

IBM Cognos Business Intelligence
Version 10.2.2

Architecture and Deployment Guide



Note

Before using this information and the product it supports, read the information in “Notices” on page 131.

Product Information

This document applies to IBM Cognos Business Intelligence Version 10.2.2 and may also apply to subsequent releases.

Licensed Materials - Property of IBM

© **Copyright IBM Corporation 2005, 2014.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Introduction	vii
Chapter 1. IBM Cognos BI	1
Chapter 2. The Multitiered Architecture	3
User Interfaces.	3
Web-based User Interfaces.	4
Windows-based User Interfaces	7
Tier 1. Web Server: IBM Cognos BI Gateways	9
Tier 2. Applications: IBM Cognos BI Servers	10
Dispatcher.	10
Content Manager	14
Tier 3. Data: Content Providers	16
Content Store.	16
Data Sources	17
Metric Store	18
Chapter 3. Communications	19
Messaging and Dispatching	20
Local Preferred Dispatching	20
Log Message Processing	20
Planning Log Message Repositories in a Distributed Installation.	21
Recommendation - Consolidate Log Messages in a Distributed Environment Using a Remote Log Server	23
Recommendation - Configure a Log File for Each Log Server.	23
Database Connection Management	24
Content Store Database	24
Query Databases	24
Metric Store Databases	24
Microsoft .NET Framework Interactions	25
Port Usage	25
Request Flow Processing	26
Accessing IBM Cognos BI	26
Viewing a Report or Analysis	29
Running a Report or Analysis	30
Scheduling a Task to Run.	32
Opening IBM Cognos Connection Folder	33
Running an Agent	34
Indexing content.	35
Searching content	36
Portal Pages	38
Chapter 4. Workflow	41
Planning for Implementation	42
Installing IBM Cognos Business Intelligence	42
Configuring IBM Cognos Business Intelligence	43
Monitoring Configuration Changes	44
Configuring Security	44
Configuring IBM Cognos Business Intelligence for Multilingual Reporting	44
Administering IBM Cognos Business Intelligence.	45
Using IBM Cognos BI for Reporting and Analysis	46
Creating Reporting Models and Packages	46
Authoring Reports	47
Using IBM Cognos Business Intelligence for Scorecarding	49
Packaging in Metric Studio	49

Authoring Scorecarding Applications	49
Using IBM Cognos Business Intelligence to Create PowerCubes	50
Managing Events	50

Chapter 5. Implementation Planning Checklist. 51

Chapter 6. Installation Options 53

Installing All Components on One Computer	53
Installing the Gateway on a Separate Computer	55
Installing Application Tier Components and Content Manager on Separate Computers	56
Multiple Installations of Content Manager	58
Modeling Tool Installation Options	59
IBM Cognos Business Intelligence with other IBM Cognos products	61
IBM Cognos products that can be upgraded to IBM Cognos Business Intelligence	62
IBM Cognos Series 7 products that can be migrated to IBM Cognos Business Intelligence	63
IBM Cognos products that interoperate with IBM Cognos Business Intelligence.	64
IBM Cognos Series 7 content that can be recreated in IBM Cognos Business Intelligence.	67

Chapter 7. Performance Planning 69

Capacity Planning	69
Estimating IBM Cognos BI User Load	70
Assessing Application Complexity.	72
Planning Infrastructure Components	72
Scalability Planning.	75
Web Server and Gateway Scalability	75
IBM Cognos BI Server Scalability	80
Availability Planning	82
IBM Cognos Business Intelligence Gateway Availability	82
IBM Cognos Business Intelligence Server Availability	82
Content Manager Availability	83
Content Store Availability.	83

Chapter 8. Performance Monitoring and Tuning 85

Performance Metrics	85
Database Tuning.	86
Application Server Tuning	87
Changing Memory Settings	87
Setting Connection Limits	87
Web Server Tuning	88
IBM Cognos BI Tuning	88
Designing Models and Reports for Performance	88
Tuning IBM Cognos BI Dispatchers	89
Tuning the Report Service, Batch Report Service, and Report Data Service	90
Setting Affinity Connections.	90
Best Practices for Scheduled Reporting	92
Using Report Bursting.	93
PDF Rendering	94
Low Bandwidth Connections	94
Disk Maintenance	94
Performance for IBM Cognos Mobile	94
Estimate the bandwidth required by IBM Cognos Mobile	94
Estimate the required number of servers.	95
Estimating the size of a report	95
Advanced Report Processing Configuration Settings.	96

Chapter 9. Globalization Considerations 97

Locales	97
Adding Fonts to the IBM Cognos BI Environment	99
Changing the Language of the User Interface.	100
Changing the Language of Reports, Data, or Metadata for Users	101

Customizing Currency, Numbers, Dates, and Times	103
Setting up a Multilingual IBM Cognos BI Environment	104
Configuring a Database for Multilingual Reporting.	105
Chapter 10. Security Architecture.	107
IBM Cognos Application Firewall	107
IBM Cognos Authentication Services	108
Cognos Namespace	108
Single Signon	109
IBM Cognos Authorization Services	109
Distributed Administration	109
Permissions	109
Cryptographic Services	110
Using a Third-party Certificate Authority	110
IBM Cognos Cryptographic Provider	110
Chapter 11. Securing the Deployment	113
Techniques for Securing the Operating System	114
Techniques for Securing the Network	117
Securing the Application.	118
Recommendation - Use IBM Cognos Application Firewall	118
Configuring the Cryptographic Environment	119
Securing Temporary Files	122
Securing IBM Cognos BI Files	122
Protecting CAM password cookies	122
Techniques for Securing Access to IBM Cognos Connection	123
Securing IBM Cognos PowerCubes	127
Securing Data Source Signons	127
Securing the content store	128
Security Audit	128
Notices	131
Index	135

Introduction

This document is intended for use with IBM® Cognos® Business Intelligence.

This document is for the business intelligence solutions architect who oversees the setup, administration, and use of IBM Cognos BI, a Web-based business intelligence solution with integrated reporting, analysis, scorecarding, and event management features. This document

- Describes the IBM Cognos BI architecture from the perspectives of structure, communications, workflow, and security.
- Provides information to help you plan to install and configure IBM Cognos BI and to maximize its performance.
- Describes the IBM Cognos BI security architecture and provides guidelines for securing the deployment.

Audience

To use this guide effectively, you should already be familiar with your information technology infrastructure and with the business needs of the people in your organization who will use IBM Cognos BI.

Finding information

To find product documentation on the web, including all translated documentation, access IBM Knowledge Center (<http://www.ibm.com/support/knowledgecenter>). Release Notes are published directly to IBM Knowledge Center and include links to the latest technotes and APARs.

You can also read PDF versions of the product online help files by clicking the PDF links at the top of each HTML page, or access the PDFs from the IBM Cognos product documentation web page (www.ibm.com/support/docview.wss?uid=swg27042003).

Forward-looking statements

This documentation describes the current functionality of the product. References to items that are not currently available may be included. No implication of any future availability should be inferred. Any such references are not a commitment, promise, or legal obligation to deliver any material, code, or functionality. The development, release, and timing of features or functionality remain at the sole discretion of IBM.

Samples disclaimer

The Sample Outdoors Company, Great Outdoors Company, GO Sales, any variation of the Sample Outdoors or Great Outdoors names, and Planning Sample depict fictitious business operations with sample data used to develop sample applications for IBM and IBM customers. These fictitious records include sample data for sales transactions, product distribution, finance, and human resources. Any resemblance to actual names, addresses, contact numbers, or transaction values is coincidental. Other sample files may contain fictional data manually or machine generated, factual data compiled from academic or public sources, or data

used with permission of the copyright holder, for use as sample data to develop sample applications. Product names referenced may be the trademarks of their respective owners. Unauthorized duplication is prohibited.

Chapter 1. IBM Cognos BI

IBM Cognos Business Intelligence is a solution designed to address the challenges of enterprise-scale reporting, analysis, scorecarding, and event notification.

The IBM Cognos BI architecture was designed for scalability, availability, and openness. It uses platform independent, industry proven technology, such as Extensible Markup Language (XML), Simple Object Access Protocol (SOAP), and Web Services Definition Language (WSDL). For this reason, IBM Cognos BI can integrate with and leverage your existing technology infrastructure on multiple platforms.

The IBM Cognos BI architecture features a consistent, zero footprint, Web-based user interface for viewing, creating, and administering reports, analyses, scorecards, and events. It has a common dispatcher and supports leading relational databases as well as Online Analytical Processing (OLAP) and dimensionally modeled relational cubes. It ensures dynamic load balancing and provides failover recovery for continuous operation. It also provides a single point of administration, as well as Web-based delegated administration. IBM Cognos BI is fully open to third-party products and custom development. It also integrates with Web farms and supports multilingual reporting and scorecarding.

IBM Cognos Data Manager

IBM Cognos BI also includes Data Manager for data integration. With Data Manager, you can extract data from source systems and data files, transform the data, and load it into a data warehouse, conformed data mart, or report staging area.

For information about the Data Manager architecture, see the *IBM Cognos Data Manager Installation and Configuration Guide* and the *IBM Cognos Data Manager User Guide*.

Chapter 2. The Multitiered Architecture

IBM Cognos Business Intelligence has a multitiered architecture. For description purposes, it can be separated into three tiers: Web server, applications, and data. The tiers are based on business function, and are typically separated by network firewalls. IBM Cognos BI user interfaces sit above the tiers.

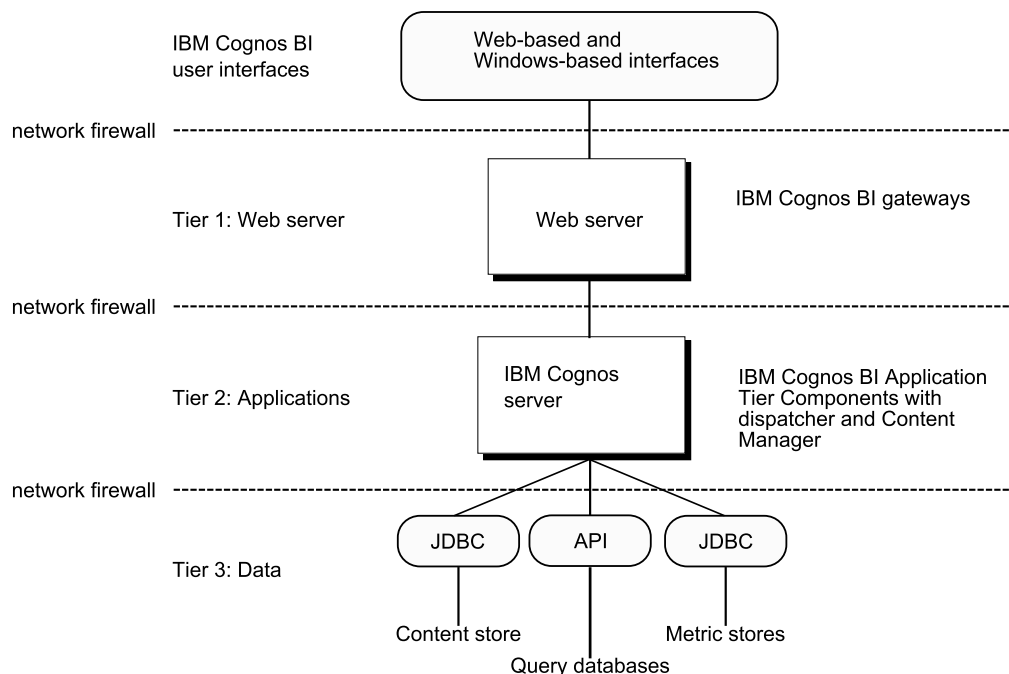


Figure 1. Multitiered architecture workflow

This information describes a single-server IBM Cognos BI configuration. To meet your requirements, you can choose a different configuration. For more information, see Chapter 6, "Installation Options," on page 53.

User Interfaces

IBM Cognos BI is configured using IBM Cognos Configuration. You also use IBM Cognos Configuration to start and stop IBM Cognos services.

In addition to IBM Cognos Configuration, IBM Cognos BI has Web-based and Windows-based user interfaces, as listed in the following table.

Table 1. IBM Cognos BI Web-based and Windows-based user interfaces

Web-based interfaces	Windows-based interfaces
Cognos Connection	Cognos Framework Manager
Cognos Administration	Cognos Metric Designer
Cognos Query Studio	Cognos Transformer
Cognos Report Studio	Cognos Map Manager
Cognos Analysis Studio	Cognos BI for Microsoft Office
Cognos Event Studio	Cognos Insight
Cognos Metric Studio	
Cognos Workspace	
Cognos Workspace Advanced	

Web-based User Interfaces

The zero footprint, Web-based interfaces include the following components:

- “ IBM Cognos Connection”
- “ IBM Cognos Administration” on page 5
- “Cognos Query Studio ” on page 6
- “Cognos Report Studio” on page 6
- “Cognos Analysis Studio” on page 6
- “Cognos Event Studio ” on page 6
- “Cognos Metric Studio” on page 6
- “Cognos Workspace” on page 7
- “Cognos Workspace Advanced” on page 7

The interfaces that are available to users depend on user permissions and on the IBM Cognos BI packages that your organization purchased.

IBM Cognos Connection

IBM Cognos Connection is a Web portal provided with IBM Cognos Business Intelligence, providing a single access point to the corporate data available for its products. It provides a single point of entry for querying, analyzing, and organizing data, and for creating reports, scorecards, and events. Users can run all their Web-based IBM Cognos BI applications through IBM Cognos Connection. Other business intelligence applications, and web addresses to other applications, can be integrated with IBM Cognos Connection.

Like the other Web browser interfaces in IBM Cognos BI, IBM Cognos Connection uses the default configurations of your browser. It does not require the use of Java™, ActiveX, or plug-ins, and does not install them.

In addition to selections for viewing data and creating objects, IBM Cognos Connection includes

- portal pages



The **New Page** button opens a wizard where users can create a customizable page that uses portlets to show different types of content at the same time.


- Public Folders

Public Folders store shared IBM Cognos BI content, such as packages “Creating Reporting Models and Packages” on page 46, reports, agents, shortcuts, and jobs.

- My Folders

My Folders store personal IBM Cognos BI content, such as reports, shortcuts, and jobs.

- User preferences

The **My Area Options** button  includes links to My Watch Items, alert lists and watch rules that help you monitor business events; My Preferences, settings for format, language, time zone, contact information, and portal content; and My Activities and Schedules, status windows where you can set priorities for and monitor your IBM Cognos BI activities.

- Link to tools and applications

The **Launch** button provides links to the IBM Cognos BI studios, Drill-through Definitions, which are used to navigate through related data when querying or analyzing data, and IBM Cognos Administration.

For information about using Cognos Connection, see the *IBM Cognos Connection User Guide*.

The open IBM Cognos BI architecture means that you can choose to integrate IBM Cognos BI into your organization's existing Web portal. You can use Portal Services, provided with IBM Cognos BI, to integrate IBM Cognos BI with a number of portals, including

- SAP Enterprise Portal
- IBM WebSphere® Portal
- Oracle WebCenter Interaction Portal
- SharePoint Portal

For more information, see the *IBM Cognos Administration and Security Guide*.

IBM Cognos Administration

IBM Cognos Administration is a central management interface that contains the administrative tasks for IBM Cognos BI. It provides easy access to the overall management of the IBM Cognos environment and is accessible through IBM Cognos Connection.

IBM Cognos Administration is organized into three sections:

- Status

Use the links in this section to monitor activities, server status, and system metrics, and change some system settings.

- Security

Use the links in this section to define users, groups, and roles for security purposes, configure capabilities for the interfaces and studios, and set properties for the user interface profiles (professional and express) that are used in Report Studio.

- **Configuration**

Use the links in this section to set up data source connections, deploy IBM Cognos BI content from one content store to another, create distribution and contact lists, add printers, set styles, manage portlets and portal layout, start or stop dispatchers and services, and change system settings.

