisa de um ID IBM?
Esqueceu seu ID IBM?

Senha: ••••••••
Esqueceu sua senha?
Alterar sua senha

☐ Mantenha-me conectado.

Ao clicar em **Enviar**, você concorda com os termos de uso do developerWorks.

Enviar Cancelar

Na primeira vez que você efetua sign in no developerWorks, um perfil é criado para você. **Informações selecionadas do seu perfil developerWorks são exibidas ao público, mas você pode editá-las a qualquer momento.** Seu primeiro nome, sobrenome (a menos que escolha ocultá-los), e seu nome de exibição acompanharão o conteúdo que postar.

Todas as informações enviadas são seguras.

Fechar [x]

Selecione seu nome de exibição

Ao se conectar ao developerWorks pela primeira vez, é criado um perfil para você e é necessário selecionar um nome de exibição. O nome de exibição acompanhará o conteúdo que você postar no developerWorks.

Escolha um nome de exibição de 3 - 31 caracteres. Seu nome de exibição deve ser exclusivo na comunidade do developerWorks e não deve ser o seu endereço de email por motivo de privacidade.

Nome de exibição: (Deve possuir de 3 a 31 caracteres.)

Ao clicar em **Enviar**, você concorda com os termos de uso do developerWorks.

Enviar Cancelar

Todas as informações enviadas são seguras.

Média de classificação (0 voto)

- 1 estrela 1 estrela
- 2 estrelas 2 estrelas
- 3 estrelas 3 estrelas
- 4 estrelas 4 estrelas
- 5 estrelas 5 estrelas

Enviar

Incluir comentário:

Conectar or registre-se para deixar um comentário.

Observação: elementos HTML não são suportados nos comentários.

Notificar-me quando um comentário for adicionado1000 caracteres restantes

Postar

Nenhum comentário postado para esse artigo