For information about using Cognos Administration, see the *IBM Cognos Business Intelligence Administration and Security Guide*.

Cognos Query Studio

Using Query Studio, users with little or no training can quickly design, create and save reports to meet reporting needs not covered by the standard, professional reports created in Report Studio.

For information about using Cognos Query Studio, see the *IBM Cognos Query Studio User Guide*.

Cognos Report Studio

Using Report Studio, report authors create, edit, and distribute a wide range of professional reports. They can also define corporate-standard report templates for use in Query Studio, and edit and modify reports created in Query Studio or Analysis Studio.

For information about using Cognos Report Studio, see the *IBM Cognos Report Studio User Guide*.

Cognos Analysis Studio

In Analysis Studio, users can explore, analyze, and compare dimensional data. Analysis Studio provides access to dimensional, OLAP (online analytical processing), and dimensionally modeled relational data sources. Analyses created in Analysis Studio can be opened in Report Studio and used to build professional reports.

For information about using Cognos Analysis Studio, see the *IBM Cognos Analysis Studio User Guide*.

Cognos Event Studio

In Event Studio, you set up agents to monitor your data and perform tasks when business events or exceptional conditions occur in your data that must be dealt with. When an event occurs, people are alerted to take action. Agents can publish details to the portal, deliver alerts by email, run and distribute reports based on events, and monitor the status of events. For example, a support call from a key customer or the cancellation of a large order may trigger an event, sending an e-mail to the appropriate people.

For information about using Cognos Event Studio, see the *IBM Cognos Event Studio User Guide*.

Cognos Metric Studio

In Metric Studio, you can create and deliver a customized scorecarding environment for monitoring and analyzing metrics throughout your organization.

Users can monitor, analyze, and report on time-critical information by using scorecards based on cross-functional metrics.

For information about using Cognos Metric Studio, see the *IBM Cognos Metric Studio User Guide*.

Cognos Workspace

In IBM Cognos Workspace, you can create sophisticated interactive workspaces using IBM Cognos content, as well as external data sources such as TM1[®] Websheets and CubeViews, according to your specific information needs. You can view and open favorite workspaces and reports, manipulate the content in the workspaces, and e-mail your workspaces. You can also use comments, activities and social software such as IBM Connections for collaborative decision making.

For more information about using Cognos Workspace, see the *IBM Cognos Workspace User Guide*.

Cognos Workspace Advanced

With IBM Cognos Workspace Advanced, a component of IBM Cognos BI, you can perform advanced data exploration and author simple reports.

With Cognos Workspace Advanced you can extend your data exploration by specifying additional measures, adding conditional formatting, and using advanced calculations.

You can also create reports with relational or dimensional data sources that display your data in lists, crosstabs, and charts. You have the option of using your own external data source.

There are two ways to start Cognos Workspace Advanced:

- From a workspace in IBM Cognos Workspace, you can click a button to create a report or do advanced exploration related to the information in that workspace.
- From the IBM Cognos Connection portal, you can click Author Business Reports.

For more information about using Cognos Workspace Advanced, see the *IBM Cognos Workspace Advanced User Guide*.

Windows-based User Interfaces

Windows-based IBM Cognos BI interfaces are IBM Cognos Framework Manager, IBM Cognos Metric Designer, IBM Cognos Transformer, IBM Cognos Map Manager, IBM Cognos BI for Microsoft Office, and IBM Cognos Insight.

Cognos Framework Manager

IBM Cognos Framework Manager is the modeling tool for creating and managing business-related metadata for use in IBM Cognos BI analysis and reporting. Metadata is published for use by reporting tools as a package, providing a single, integrated business view of any number of heterogeneous data sources.

OLAP cubes are designed to contain metadata for business intelligence reporting and analysis. All metadata, including all members, cube dimensions, hierarchies, and levels are loaded at run time.

For information about using Cognos Framework Manager, see the *IBM Cognos Framework Manager User Guide*.

Cognos Metric Designer

Metric Designer is the modeling tool used to create extracts for use in IBM Cognos BI scorecarding applications. Extracts are used to map and transfer information from existing metadata sources such as IBM Cognos Framework Manager and Impromptu® Query Definition (.iqd) files.

For information about using Cognos Metric Designer, see the *IBM Cognos Metric Designer User Guide*.

Cognos BI for Microsoft Office

With IBM Cognos BI for Microsoft Office you can access IBM Cognos reporting data directly from within Microsoft Office applications.

IBM Cognos BI for Microsoft Office makes use of the Microsoft .NET Framework to allow clients to interact with server-based components. IBM Cognos BI for Microsoft Office provide two types of clients:

- The smart client is a zero-administration client with a zero-deployment impact. Product updates are automatically applied through the smart client.
- The COM add-in client requires a client installation. Product updates are delivered by uninstalling and reinstalling the COM add-in client.

For more information about using IBM Cognos BI for Microsoft Office, see the *IBM Cognos BI for Microsoft Office User Guide*. For more information about configuring and deploying IBM Cognos BI for Microsoft Office clients, see the *IBM Cognos Business Intelligence Installation and Configuration Guide*.

Cognos Transformer

IBM Cognos Transformer is the IBM Cognos BI modeling tool used to create PowerCubes for use in IBM Cognos BI. Secured IBM Cognos BI PowerCubes are not compatible with IBM Cognos Series 7.

For information about installing and configuring versions of Transformer that are earlier than 8.4, see the documentation provided with your edition of Transformer.

Cognos Map Manager

IBM Cognos Map Manager is a Window-based utility that administrators and modelers use to import maps and update labels for maps in Report Studio. For map features such as country or region and city names, administrators and modelers can define alternative names to provide multilingual versions of text that appears on the map.

For information about using Cognos Map Manager, see the *IBM Cognos Map Manager Installation and User Guide*.

Cognos Insight

In IBM Cognos Insight, you can analyze data, explore scenarios, and influence decisions by creating personal or managed workspaces. Use these interactive

workspaces to communicate results to managers. Because Cognos Insight supports write-back, you can also use these workspaces to gather and consolidate management targets, commitments, and forecasts.

IBM® Cognos® Insight is provided with IBM Cognos BI. Use the IBM Cognos Connection Installer for Cognos Insight to install provisioning software on Cognos BI servers. This software allows multiple users to download and install IBM Cognos Insight on their computers from the Cognos Connection interface.

For more information about using Cognos Insight, see the *IBM Cognos Insight User Guide*.

Tier 1. Web Server: IBM Cognos BI Gateways

The IBM Cognos BI Web server tier contains one or more IBM Cognos BI gateways.

Web communication in IBM Cognos Business Intelligence is typically through gateways, which reside on one or more Web servers. A gateway is an extension of a Web server program that transfers information from the Web server to another server.

Web communication can also occur directly with an IBM Cognos BI dispatcher, although this option is less common than using gateways.

If you install the gateway component on a different computer from Content Manager or Application Tier Components, you must configure the gateway computer so that it knows the location of a dispatcher, preferably one on an Application Tier Components computer. For failover protection, you can configure more than one dispatcher for a gateway computer. For more information, see “Dispatcher” on page 10.

IBM Cognos BI supports several types of Web gateways, including

- ISAPI
ISAPI can be used for the Microsoft Internet Information Services (IIS) Web server. It delivers faster performance for IIS.
- apache_mod
You can use an apache_mod gateway with the Apache Web server.
- servlet
If your Web server infrastructure supports servlets or you are using an application server, you can use a servlet gateway.
- CGI
The default gateway, CGI can be used for all supported Web servers but should not be used in a production environment.

When an IBM Cognos BI gateway receives a request, it

- encrypts passwords to ensure security
- extracts information needed to submit the request to an IBM Cognos BI server
- attaches environment variables for the Web server
- adds a default namespace to the request to ensure that the server authenticates the user in the correct namespace
- passes requests to an IBM Cognos BI dispatcher for processing

For information about configuring IBM Cognos BI gateways, see the *IBM Cognos Business Intelligence Installation and Configuration Guide*.

Tier 2. Applications: IBM Cognos BI Servers

The IBM Cognos BI applications tier contains one or more IBM Cognos BI servers. An IBM Cognos BI server runs requests, such as reports, analyses, and queries, that are forwarded by a gateway. An IBM Cognos BI server also renders the IBM Cognos Connection and Metric Studio interfaces.

Each IBM Cognos BI installation includes

- Application Tier Components, which include a dispatcher, that operates services and routes requests
- Content Manager, which manages IBM Cognos BI information

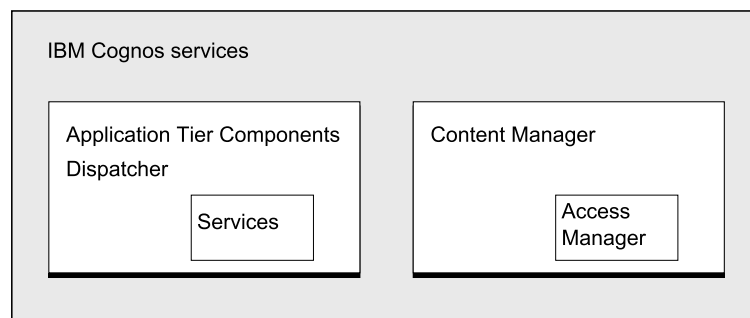


Figure 2. IBM Cognos services

Dispatcher

The dispatcher starts all IBM Cognos services configured and enabled on a computer, and routes requests.

The dispatcher is a multithreaded application that uses one or more threads per request. Configuration changes are routinely communicated to all running dispatchers. The dispatcher includes IBM Cognos Application Firewall to provide security for IBM Cognos BI.

The dispatcher can route requests to a local service, such as the report service, presentation service, job service, or monitor service.

A dispatcher can also route requests to a specific dispatcher to run a given request. Requests can be routed to specific dispatchers based on load-balancing needs, or package or user group requirements. For example, if a particular OLAP data source is available for only one IBM Cognos server group, you specify that all requests for the data source be routed to that IBM Cognos server group. For more information about routing requests based on packages or user groups, see the *Administration and Security Guide*.

When you configure IBM Cognos BI gateways, you can list the universal resource identifiers (URIs) of target dispatchers in order of most to least preferred. If a dispatcher fails, requests are routed to another dispatcher based on the list. The primary dispatcher status is monitored by the gateway, and requests are routed back to this component when it returns to service. For more information, see the *IBM Cognos Business Intelligence Installation and Configuration Guide*.

When a dispatcher starts, it registers itself with Content Manager. As a result, each dispatcher is aware of the other dispatchers. If a dispatcher fails or is unavailable, requests for that dispatcher are routed to the next available dispatcher until the failed dispatcher reregisters itself.

IBM Cognos services

After you install and configure IBM Cognos BI, one dispatcher is available on each computer by default. Each dispatcher has a set of associated services, listed in the following table.

Table 2. IBM Cognos services

Service	Purpose
Agent service	Runs agents. If the conditions for an agent are met when the agent runs, the agent service asks the monitor service to run the tasks.
Annotation service	Enables the addition of commentary to reports via the IBM Cognos Workspace. These comments persist across versions of the report.
Batch report service	Manages background requests to run reports and provides output on behalf of the monitor service.
Content Manager cache service	Enhances the overall system performance and Content Manager scalability by caching frequent query results in each dispatcher.
Content Manager service	<ul style="list-style-type: none"> • Performs object manipulation functions in the content store, such as add, query, update, delete, move, and copy • Performs content store management functions, such as import and export
Data movement service	Manages the execution of data movement tasks in IBM Cognos BI. Data movement tasks, such as Builds and JobStreams, are created in Data Manager Designer and published to IBM Cognos BI.
Delivery service	Sends emails to an external SMTP server on behalf of other services, such as the report service, job service, agent service, or data integration service
Event management service	Creates, schedules, and manages event objects that represent reports, jobs, agents, content store maintenance, deployment imports and exports, and metrics
Graphics service	Produces graphics on behalf of the Report service. Graphics can be generated in 4 different formats: Raster, Vector, Microsoft Excel XML or PDF.
Human task service	Enables the creation and management of human tasks. A human task such as report approval can be assigned to individuals or groups on an ad hoc basis or by any of the other services.

Table 2. IBM Cognos services (continued)

Service	Purpose
Index data service	Provides basic full-text functions for storage and retrieval of terms and indexed summary documents.
Index search service	Provides search and drill-through functions, including lists of aliases and examples.
Index update service	Provides write, update, delete, and administration functions.
Job service	Runs jobs by signaling the monitor service to run job steps in the background. Steps include reports, other jobs, import, exports, and so on.
Log service	Records log messages generated by the dispatcher and other services. The log service can be configured to record log information in a file, a database, a remote log server, Windows Event Viewer, or a UNIX system log. The log information can then be analyzed by customers or by Cognos Software Services, including: <ul style="list-style-type: none"> • security events • system and application error information • selected diagnostic information
Metadata service	Provides support for data lineage information displayed in Cognos Viewer, Report Studio, Query Studio, and Analysis Studio. Lineage information includes information such as data source and calculation expressions.
Metric Studio service	Provides the Metric Studio user interface for monitoring and entering performance information
Migration service	Manages the migration from IBM Cognos Series 7 to IBM Cognos BI.

Table 2. IBM Cognos services (continued)

Service	Purpose
Mobile service	<p>Manages activities related to IBM Cognos Mobile client:</p> <ul style="list-style-type: none"> • Transforms Cognos Business Intelligence reports and analyses for mobile consumption. • Compresses Cognos BI report and analysis content for fast distribution over-the-air to the mobile devices and access from those devices. • Pushes report and analysis content to the mobile devices. • Facilitates incoming and outgoing report-related and analysis-related requests between the mobile device and the environment to search, browse, or run reports. • Synchronizes the mobile content store on the server with the mobile database on the mobile device. • Translates Cognos BI Simple Object Access Protocol (SOAP) messages into wireless-friendly messages. • Communicates with the mobile device.
Monitor service	<ul style="list-style-type: none"> • Manages the monitoring and execution of tasks that are scheduled, submitted for execution at a later time, or run as a background task • Assigns a target service to handle a scheduled task. For example, the monitor service may ask the batch report service to run a report, the job service to run a job, or the agent service to run an agent. • Creates history objects within the content manager and manages failover and recovery for executing entries
Planning administration console service	Manages communication with the Contributor Administration Console.
Planning data service	Manages communications for real-time reporting from Contributor plan data in IBM Cognos BI.
Planning job service	Manages communications with the Planning Job Server subsystem.
Planning web service	Manages communications with Contributor Web and Contributor Add-in for <i>Excel</i> users.
PowerPlay® service	Manages requests to run PowerPlay reports.
Presentation service	<ul style="list-style-type: none"> • Transforms generic XML responses from another service into output format, such as HTML or PDF • Provides display, navigation, and administration capabilities in IBM Cognos Connection

Table 2. IBM Cognos services (continued)

Service	Purpose
Query service	Manages Dynamic Query requests and returns the result to the requesting batch or report service.
Report data service	Manages the transfer of report data between IBM Cognos BI and applications that consume the data, such as IBM Cognos BI for Microsoft Office and IBM Cognos Mobile.
Report service	Manages interactive requests to run reports and provides output for a user in IBM Cognos Connection or a studio.
Repository service	Manages requests to retrieve archived report output from an archive repository or object store.
System service	Defines the Business Intelligence Bus API-compliant service used to obtain application-wide IBM Cognos BI configuration parameters. It also provides methods that normalize and validate locale strings and map locale strings to locales supported by your application.
Visualization Gallery service	Enables the Visualization Gallery in Report Studio.

Content Manager

Content Manager is the IBM Cognos BI service that manages the storage of customer application data, including interactive visualization discovery, relational metadata service, security, configuration data, models, metrics, report specifications, and report output. Content Manager is needed to publish packages, retrieve or store report specifications, manage scheduling information, and manage the Cognos namespace.

Content Manager stores information in a content store database, which is typically located in Tier 3 of the architecture. For more information, see “Dispatcher” on page 10.

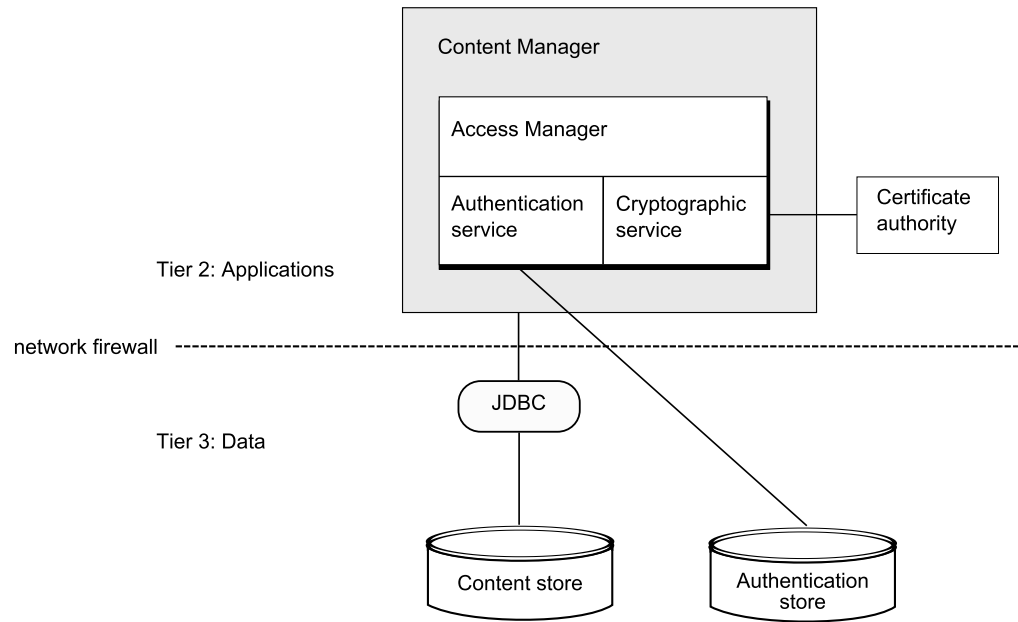


Figure 3. Diagram of the Content Manager

Your installation may include more than one Content Manager, each on a different computer. One Content Manager computer is active and one or more Content Manager computers are on standby.

The information stored by Content Manager includes

- reports
Reports contain specifications, properties, security settings, and outputs. This includes analyses created in Analysis Studio, queries created in Query Studio, and reports created in Report Studio.
- report packages
Packages contain metadata, reports, and folders.
- metric packages
Metric packages contain metadata, scorecards, and folders.
- agents
Agents include the conditions, schedules, and tasks used to monitor events and deliver notifications. This includes the list of recently detected instances of an event.
- server configuration
Server configuration contains directory information, the Cognos namespace “Cognos Namespace” on page 108, and information about contacts, distribution lists, data sources, and printers.
- personal user information
Personal user information consists of My Folders and My Pages.
- language information
Language information includes names, descriptions, and tool tips in different languages to support IBM Cognos BI multilingual capabilities.
- workspaces
Workspaces shared to Cognos Connection from Cognos Insight

Content Manager performs general functions, such as add, query, update, delete, move, and copy. It also performs content store management functions, such as export and import.

Access Manager

Content Manager contains Access Manager, the primary security component of IBM Cognos BI. Access Manager leverages your existing security providers for use with IBM Cognos BI.

It provides IBM Cognos BI with a consistent set of security capabilities and APIs, including user authentication, authorization, and encryption. It also provides support for the Cognos namespace.

Some security capabilities, such as user authentication, are external to IBM Cognos BI but are exposed to IBM Cognos BI by Access Manager. Other capabilities, such as authorization, are internal to IBM Cognos BI, and are implemented by Access Manager.

For many security-related functions, Access Manager requires certificates, and interacts with a certificate authority. By default, IBM Cognos BI uses its own certificate authority service to establish the root of trust in the IBM Cognos BI security infrastructure. If you use a third-party certificate authority, you can configure IBM Cognos BI to use it instead of the default IBM Cognos BI certificate authority. For more information, see Chapter 10, “Security Architecture,” on page 107.

Tier 3. Data: Content Providers

The IBM Cognos Business Intelligence data tier contains the following:

- “Content Store”
- “Data Sources” on page 17
- “Metric Store” on page 18

Content Store

The content store is a relational database that contains data that your IBM Cognos BI product needs to operate, such as report specifications, published models, and the packages that contain them; connection information for data sources; information about the external namespace, and the Cognos namespace itself; and information about scheduling and bursting reports.

IBM Cognos BI includes the IBM Cognos Content Database as a default content store for test and proof of concept installations but it should never be used in a production environment.

The IBM Cognos service that uses the content store is named Content Manager.

Content Manager uses a JDBC (Java DataBase Connectivity) API to access the content store and metric stores. IBM Cognos BI comes with the JDBC drivers for IBM Cognos Content Database and IBM DB2®. If you are using Oracle, Microsoft SQL Server, or Sybase databases, ensure you obtain the appropriate JDBC drivers.

Report results in other formats, such as HTML, XML, and CSV (comma separated values), are stored in compressed form and are uncompressed by Content Manager before they are sent to a user.

IBM Cognos Content Database

IBM Cognos Content Database is an instance of an Apache Derby database that can be optionally installed and used as the default content store. IBM Cognos Content Database can be used where you do not want to implement a commercial database for the content store, such as in a test or proof-of-concept environment. You must use a supported commercial database for the content store in a production environment.

Apache Derby is open source software whose license terms can be found on the Apache Derby Web site. Any modifications to the Apache Derby database, and its use with other than IBM Cognos products is not supported. Any modifications you make to the Apache Derby database are at your own risk.

IBM Cognos Content Database can be installed with other IBM Cognos BI components or installed on a separate computer. The Cognos Content Database service starts the Apache Derby database in which the IBM Cognos Content Database is running.

If you install IBM Cognos Content Database on the same computer as Content Manager, IBM Cognos Content Database will be used as the default content store. For information about changing your content store, see the *IBM Cognos Business Intelligence Installation and Configuration Guide*.

Data Sources

The data sources that can be accessed through IBM Cognos BI include relational databases, dimensional or OLAP cubes, flat files, and other physical data stores. They also include the connection information necessary for accessing the data.

Application Tier Components use data source connections to access data sources.

Enterprise Information Integrators

IBM Cognos BI can be used with Enterprise Information Integration (EII) products such as IBM Cognos BI Virtual View Manager.

IBM Cognos BI Virtual View Manager provides access to additional data sources such as LDAP, Java Database Connectivity (JDBC), Open XML and WSDL, and improves performance when querying data from different data sources.

In the following scenario, the EII product models a set of databases, producing a unified view as a single virtual data source. IBM Cognos BI accesses the EII service as though it were a single database, and the EII service joins data from the various enterprise data sources as needed.

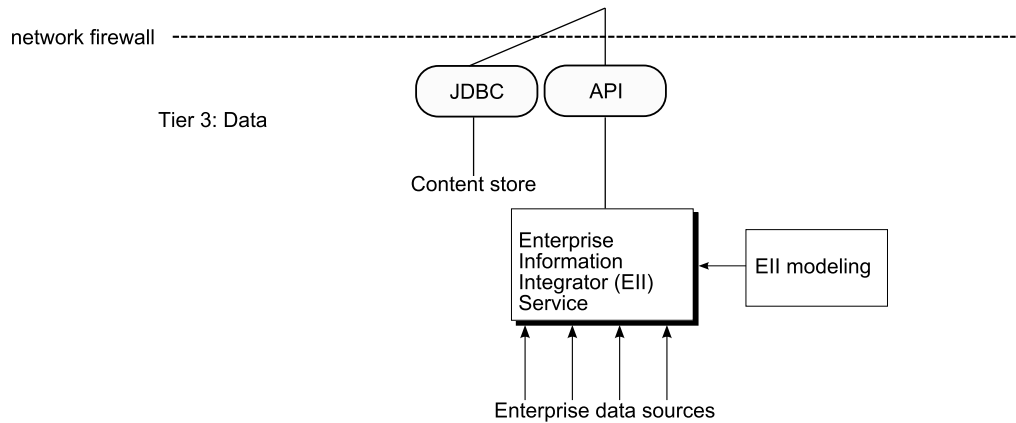


Figure 4. A diagram showing four enterprise data sources feeding into a single virtual EII data source

Metric Store

A metric store is a relational database that contains content for metric packages. A metric store also contains Metric Studio settings, such as user preferences.

More than one metric store may be created. For example, one metric store may contain content for a sales application and another metric store may contain content for a finance application.

Chapter 3. Communications

IBM Cognos Business Intelligence components communicate with each other, and with any additional applications integrated with IBM Cognos BI, using the BI Bus.

The BI Bus is an open, documented, Simple Object Access Protocol (SOAP) API that supports Web Services Definition Language (WSDL). For information about integrating applications with IBM Cognos BI components, see the *Software Development Kit Developer Guide*.

The BI Bus is not a software component like Content Manager or IBM Cognos BI server, but a set of protocols that govern communications among IBM Cognos services. It also defines how industry standards and protocols are used with IBM Cognos BI, enabling IBM Cognos BI to be a fully open system.

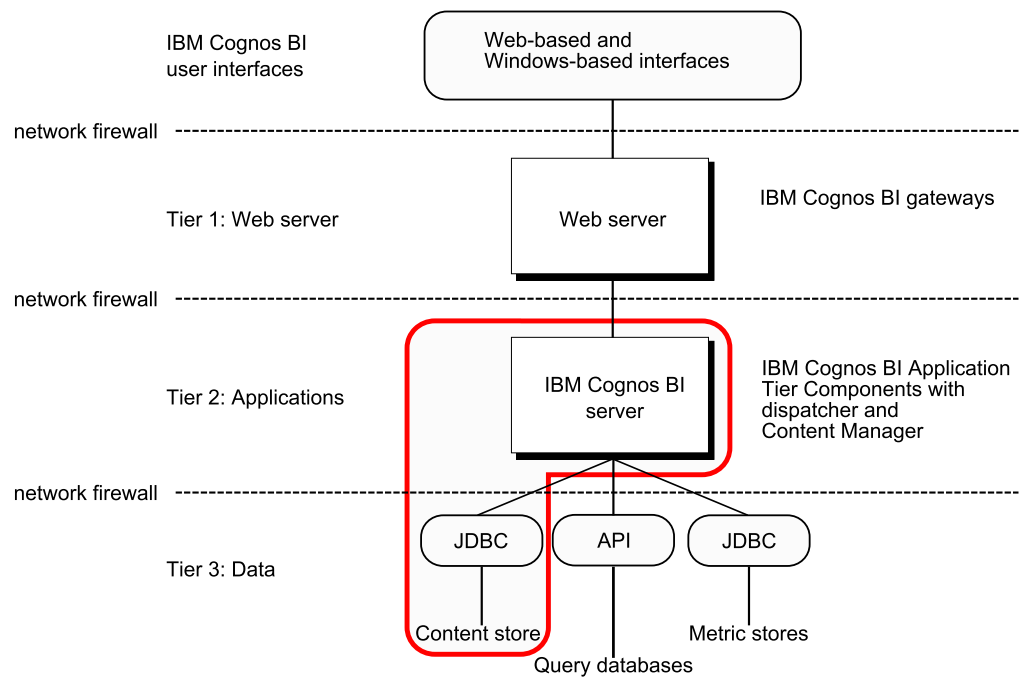


Figure 5. A diagram highlighting the Content Store and IBM Cognos servers in the IBM Cognos software architecture

Everything that is managed through IBM Cognos Connection or your portal is exposed through the BI Bus. This includes packages, folders, reports, analyses, events, directory objects, servers, deployment objects, and metadata. Using an API through the IBM Cognos Software Development Kit, you can create, read, update, and delete these objects, and set security and other properties.

The processes enabled by the BI Bus protocol include

- messaging and dispatching
- log message processing
- database connection management
- Microsoft .NET Framework interactions
- port usage

- request flow processing
- portal pages

Messaging and Dispatching

The BI Bus protocol includes messaging and dispatching processes.

The IBM Cognos BI architecture is tuned to minimize dispatch time. IBM Cognos BI can use network capabilities, such as load-balancing routers, to ensure that dispatchers and Web gateways are used evenly. Load-balancing routers distribute requests across multiple Web or application servers, ensuring that all dispatchers share the workload.

The dispatcher load-balancing scheme is a static algorithm. You can specify a weight for each dispatcher. A dispatcher with a weight of 2 can do twice the work of a dispatcher with a weight of 1, and so on. Each dispatcher spreads work among all the dispatchers using a weighted round-robin algorithm.

Local Preferred Dispatching

When using any sort of external load-balancing mechanism, you should use the local preferred dispatch option.

By using this option, the dispatcher does not perform load balancing. Requests that can be processed locally will be processed locally. If the external load balancing mechanism sends a request to a computer on which the required service is not available, the dispatcher routes the request to an appropriate computer.

For more information, see “Load Balancing” on page 75.

Log Message Processing

The BI Bus protocol includes log message processing, an important diagnostic tool for investigating the behavior of IBM Cognos BI.

In addition to error messages, log messages provide information about the status of components and a high-level view of important events. For example, log messages can provide information about attempts to start and stop services, completion of processing requests, and indicators for fatal errors. Audit logs, which are available from a logging database, provide information about user and report activity.

The IBM Cognos services on each computer send information about errors and events to a local log server. A local log server is installed in the *c10_location/logs* folder on every IBM Cognos BI computer that contains Content Manager or Application Tier Components. Because the log server uses a different port from the other IBM Cognos BI components, it continues to process events even if other services on the local computer, such as the dispatcher, are disabled.

The following workflow shows the tasks that are required to prepare for logging.

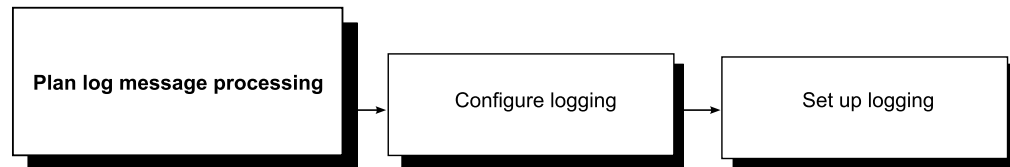


Figure 6. The workflow for implementing logging

- During planning, determine the logging configuration that is suitable for your environment. For example, evaluate various log message repositories, such as remote log servers and log files, such as the UNIX or Linux syslog or the Windows NT Event log, in addition to the local log file. You can also send only audit logging information to a database. Consider security, such as methods available for protecting log files from system failures and user tampering. For information about planning, see the *IBM Cognos Business Intelligence Architecture and Deployment Guide*.
- During configuration, define the startup properties for logging, such as connection settings for databases. You must also create a logging database if you plan to collect audit logs. If communication between a local log server and a remote log server must be secured, make the appropriate configuration changes on both IBM Cognos BI computers. You can also enable certain logging features, such as user-specific logging. For information about configuring logging, see the *IBM Cognos Business Intelligence Installation and Configuration Guide*.
- When setting up logging, specify the level of detail to log to focus messages on the information that is relevant in your organization. Audit reports may also be set up to track user and report activity. For information about setting up logging, see the *IBM Cognos Business Intelligence Administration and Security Guide*.

For information about using log messages to solve problems and resolving logging-related issues, see the *IBM Cognos Business Intelligence Troubleshooting Guide*.

Planning Log Message Repositories in a Distributed Installation

Distributed installations of IBM Cognos BI have more than one log server. With distributed installations, you can send log information to a central location. For example, you can configure IBM Cognos BI to send log information to a common log server. This log server sends the log information to a single repository on the same or a different computer, as shown in the following diagram.

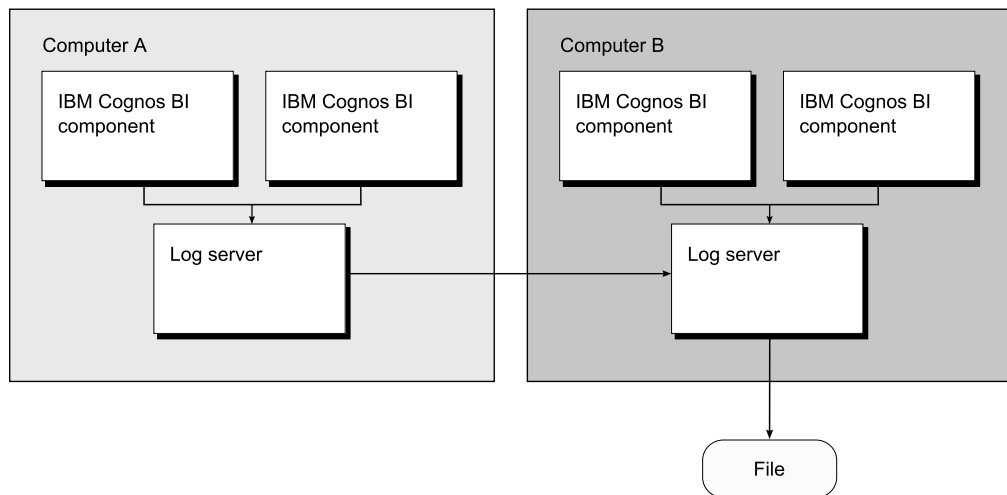


Figure 7. A distributed installation of IBM Cognos software where multiple computers are using the same log file location

You can also configure IBM Cognos BI to send audit log information from each log server to a common database. The common database can be on the same computer as one of the log servers, or on a different computer.

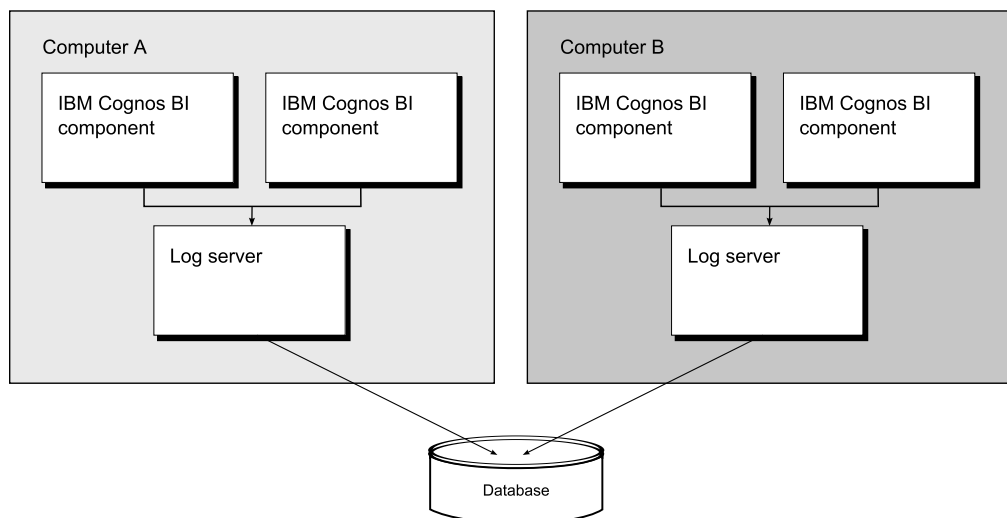


Figure 8. A distributed installation of IBM Cognos software where multiple computers are using the same logging database

The local log server provides failover and recovery processes in the following three circumstances:

- When the local log server is configured to send log information to a remote log server that is not available, log information from the local log server is stored in local recovery files. When the remote log server becomes available, an automatic recovery process moves information from the local recovery files to the remote log server, and deletes the local recovery files.
- When local IBM Cognos BI components are configured to communicate with the local log server using a TCP connection and this connection is not available, log information for these local components is stored in local recovery files. When the

TCP connection becomes available, an automatic recovery process moves information from the local recovery files to the remote log server, and deletes the local recovery files.

- When a log server is configured to send audit log information to a database, and the connection between the log server and the database fails, no information is logged in the database. When the connection is restored, information about the connection failure and restoration is stored in the local log file, if it exists, and the log server resumes sending new log information to the database. This information stored in the local log file is not stored in the logging database.

For information about specifying where to send log messages and configuring TCP connections, see the *IBM Cognos Business Intelligence Installation and Configuration Guide*.

Recommendation - Consolidate Log Messages in a Distributed Environment Using a Remote Log Server

In a default configuration, the local log server on each Content Manager or Application Tier Components computer writes log messages to a local file. Configurations that consolidate the contents of individual log files may improve usability and performance.

Consider consolidating log messages produced on each IBM Cognos BI computer by sending them to a remote log server. Configure the remote log server to send all messages to a single log file or to send audit logs to a database. For more information, see “Planning Log Message Repositories in a Distributed Installation” on page 21.

Log messages may be easier to interpret if all messages from each IBM Cognos BI computer appear in a consolidated location. For example, the log messages can then be sorted by their timestamp to determine the order in which events on various IBM Cognos BI computers occurred.

If you are using a database to capture audit log messages, performance may be improved if you route all audit log messages to a single log server that sends messages to the database. If a single log server is not used, the local log server on each IBM Cognos BI computer would require its own connection to the database.

Another benefit of using a single log server with a database is that configuration changes to the database are easier to maintain. You must update the configuration of only the remote log server.

Recommendation - Configure a Log File for Each Log Server

Configure a log file for each remote log server. Log files can provide important diagnostic and backup information if a communication issue occurs between a log server and the log message repository. For example, the TCP/IP connection between a local log server and a remote log server may become unavailable or a logging database may fail.

For local log servers, do not remove the default log files, even if you specify another repository for log messages, such as a database or remote log server. If the log messages may contain sensitive information, ensure that the log files on each computer are secured appropriately.

If a communication issue occurs, the local log server writes the log messages that it receives to the local log file. This action means that log messages are not lost when they cannot be written to a repository that is no longer available. As well, the log server writes information to the log file about the communication issue, which may help diagnose the problem. For example, if a database becomes unavailable, the log file contains information about when it failed, as well as when it recovered, if applicable.

Database Connection Management

IBM Cognos BI uses databases for several purposes: content store database, query database, or metric store database.

For some types of databases, such as Oracle, API client software must be installed and configured on each IBM Cognos BI server.

Content Store Database

The Content Manager service accesses the content store. Content Manager uses one database connection per request. Content Manager creates new database connections as required, pools connections, and reuses existing connections when possible. Content Manager maintains all database connections for the duration of the Content Manager operation. The theoretical maximum number of concurrent Content Manager requests equals the number of requests accepted by the Java application server or WebSphere Application Server Liberty Profile (the default application server).

When other IBM Cognos services are on the same computer as Content Manager, requests may be divided between Content Manager and the other services. In this case, the number of connections available to Content Manager may be fewer than the maximum possible connections.

Query Databases

The IBM Cognos BI server computer accesses the query databases. You can configure the maximum number of query database connections available to the IBM Cognos BI server computer, and the duration that connections are retained. A cleanup thread examines the connections every minute. Any connection that has been inactive longer than the time-out value is removed.

Inactive query database connections can be claimed by a new request. This occurs when the maximum number of connections has been reached and none of the inactive connections can be used by the new request. In this case, the oldest inactive connection is terminated and a new connection is created. A query database connection is only reused when the database credentials of the connection match those of the new request.

If the maximum number of connections is reached, and all are active, additional requests fail.

Metric Store Databases

A metric store database is a special case of a query database. A metric store database is used to store the information associated with metrics that appear in scorecards, including

- targets
- performance metrics

- thresholds
- membership in scorecards
- links to related reports, initiatives, and counter measures

Metric Studio accesses the metric store database. Metric Designer is used to define jobs that extract data from other query databases and populate the metric store database, although you can also manually create processes to do this.

Microsoft .NET Framework Interactions

Microsoft .NET Framework allows managed-code applications to interact with server-based applications through the use of Web services. IBM Cognos BI uses Microsoft .NET Framework to enable users' computers to interact with IBM Cognos BI server components for access to IBM Cognos BI for Microsoft Office and its features.

IBM Cognos BI for Microsoft Office is a managed-code application that takes advantage of the Microsoft .NET Framework. IBM Cognos BI for Microsoft Office functions like a Microsoft Office plug-in, but is installed, configured, and deployed as a managed-code application.

IBM Cognos for Microsoft Office uses Microsoft .NET Framework to allow users to interact with server-based components. Microsoft .NET Framework and the required updates are downloaded and installed by the setup file when you install IBM Cognos for Microsoft Office. The setup file must be run on all user computers.

For a list of supported versions of Microsoft .NET Framework, see the IBM Software Product Compatibility Reports page (www.ibm.com/support/docview.wss?uid=swg27042164).

The Microsoft .NET Framework does not have to be installed on your IBM Cognos BI server. IBM Cognos BI for Microsoft Office can run on any supported IBM Cognos BI server platform.

For information about configuring IBM Cognos BI for Microsoft Office, see the *IBM Cognos Business Intelligence Installation and Configuration Guide*.

Port Usage

All communication between IBM Cognos BI components, except for IBM Cognos Content Database and log server communication, can take place through one incoming port. This is true whether components are on the same computer or on different computers and whether communication is all non-SSL protocol or all SSL protocol. The default port number is 9300.

If IBM Cognos BI is configured to use a combination of non-SSL protocol and SSL protocol, communication takes place through two ports. You can use the default port for the non-SSL protocol communication and use a different port, such as 9334, for the SSL protocol communication.

Log server communication must take place through a unique port. The default port is 9362. You can configure log server communication to use either non-SSL or SSL protocol.

Framework Manager, Metric Designer, and IBM Cognos Transformer can communicate with the IBM Cognos BI server using either of two routes: through the Web server gateway, or directly to the Application Tier Components dispatcher. For more information see “Modeling Tool Installation Options” on page 59.

Communications with other software products, such as databases and authentication providers, use the ports required by those products.

For information about using SSL and specifying where to send log messages, see the *IBM Cognos Business Intelligence Installation and Configuration Guide*.

Request Flow Processing

Request flow describes internal IBM Cognos BI responses to user requests. In general, browser requests go through the IBM Cognos BI Web gateway and are sent to a dispatcher. Before any processing is performed by the dispatcher, the request is validated by IBM Cognos Application Firewall. A passport is attached to each request as a record of a valid user session.

Simple Object Access Protocol (SOAP) requests can be directed to either the IBM Cognos BI Web gateway or the dispatcher. For more information, see the *IBM Cognos Business Intelligence Installation and Configuration Guide*.

There are hundreds of types of requests and responses in IBM Cognos BI. To illustrate request flow, this section describes how IBM Cognos BI responds to a request.

Accessing IBM Cognos BI

A user can request anonymous or authenticated access to IBM Cognos BI. Anonymous access can be enabled or disabled for IBM Cognos BI.

For more information see “IBM Cognos Authentication Services” on page 108.

Anonymous Access

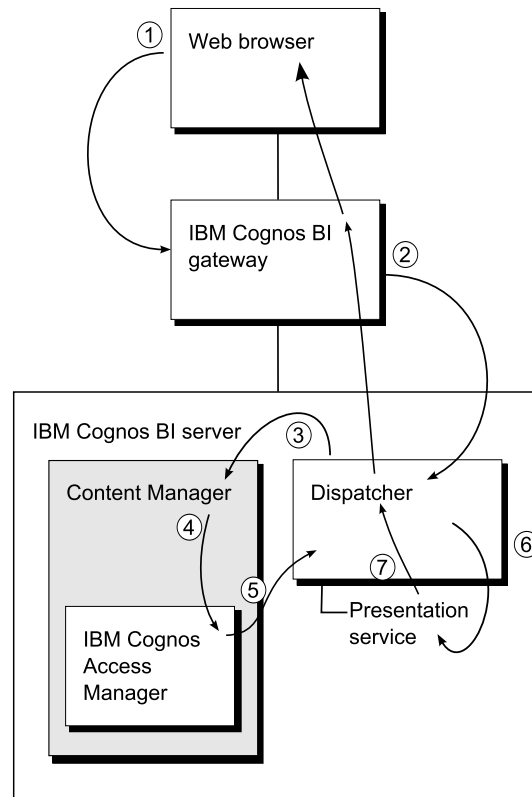


Figure 9. The interaction of services for an anonymous access request.

When a user requests anonymous access to IBM Cognos BI, the following occurs:

1. The user attempts to access the IBM Cognos BI Welcome page or any other IBM Cognos BI user interface from a Web browser, sending a request to the IBM Cognos BI gateway.
2. The IBM Cognos BI gateway accepts the request and sends it to a dispatcher.
3. The dispatcher notes that there is no passport attached to the request, and sends the request to Content Manager.
4. Content Manager sends the request to Access Manager.
5. Anonymous access is enabled in this IBM Cognos BI system, so a passport is attached to the request and the request is returned through Content Manager to the dispatcher.
6. The dispatcher processes the request and sends it to the presentation service.
7. The presentation service sends the Welcome page back through the dispatcher and the gateway to the user.

Authenticated Access

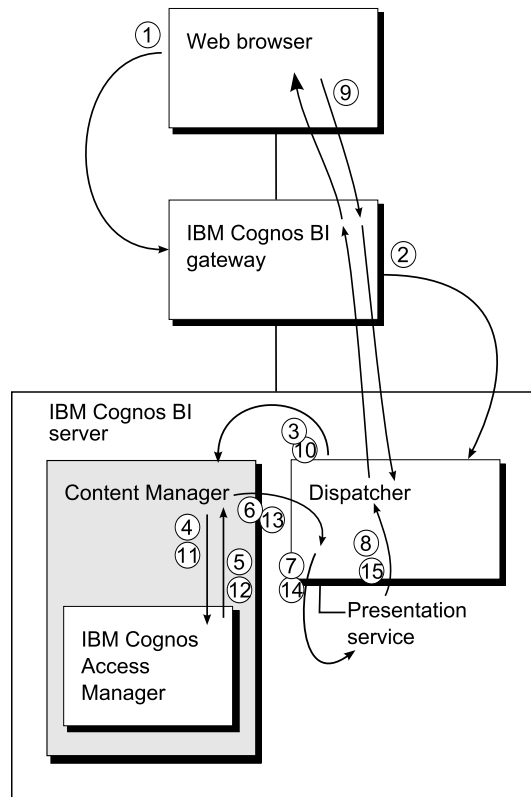


Figure 10. The interaction of services for an authenticated access request.

When a user requests authenticated access to IBM Cognos BI, the following occurs:

1. The user attempts to access the IBM Cognos BI Welcome page or any other IBM Cognos BI user interface from a Web browser, sending a request to the IBM Cognos BI gateway.
2. The gateway accepts the request and sends it to a dispatcher.
3. The dispatcher notes that there is no passport attached to the request and sends the request to Content Manager.
4. Content Manager sends the request to Access Manager.
5. Anonymous access is disabled in this IBM Cognos BI system, so Access Manager sends the request back to Content Manager with a fault attached. The fault contains information about what is needed to log on. For example, if there are multiple namespaces, the user may be required to select a namespace. If there is only one namespace, the user may be required to provide a user ID and password.
6. Content Manager returns the request with the attached fault to the dispatcher.
7. The dispatcher sends the request to the presentation service.
8. The presentation service creates the appropriate logon page for the user, and returns the page through the dispatcher and the gateway to the user.
9. The user enters the required information, such as a user ID and password. The information is attached to the original request and sent through the gateway to the dispatcher.
10. The dispatcher sends the request to Content Manager.

11. Content Manager sends the request to Access Manager.
12. If all the required information is correct, Access Manager issues a passport, attaches it to the original request, and sends the request back to Content Manager. If the required information is incorrect or incomplete, then the request faults back to step 9.
13. Content Manager sends the request to a dispatcher.
14. The dispatcher processes the request and sends it to the presentation service.
15. The presentation service sends the Welcome page back through the dispatcher and the gateway to the user.

Viewing a Report or Analysis

Reports and analyses can be viewed in IBM Cognos BI in different formats, including HTML and PDF.

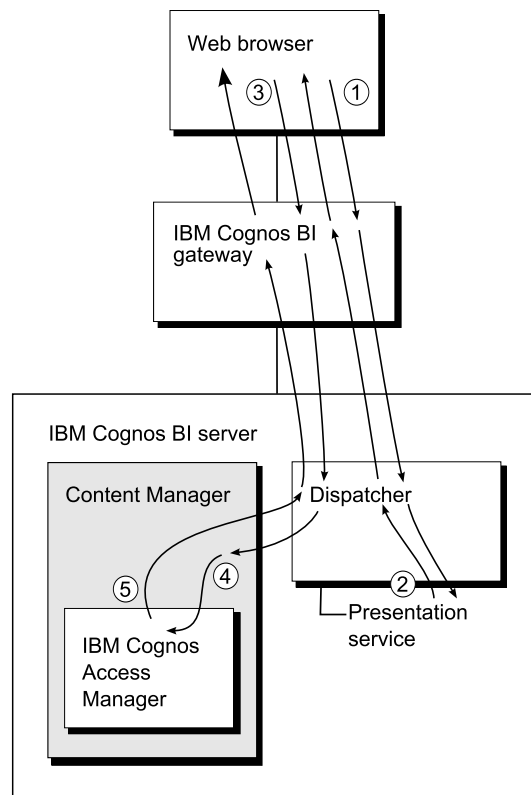


Figure 11. The interaction of services when viewing a report or analysis

When an authenticated user views a saved HTML or PDF report or analysis through IBM Cognos Connection, the following occurs:

1. The user clicks a report or analysis to view it, and the request goes through the gateway and the dispatcher to the presentation service.
2. The presentation service returns the Cognos Viewer through the dispatcher and gateway to the browser. The Cognos Viewer has an HTML frame that shows the report or analysis page. The data view of the page contains a URL to a Content Manager object to be displayed.
3. The browser sends the URL through the gateway and dispatcher to Content Manager.

4. Content Manager checks with Access Manager to see whether the user has read privileges for the report or analysis. To do this, Content Manager sends Access Manager the access control lists for the report or analysis, the attempted action (read), and the user information.
5. Access Manager determines that the user can perform the action, and Content Manager sends the report or analysis in the form of an HTML page or PDF document through the dispatcher and gateway to the user. When serving a PDF report or analysis, byte serving is used.

Running a Report or Analysis

You can run a report or analysis in HTML or PDF format.

Running an HTML Report

When the user presses page down or page bottom in the browser, the same path is followed again. The request has a high state of request affinity to ensure that it is routed to the same report service for additional rows of data. The report is cached so that the process does not have to restart.

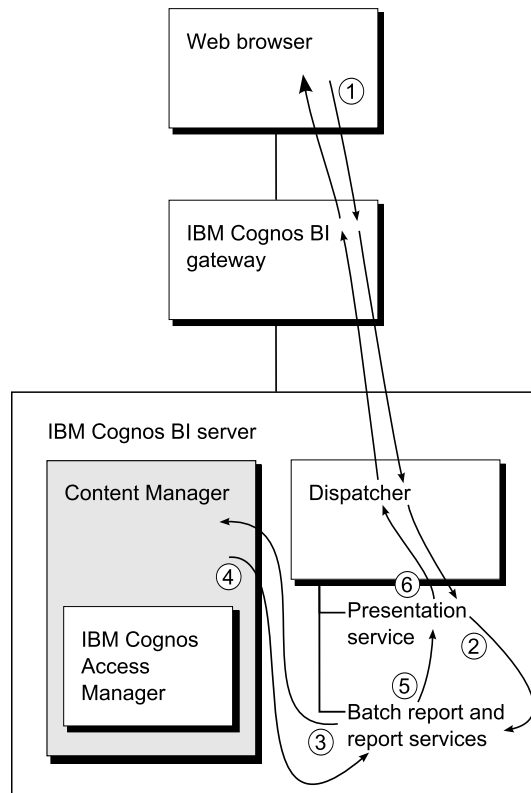


Figure 12. A diagram showing how the services interact when running an HTML report

When a user runs an HTML report or analysis through IBM Cognos Connection, the following occurs:

1. The user clicks a report or analysis to run it, and the request goes through the gateway and the dispatcher to the presentation service.
2. The presentation service sends the request to the report service through the dispatcher.
3. The report service requests the report or analysis and metadata from Content Manager, through the dispatcher.

4. Content Manager sends the report or analysis XML specifications and metadata to the report service. Content Manager refreshes metadata only when IBM Cognos BI is stopped and restarted or the model is updated and republished.
5. The report service returns one of these results to the presentation service:
 - an error page
 - a not ready page
 - a page of an HTML report or analysis
6. The presentation service sends one of these results through the dispatcher and gateway to the browser:
 - an error page
 - a wait or cancel page
 - a page of a completed HTML report or analysis in the Cognos Viewer interface

Running a PDF Report or Analysis

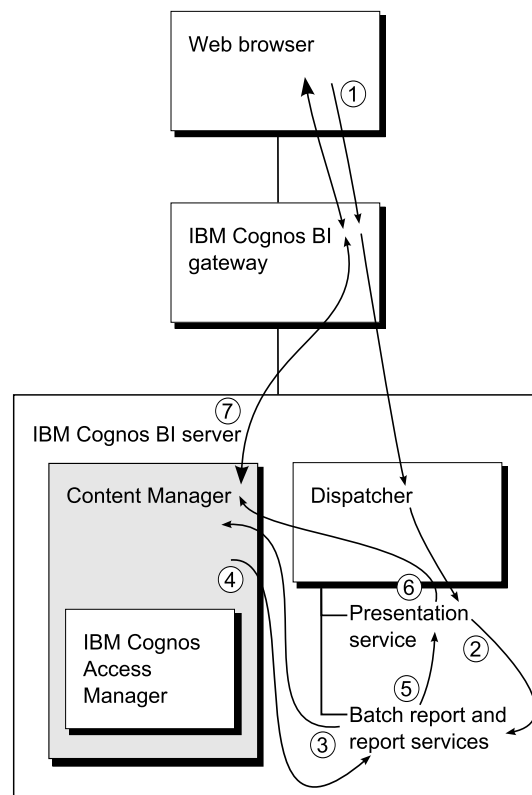


Figure 13. A diagram showing how services interact when running a PDF report.

When a user runs a PDF report or analysis through IBM Cognos Connection, the following occurs:

1. The user clicks a report or analysis to run it, and the request goes through the gateway and the dispatcher to the presentation service.
2. The presentation service sends the request to the report service through the dispatcher.
3. The report service requests the report XML specification and metadata from Content Manager, through the dispatcher.

4. Content Manager sends the report XML specification and metadata to the report service. Content Manager refreshes metadata only when IBM Cognos BI is stopped and restarted or the model is updated and republished.
5. The report service returns one of these results to the presentation service:
 - an error page
 - a not ready page
 - a PDF report or analysis
6. The presentation service sends the PDF result to Content Manager for storage in the user's session temporary area. Byte serving is used.
7. The wait/cancel page polls every few seconds to see if the report or analysis is complete. When it is complete, the Cognos Viewer HTML frame content is replaced with the PDF. A request is sent through the gateway and the dispatcher to the Content Manager and back with the PDF.

Scheduling a Task to Run

You can schedule a task to run for a report, query, analysis, data integration, agent, job, import, export, or content management.

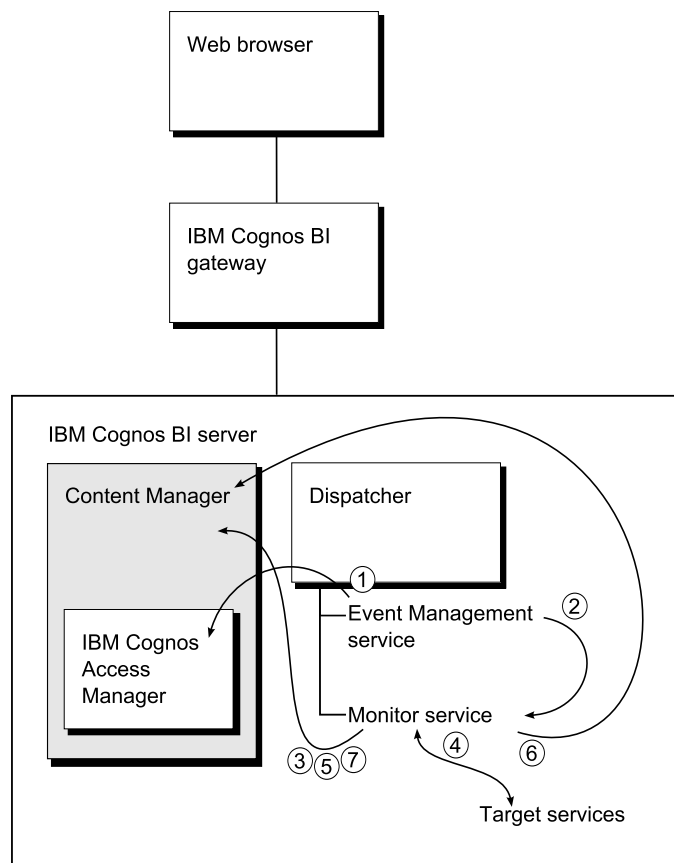


Figure 14. A diagram showing how services interact when scheduling a task

When a scheduled task runs, the following occurs:

1. At the scheduled time, the event management service sends a trusted request to Content Manager, via the dispatcher, to retrieve the user credentials, and then logs on as the user to obtain the user passport.

2. The event management service sends a request to the monitor service to run the scheduled task through the dispatcher. This request is a background request, and the conversation between the event management service and the monitor service ends.
3. The monitor service sends a request to Content Manager through the dispatcher to create a history object. This object is required to ensure that the correct status appears in the user interface.
4. The monitor service forwards the run request to the relevant service through the dispatcher and maintains the asynchronous protocol with the target service.
5. The monitor service updates the status of the history as "execution".
6. When the task completes, the target service stores any relevant information in Content Manager and ends communication with the monitor service. Information stored in Content Manager may include report output, agent event lists, and so on.
7. The monitor service detects the final state of the task run and updates the history object with a status that indicates whether the task was successful.

Opening IBM Cognos Connection Folder

IBM Cognos Connection is a Web portal that comes with IBM Cognos BI. You can also integrate IBM Cognos BI with your corporate Web portal.

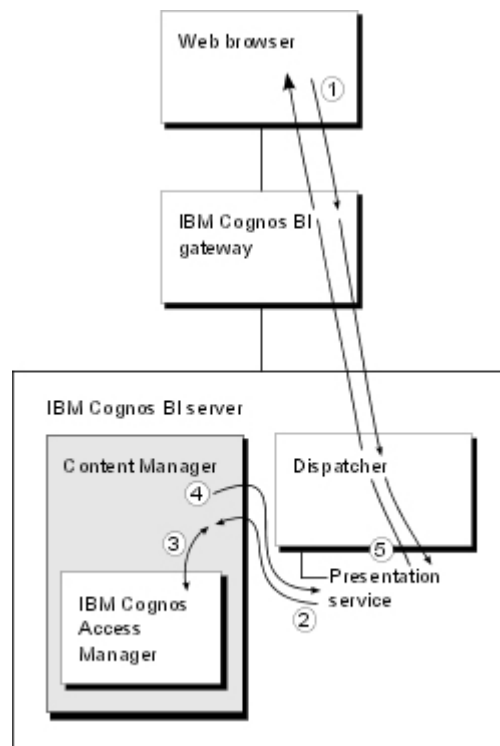


Figure 15. A diagram showing how services interact when opening a folder

When a user opens a folder in IBM Cognos Connection, the following occurs:

1. The user clicks a folder to open it, and the request goes through the gateway and the dispatcher to the presentation service.
2. The presentation service sends the request to Content Manager through the dispatcher.

3. Content Manager checks with Access Manager to determine whether access is granted.
4. Content Manager sends the folder contents or an error message to the presentation service.
5. The presentation service formats the appropriate HTML page and sends it through the dispatcher and the gateway to the user.

Running an Agent

You can run agents to monitor your data and detect occurrences of business events.

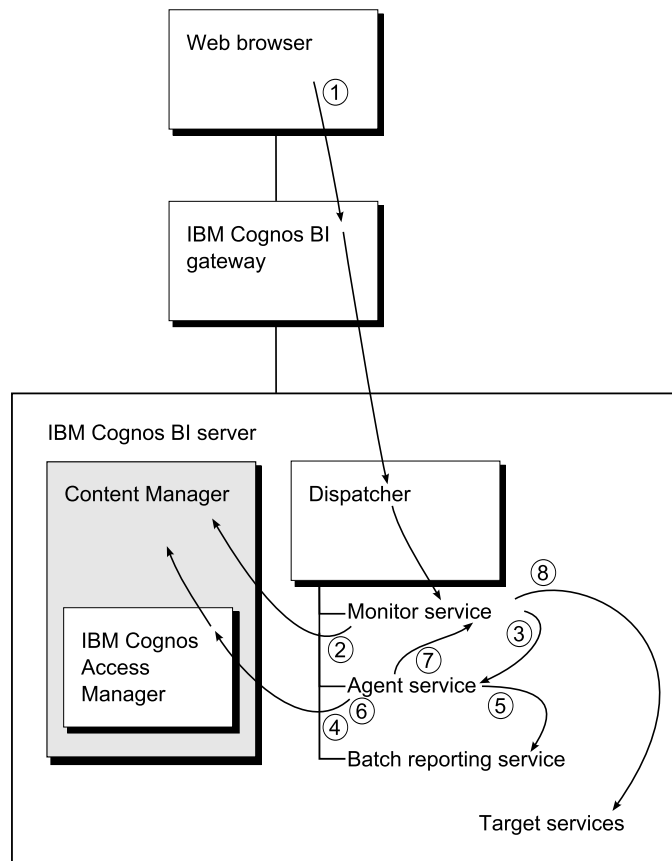


Figure 16. A diagram showing how services interact when running an agent

When the user clicks an agent's run link, the following occurs:

1. The request goes through the gateway and the dispatcher to the monitor service.
2. The monitor service authenticates the request and creates a history in Content Manager for the agent run.
3. The monitor service forwards the request to the agent service. The monitor service maintains the asynchronous protocol (wait/cancel) on behalf of the gateway.
4. The agent service requests the agent definition and the previous agent event list from Content Manager.
5. The agent service executes the agent condition through the batch report service.

6. The agent service compares the generated result set with the previous event list, and creates and stores the updated agent event list in Content Manager.
7. Based on the authored agent tasks, the agent service executes its tasks through the monitor service.
8. The monitor service creates a history in Content Manager for each step and forwards the request (maintaining the asynchronous protocol) to the relevant service. For example, email messages are forwarded to the delivery service, reports are forwarded to the batch report service, and jobs are forwarded to the job service.

Indexing content

Administrators create and update the search index using an index update task in IBM Cognos Administration. When you create an index update task, you can run the task immediately, or define a schedule to run the task at a later time.

All communication between services is managed by dispatchers. The following diagram and description summarize the request flow by showing logical communication flow between services.

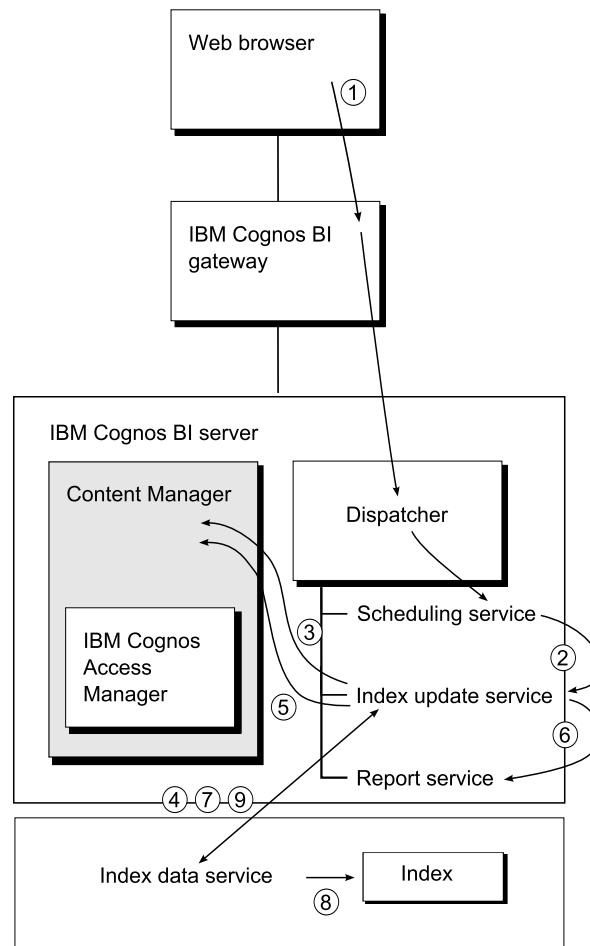


Figure 17. A diagram showing events when an index update is initialized

When you initiate an index update, the following occurs:

1. The index update request goes through the gateway and dispatcher to the scheduling service.

2. The scheduling service executes the index update task.
3. The index update service requests a capability check from Content Manager.
4. The index update service sends an index start request to the index data service.
5. Terms are extracted from Content Manager.
6. The index update service extracts all references to queryItems, then queries the report service for values.
7. The report service retrieves every unique query item instance used in all objects.
8. The index add request is sent to the index data service.
9. The index data service writes to the index.
10. Term extraction and writing to the index is repeated iteratively until the indexing is complete.
11. The index update service informs the scheduling service that the index update is complete.

Searching content

Users can run a full-text search from IBM Cognos Connection, IBM Cognos Analysis Studio, IBM Cognos Query Studio, or IBM Cognos Viewer.

When a search is run, one of two check methods is applied: Content Manager security check or internal security check. To use the internal security check, select **Index Access Control List** in **Index, General**, in **Search, General**, and in **Storage, General**. If all three settings do not match, the Content Manager security check is used.

All communication between services is managed by dispatchers. The following diagrams and descriptions summarize the request flows by showing the logical communication between the services.

Content Manager Security Check

This method checks the security of Content Manager items referenced in the result set each time a search is run. The Content Manager security check is used for searching if **Index Access Control List** is set to false.

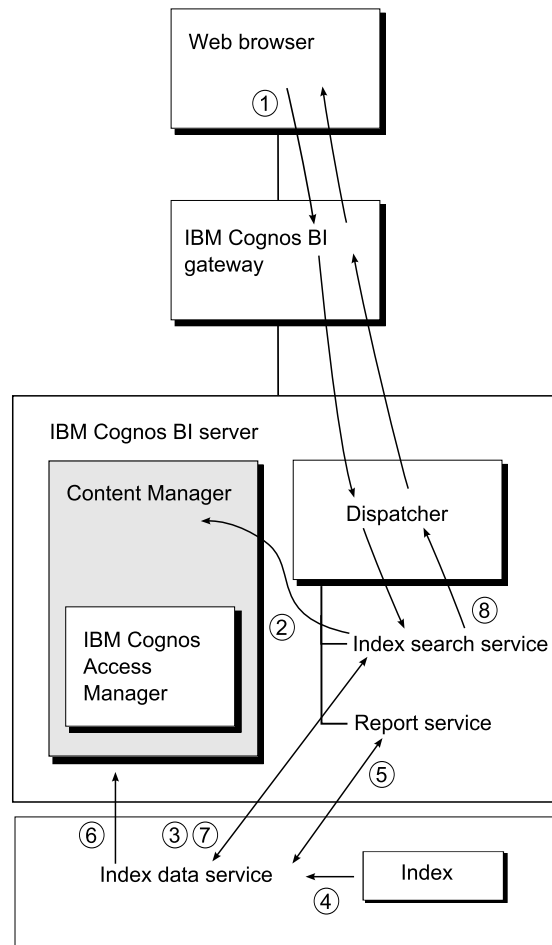


Figure 18. A diagram showing events in a full-text search that has the index access control list set to false

When a user runs a full-text search and **Index Access Control List** is set to false, the following occurs:

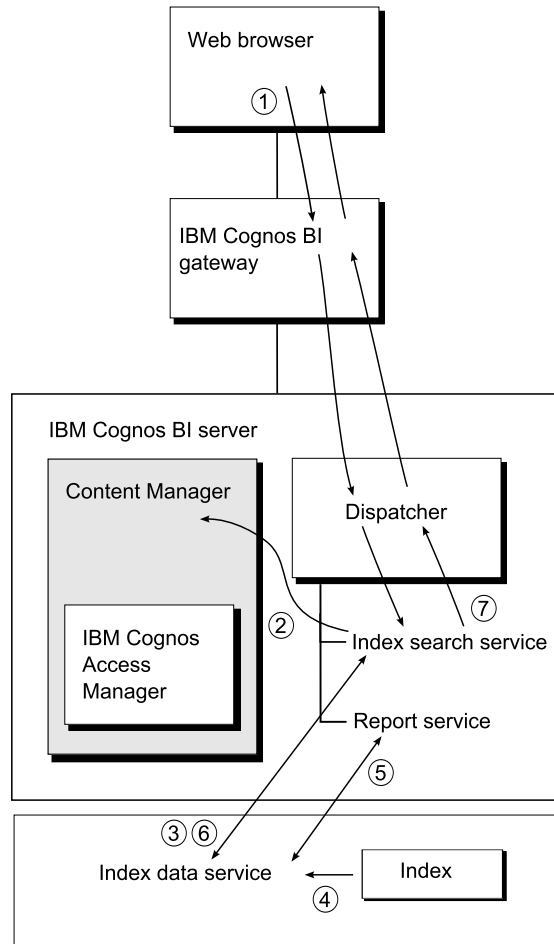
1. The search request is sent to the index search service.
2. The index search service requests a capability check from Content Manager.
3. The search request is sent to the index data service.
4. The result set is extracted from the index.
5. The security of metadata and sample data referenced in the result set is checked. This step is dependent on the Secure refinement results index data service setting.
6. The security of Content Manager items referenced in the result set is checked.
7. The filtered result set is returned to the index search service.
8. The result set is returned to the user.

Internal Security Check

This method checks the security of items referenced in the result set based on an internal check of the cached access control list.

The access control list is created when you generate or update an index. The internal security check is faster than the Content Manager security check. To capture ongoing security changes, run frequent incremental index updates. The

internal security check is used for searching if **Index Access Control List** is set to true. This is the default approach.



When a user runs a full-text search and **Index Access Control List** is set to true, the following occurs:

1. The search request is sent to the index search service.
2. The index search service requests a capability check from Content Manager.
3. The search request is sent to the index data service.
4. The result set is extracted from the index based on an internal security check in the index.
5. The security of metadata and sample data referenced in the result set is checked. This step is dependent on the Secure refinement results index data service setting.
6. The filtered result set is returned to the index search service.
7. The result set is returned to the user.

Figure 19. A graphic showing events in a full-text search that has the index access control list set to true

Portal Pages

Whether you are using IBM Cognos Connection or another portal, all IBM Cognos functionality is available on the BI Bus. You can search for reports and view them in the portal and perform additional analysis, if needed. You can also monitor, configure, and administer IBM Cognos users and content using the portal. Whether

you are working with reports or performing administration tasks, requests are sent to the BI Bus and then forwarded to the appropriate IBM Cognos service for processing.

The following IBM Cognos functions are commonly provided through portlets:

- Cognos Navigator retrieves selected content.
- Cognos Search finds and opens published content.
- Cognos Viewer shows content selected in Cognos Navigator or Cognos Search.

For each portlet, all security permissions and credentials are inherited and passed along through the request. For example, if you go to a particular folder or search for a particular object, only those objects that you have permission to view are returned. Similarly, if you click a report in the Cognos Navigator or Search portlet, the report identifier and security credentials are included with the request. You can view the report in either the same portlet or a new portlet, but only the data that you have access to will appear.

Chapter 4. Workflow

The series of tasks that people in your organization will perform to understand, install, configure, and use IBM Cognos Business Intelligence include the following:

- planning for implementation
Implementation planning should be done before installing and configuring IBM Cognos BI. It is typically carried out by a team assembled and led by the business intelligence solutions architect.
- installing and configuring IBM Cognos BI
Technical personnel install and configure IBM Cognos BI, typically under the direction of the business intelligence solutions architect.
- administering IBM Cognos BI
Administrators establish and maintain security, set up multilingual capabilities, install fonts, manage report distribution, and perform ongoing administration.
- working with models and packages to author reports and analyses for viewing
Modelers create one or more metadata models, and use those models to publish packages that can be used to author reports and analyses.
Authors use published models to create and maintain reports and analyses.
Report users view and print reports and analyses through IBM Cognos Connection. For more information, see the *IBM Cognos Connection User Guide*.
Mobile report users view reports with a IBM Cognos Mobile client application.
Authors and report users import report data to Microsoft Office workbooks and presentations using IBM Cognos BI for Microsoft Office.
- creating scorecarding applications and monitoring metrics
Scorecard authors create packages that contain connection, report, and maintenance task information. Authors then deploy, maintain, and access scorecard applications in Metric Studio.
Business users use metrics to monitor and analyze performance in key business areas. For more information, see the *Metric Studio User Guide*.
- creating Transformer models and PowerCubes
Modelers create one or more metadata models and then use those models to create PowerCubes that can be used in reporting and analysis
- managing events
Users create agents to monitor data and detect occurrences of business events.

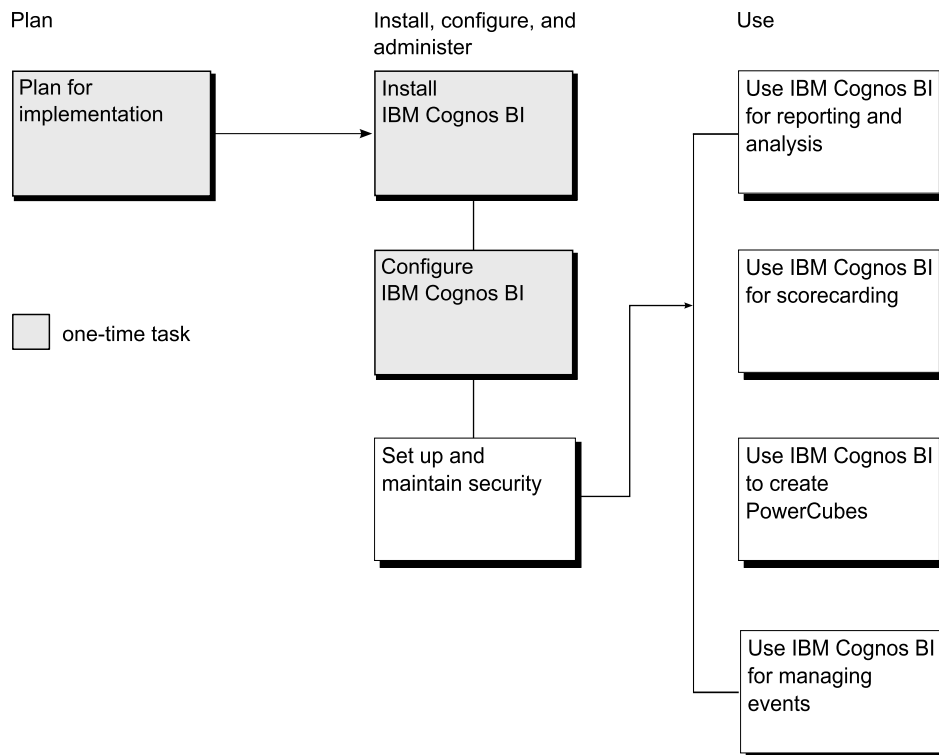


Figure 20. Workflow to understand, install, configure, and use IBM Cognos Business Intelligence software

Planning for Implementation

Implementing IBM Cognos Business Intelligence means installing and configuring it to integrate effectively with your existing infrastructure.

To ensure that IBM Cognos BI is implemented effectively, it is important to plan your implementation carefully. For information about implementation planning, see the implementation planning checklist available in Chapter 5, “Implementation Planning Checklist,” on page 51.

Installing IBM Cognos Business Intelligence

Installing IBM Cognos BI is typically done by Information Technology personnel under the direction of the business intelligence solutions architect.

When you install IBM Cognos BI using the **Installation** wizard, you specify where to install each of these components:

- gateways
For more information, see “Tier 1. Web Server: IBM Cognos BI Gateways” on page 9.
- Application Tier Components
For more information, see “Tier 2. Applications: IBM Cognos BI Servers” on page 10.
- Content Manager
For more information, see “Content Manager” on page 14.

You can install the components on one computer, or distribute them across a network. Before installing IBM Cognos BI, choose the appropriate installation and configuration option Chapter 6, “Installation Options,” on page 53.

You must also install Framework Manager, a Microsoft Windows-based metadata modeling tool. The studio interfaces are HTML- and Java-based, and do not require installation.

You can choose to install optional Windows-based metadata modeling tools. If you plan to use IBM Cognos BI for scorecarding, you can install Metric Designer. If you plan to create PowerCubes in IBM Cognos BI, you can install IBM Cognos Transformer.

Unattended Installation

If you plan to install an identical IBM Cognos BI configuration across several computers on a network, or to install multiple configurations, you can set up and run an unattended installation.

This is a noninteractive method of installing and configuring IBM Cognos BI in which all the tasks run automatically, without user intervention. You can run the unattended installation as part of a script, or from the command line.

An unattended installation is useful if you must install IBM Cognos BI at different geographic locations, some of which have no technical personnel to perform the installation.

For more information, see the *IBM Cognos Business Intelligence Installation and Configuration Guide*.

Configuring IBM Cognos Business Intelligence

One of the tools installed with IBM Cognos BI is IBM Cognos Configuration. You use it immediately after installation to set the initial IBM Cognos BI configuration. Some of the things you can configure are

- logging

You can specify the destination log for messages generated by IBM Cognos BI. For more information, see “Log Message Processing” on page 20.

- security

You can run IBM Cognos BI with or without security. By default, the only security that is enabled is IBM Cognos Application Firewall. If you want to set up security, you should configure security settings immediately after installing IBM Cognos BI. For more information, see Chapter 10, “Security Architecture,” on page 107.

- data access

You must specify database connection information for the IBM Cognos BI content store. For more information, see “Accessing IBM Cognos BI” on page 26.

Following initial configuration, if a property changes or components are added, you can use IBM Cognos Configuration to reconfigure IBM Cognos BI.

For information about initial configuration, see the *IBM Cognos Business Intelligence Installation and Configuration Guide*.

Monitoring Configuration Changes

Each time you save a configuration after making changes, date-stamped versions of these two configuration files are automatically saved in the *c10_location/configuration* directory:

- cogstartup.xml

This file records configuration settings. An example is *cogstartup_200211231540.xml*

- coglocale.xml

This file records locale settings used for multilingual reporting. An example is *coglocale_200211261401.xml*

If you are unable to save a configuration, or you have problems with a configuration, you can revert to a previous configuration file. You can use the files to review your configuration history. Before calling Cognos Software Services for help, print a history of the configuration changes made in IBM Cognos BI.

For more information about the cogstartup.xml and coglocale.xml files, see the *IBM Cognos Business Intelligence Installation and Configuration Guide*. For information about troubleshooting, see the *IBM Cognos Business Intelligence Troubleshooting Guide*.

Configuring Security

IBM Cognos BI integrates with an existing security infrastructure to provide user authentication.

IBM Cognos BI can secure content by using the user and group definitions from your security system, without any changes required. An Cognos namespace is included to provide the optional ability to define additional groups for securing content. These groups can simplify security administration by including users and groups from one or more authentication providers.

IBM Cognos BI includes IBM Cognos Application Firewall, which is included with the dispatcher to validate and filter incoming and outgoing traffic at the dispatcher layer. By default, IBM Cognos Application Firewall is enabled.

IBM Cognos BI also provides an authorization facility for assigning permissions to users defined in the authentication provider. It also provides a standard certificate authority (CA) for setting up encryption. Enhanced capabilities are available separately upon request.

If you intend to set up security for IBM Cognos BI, it should be the first thing you do after installation. For information about setting up and maintaining security, see Chapter 10, “Security Architecture,” on page 107 and the *Administration and Security Guide*.

Configuring IBM Cognos Business Intelligence for Multilingual Reporting

IBM Cognos BI is a Unicode product capable of querying data in many languages and encodings. To facilitate multilingual reporting in IBM Cognos BI, you may have to install additional fonts and configure your users' Web browsers.

Installing Fonts

IBM Cognos BI uses fonts to render PDF reports and to render charts used in PDF and HTML reports. To show output correctly, fonts must be available where the report or chart is rendered. This may involve installing additional fonts on the IBM Cognos BI server, and on the personal computers of IBM Cognos BI users. If users specify a font that is not installed, IBM Cognos BI substitutes a default font. For more information, see “Adding Fonts to the IBM Cognos BI Environment” on page 99.

Configuring Browsers

IBM Cognos BI uses the default browser configurations of supported browsers. To ensure that IBM Cognos BI operates effectively, you should check your browser configuration settings and modify them if necessary. For information, see Chapter 9, “Globalization Considerations,” on page 97.

Administering IBM Cognos Business Intelligence

After IBM Cognos BI is installed and configured, you can use IBM Cognos Connection or your third-party portal to do the following:

- define users, groups, and roles for security purposes
- set up folders where reports are stored
- make reports available to business users
- monitor and administer servers and activities
- back up data
- maintain security
- deploy IBM Cognos BI from one environment to another

For information about using IBM Cognos Connection, see the IBM Cognos Connection *User Guide*. For information about administration, setting up sample report projects and models, and troubleshooting problems, see the *Administration and Security Guide* and *IBM Cognos Business Intelligence Troubleshooting Guide*.

Using IBM Cognos BI for Reporting and Analysis

The following diagram shows the complete reporting and analysis workflow for IBM Cognos BI.

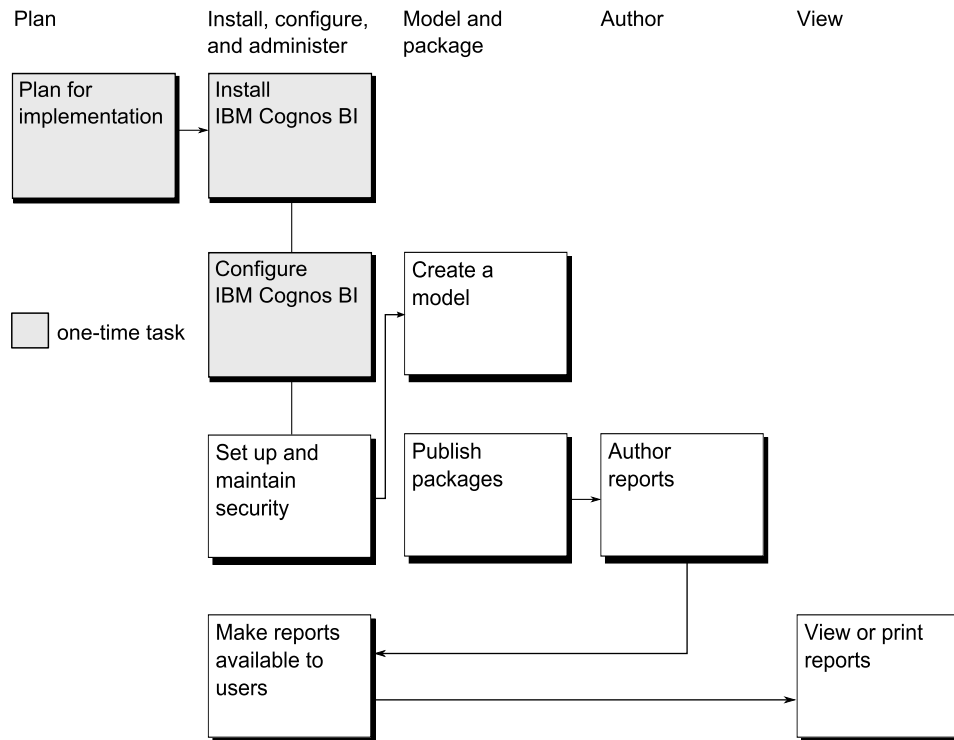


Figure 21. Reporting and analysis workflow for IBM Cognos BI software

Creating Reporting Models and Packages

A model serves as an insulating layer between IBM Cognos BI reporting users and the database. Packages are model subsets that ensure users are provided with data appropriate for the reporting they need to do, and that the data is structured in ways that make sense from a business perspective.

Creating models and publishing packages are tasks that should be planned carefully. Models and packages that are well-designed from the start ensure that user requirements are met, data is secure, and your IBM Cognos BI application can be easily administered.

To understand the modeling and packaging process, users can study the sample models, packages, and reports provided with IBM Cognos BI. For information about setting up the samples, see the *IBM Cognos Administration and Security Guide*.

For IBM Cognos BI reporting, models and packages are created using Framework Manager. The following topics provide an overview. For more information, see the *IBM Cognos Framework Manager User Guide*.

Modeling

Framework Manager is used to create a model that provides users with a single, integrated, business view of the database, and to provide IBM Cognos BI with information about how data is accessed, related, and secured.

A model that is designed to meet user requirements adds significant value to your data. It structures, adds to, and manages the data in ways that make sense to business users. Creating a model is an important task that should be planned and executed by a modeler or a modeling team familiar with both the database structure and the needs of your business users.

When you create a model, you

- specify the metadata to import from data sources defined in the IBM Cognos BI content store
- refine the metadata by adding business names, descriptions, multilingual values, calculations, filters, and other components
- specify joins and relationships
- organize the data for presentation in ways that make sense to business users and add value to your databases
- add security to the metadata to determine who can use the metadata and for what purposes

Packaging

After a model is created, packages are published to locations on the IBM Cognos BI server where report authors can use them to create reports. A different package, containing only the necessary information, can be published for each group of users.

Reports cannot contain data from more than one package. When publishing a package, it is important to ensure that the package contains all the data required to meet the needs of the intended users.

The hierarchical structure of a package controls the way in which folders, reports, and other data objects are structured in the interface used by the report author. It also controls how security is applied to the objects, and how easy it is to deploy the package to other environments. As a result, it is important to ensure that the structure of a package makes sense from the perspective of a business user, and not just from an administrative perspective.

Authoring Reports

IBM Cognos BI can be used to create many different types of reports, including lists, crosstab reports, charts, master and detail reports, and user-designed reports.

You create planned, professional reports in Report Studio, and ad hoc reports in Query Studio. You can explore and analyze data in Analysis Studio. You can use report data from Report Studio, Query Studio, and Analysis Studio in Microsoft Office applications through Cognos BI for Microsoft Office.

The IBM Cognos BI architecture is fully open to third-party products and to custom development. IBM Cognos BI can be integrated with existing transaction-based Web products or portals. For information about custom

development, see the *Software Development Kit Developer Guide*. For information about integrating IBM Cognos BI with other enterprise portals, see the *IBM Cognos Administration and Security Guide*.

Query Studio

Report authors and users create ad hoc reports using Query Studio. Ad hoc reports, also called ad hoc queries, can be created quickly, with little or no training, to meet reporting needs not covered by standard, professional reports.

Authors can save query specifications for future revision, or as templates for other new reports. Reports can be made available in interactive mode, so that users can expand them, or in read-only mode. Reports created in Query Studio can be viewed and edited in Report Studio.

Before creating ad hoc queries, users should complete the tutorial provided to familiarize themselves with best practices in report creation. For more information, see the *Getting Started Guide*.

For information about Query Studio, see the *IBM Cognos Query Studio User Guide*.

Report Studio

Report authors create professional reports using Report Studio. Planned reports are standard, professional reports designed to meet specific, recurring needs of business users. Authors can also use Report Studio to edit reports generated in Query Studio.

To create a report in Report Studio, an author specifies the model that will provide data for the report. The author then builds a report specification that defines the queries and prompts used to retrieve the data. The author also creates the layouts and styles used to present the data. In addition to creating new reports, authors can modify existing reports.

Before creating reports for corporate use, report authors should use the tutorial provided to familiarize themselves with best practices in report creation. For more information, see the *Getting Started Guide*.

For information about Report Studio, see the *IBM Cognos Report Studio User Guide*.

Analysis Studio

In Analysis Studio, users can explore, analyze, and compare dimensional data. Analysis Studio provides access to dimensional, OLAP (online analytical processing), and dimensionally modeled relational data sources. Analyses created in Analysis Studio can be opened in Report Studio and used to build professional reports.

Before creating an analysis, the administrator must have created a package in Framework Manager and published it to a location in the IBM Cognos Connection portal for user access. Users can then select the package and find the data they require for the analysis. Users may also choose to share findings with others.

For information about using Analysis Studio, see the *IBM Cognos Analysis Studio User Guide*.

IBM Cognos BI for Microsoft Office

Authors and report users may want to use data from IBM Cognos reports in Microsoft Office workbooks, documents, and presentations. In IBM Cognos BI for Microsoft Office, users can import or remove IBM Cognos report elements from Microsoft Excel workbooks, Microsoft Word documents, and Microsoft PowerPoint presentations. Users can run reports using the IBM Cognos studios and publish workbooks and presentations to IBM Cognos Connection.

For information about using IBM Cognos BI for Microsoft Office, see the IBM Cognos BI for Microsoft Office *User Guide*. For more information about configuring and deploying IBM Cognos BI for Microsoft Office, see the *IBM Cognos Business Intelligence Installation and Configuration Guide*.

Using IBM Cognos Business Intelligence for Scorecarding

The following diagram shows the complete scorecarding workflow for IBM Cognos Business Intelligence.

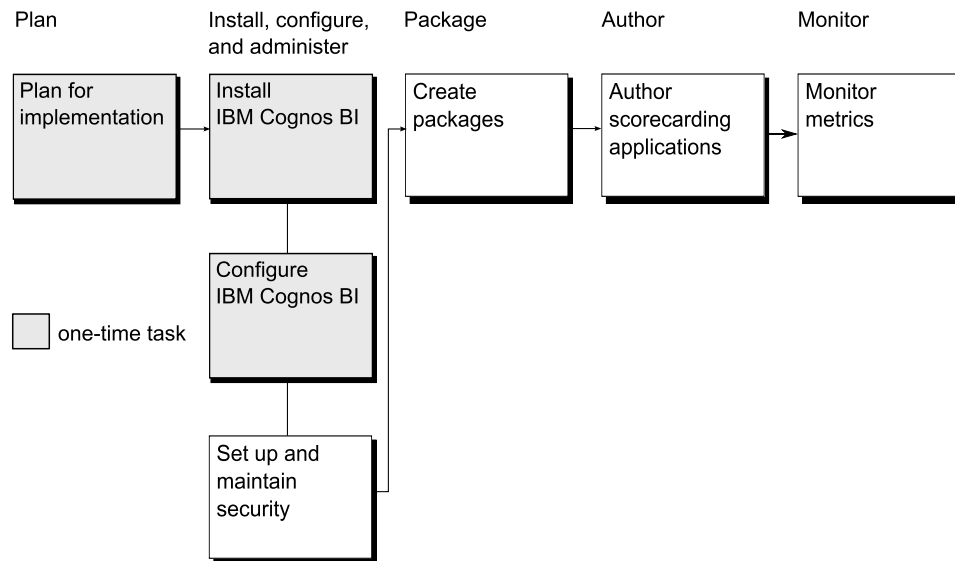


Figure 22. Scorecarding workflow for IBM Cognos Business Intelligence software

Packaging in Metric Studio

A metric package is an IBM Cognos Connection representation of a Metric Studio scorecarding application. A metric package contains connection information, reports, and metric management tasks for that application. The metric package content is stored in a metric store.

You must create a package the first time you access Metric Studio. You can create other packages in IBM Cognos Connection or Metric Studio. For more information, see the *IBM Cognos Metric Studio User Guide*.

Authoring Scorecarding Applications

A scorecarding application is a set of scorecards, metrics and projects used to monitor the performance of a specific aspect of an organization.

You create scorecarding applications using Metric Studio. You use a Metric Studio package to deploy, maintain and access a scorecarding application. For more information, see the *IBM Cognos Metric Studio User Guide*.

Using IBM Cognos Business Intelligence to Create PowerCubes

The following diagram shows the complete Transformer model and PowerCube workflow for IBM Cognos BI.

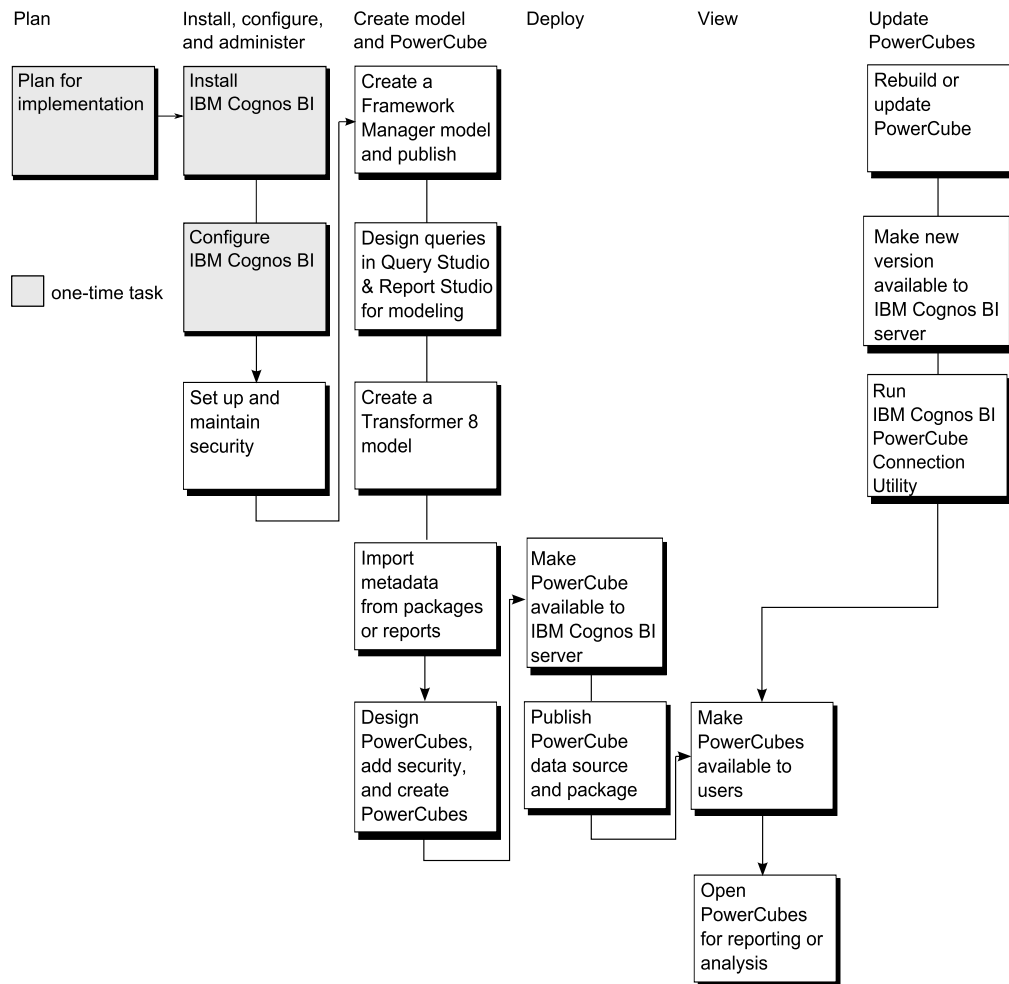


Figure 23. Transformer model and PowerCube workflow for IBM Cognos Business Intelligence software

Managing Events

An event is any situation that can affect the success of your business. To ensure that the appropriate personnel are made aware of an event, you create agents in Event Studio to monitor your data and detect occurrences of business events.

Chapter 5. Implementation Planning Checklist

To get the most from IBM Cognos Business Intelligence, you must implement it effectively. This means installing and configuring IBM Cognos BI so that it integrates with your information technology infrastructure and meets your reporting requirements.

To plan an effective IBM Cognos BI implementation, do the following:

- Familiarize yourself with the IBM Cognos BI architecture.
For more information, see the architecture section of this document. It will help you understand the components that make up IBM Cognos BI, their functions, and the ways in which they interact with each other, your infrastructure, and your authors and users.
- Decide how to install and configure IBM Cognos BI.
Know what your options are for installing and configuring IBM Cognos BI, and decide which best meet your needs. For more information, see Chapter 6, “Installation Options,” on page 53.
- Decide how to maximize IBM Cognos BI performance in your environment.
Understand the factors that can affect IBM Cognos BI performance, and plan to ensure and maintain adequate capacity, scalability, and availability for IBM Cognos BI in your environment. For more information, see Chapter 7, “Performance Planning,” on page 69.
- Decide how to configure IBM Cognos BI multilingual capabilities.
If you will use IBM Cognos BI in a global environment, decide how to configure IBM Cognos BI so that interface elements and report contents appear in the languages that users need. For more information, see Chapter 9, “Globalization Considerations,” on page 97.

When you complete your planning and are ready to install and use IBM Cognos BI, refer to the other IBM Cognos BI documents for step-by-step instructions.

Chapter 6. Installation Options

Before implementing IBM Cognos Business Intelligence, decide how you will install and configure it to provide the best possible performance. The installation and configuration choices that produce the best performance depend on your reporting requirements, resources, and preferences.

When you assess your installation options for IBM Cognos BI, you must consider whether you are installing the product for the first time or upgrading. For information about upgrading, see the *IBM Cognos Business Intelligence Installation and Configuration Guide*.

When you install IBM Cognos BI, you specify where to install the gateways, Application Tier Components, and Content Manager. You can install all IBM Cognos BI components on one computer, or distribute them across a network.

You must install Framework Manager, the metadata modeling application for business intelligence. You can choose to install optional metadata modeling applications such as Metric Designer for scorecarding and Transformer for creating PowerCubes.

IBM Cognos BI is compatible with other IBM Cognos products. If your environment includes other IBM Cognos products, you must consider how IBM Cognos BI will fit into that environment. For more information, see “IBM Cognos Business Intelligence with other IBM Cognos products” on page 61.

Installing All Components on One Computer

Install all components on one computer only for proof of concept or in demonstration environments where the user load is small. Because the gateway must be located with the Web server, the single computer must also be running a Web server.

In the following diagram, all IBM Cognos BI components are installed on one computer.

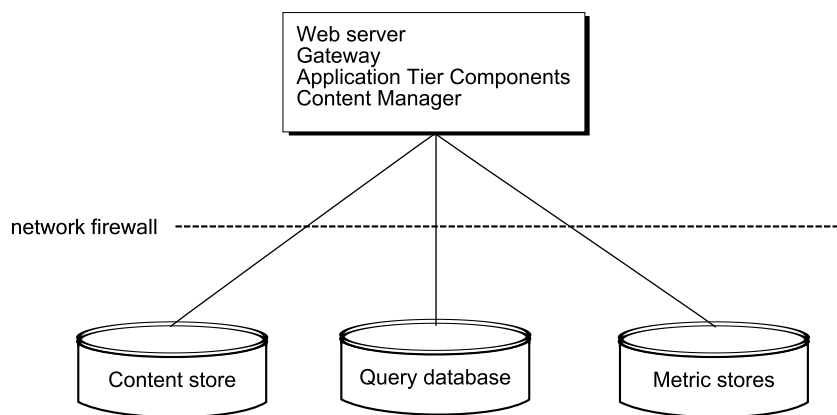


Figure 24. Installing all components on one computer

The following diagram provides a more detailed view of an IBM Cognos BI installation in which all server components are installed on a single computer. The modeling components, such as Framework Manager, Metric Designer, and Transformer, can be installed on different computers.

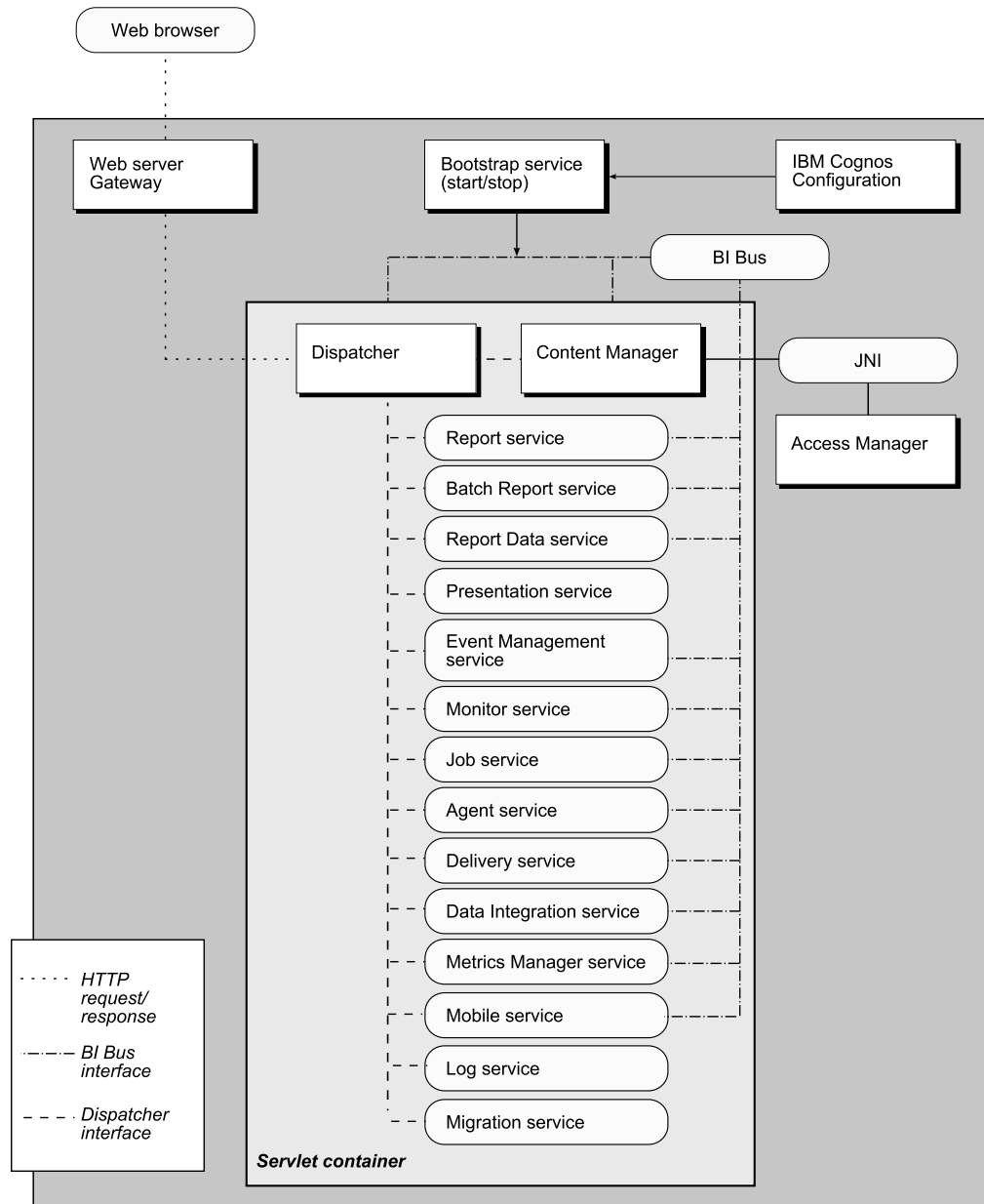


Figure 25. Installing server and modelling components on different computers

If IBM Cognos BI is installed on a Microsoft Windows operating system, you can install the modeling tools on the same computer. If IBM Cognos BI is installed on a UNIX or Linux operating system, you must install the Windows-based modeling tools on a separate computer that runs under Windows.

Installing the Gateway on a Separate Computer

You can install the gateway and a Web server on one computer, and install the remaining IBM Cognos BI components on other computers. If you have a Web farm, you may want to install an IBM Cognos BI gateway on each Web server. Using multiple Web servers to manage incoming requests provides a better level of service.

If you install only the gateway component on the same computer as the Web server, your Web server manages the core Web services and does not process user requests. This separation of processing may be required if you have a network firewall between the Web server and your Application Tier Components computers.

In the following diagram, the Web server has a gateway installed. Incoming requests are passed to the gateway and forwarded to the Application Tier Components computer. If request information is not saved, the result is returned from the Application Tier Components computer. If request information is saved, it is saved in the content store.

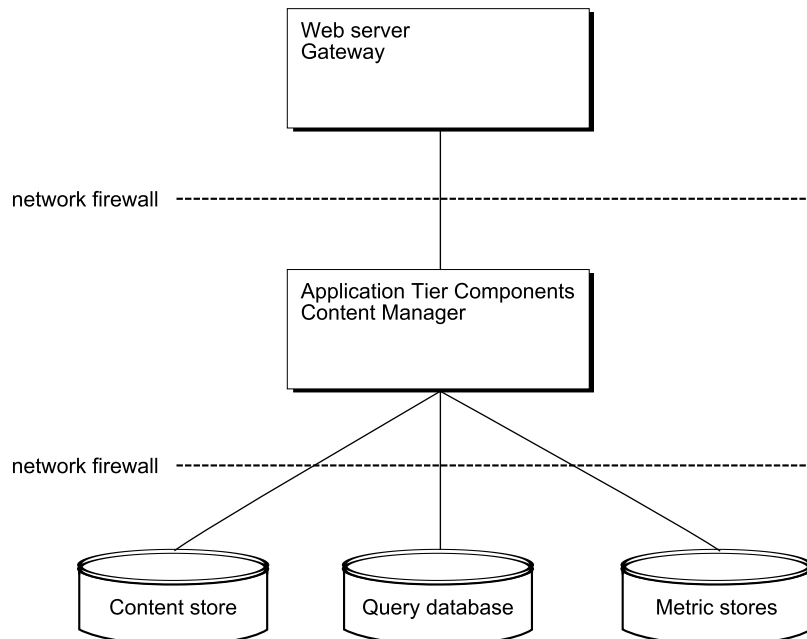


Figure 26. IBM Cognos components installed on different computers, where the gateway is separated from the Application Tier Components and Content Manager

The following diagram provides a more detailed view of an installation in which the gateway is on a separate computer from other IBM Cognos BI components. In this example, two Web servers are used, each with a gateway.

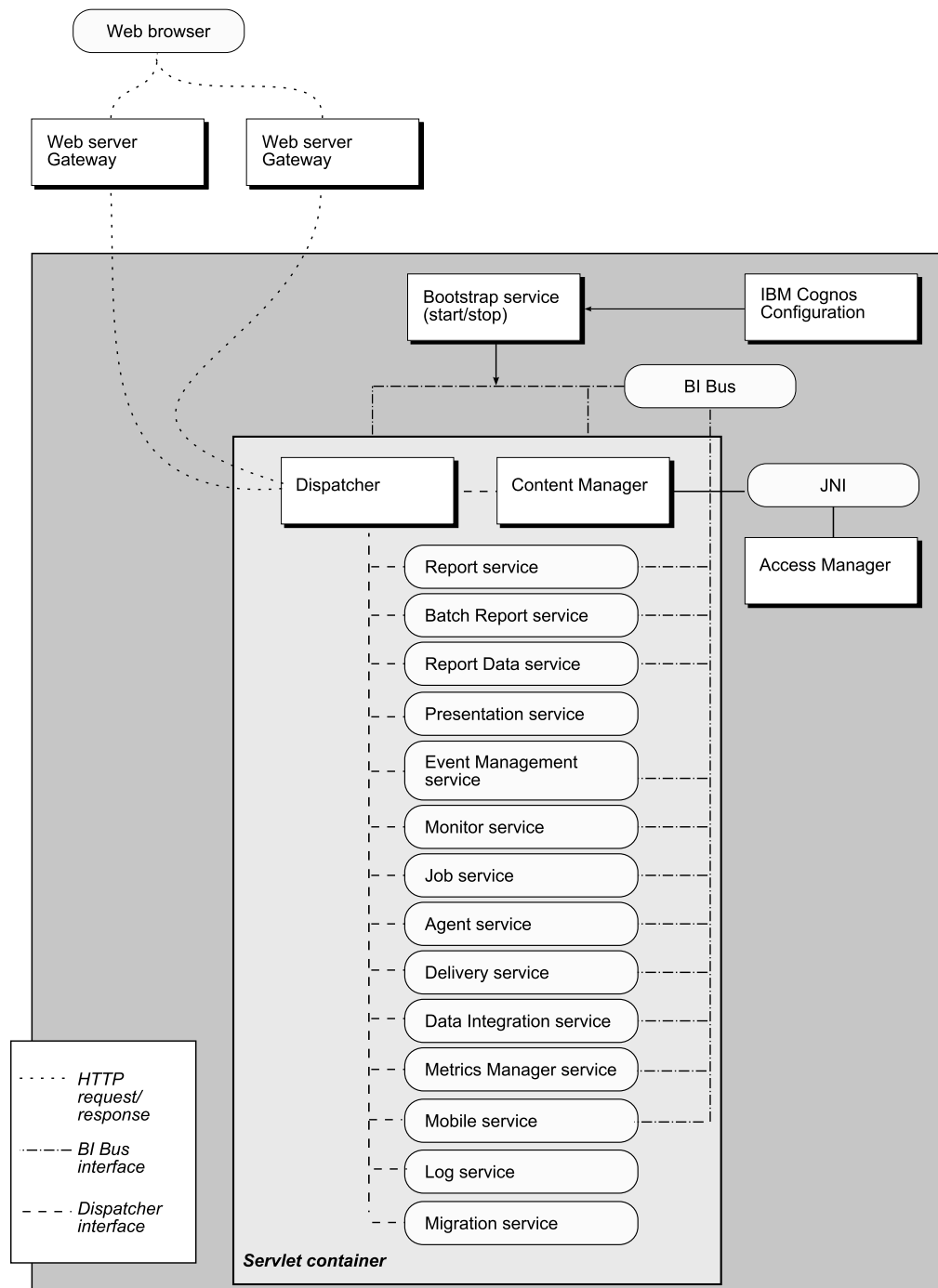


Figure 27. Detailed view of an installation where the gateway is on a separate computer from other IBM Cognos BI components.

Installing Application Tier Components and Content Manager on Separate Computers

Installing Application Tier Components on separate computers from the Content Manager can improve performance, availability, and capacity.

You may choose to install Content Manager separately from the Application Tier Components to isolate and protect sensitive data that is managed by Content Manager.

You may also choose to install Content Manager on a separate computer if large volumes of data are managed by Content Manager. In this type of environment, IBM Cognos BI scalability can be improved by increasing the size of the processor on which Content Manager is installed.

In the following diagram, incoming requests are routed to a gateway. The gateway forwards the request to the Application Tier Components computer. The Application Tier Components computer forwards it to the active Content Manager computer, which queries the content store and sends the results back to the Application Tier Components computer for rendering.

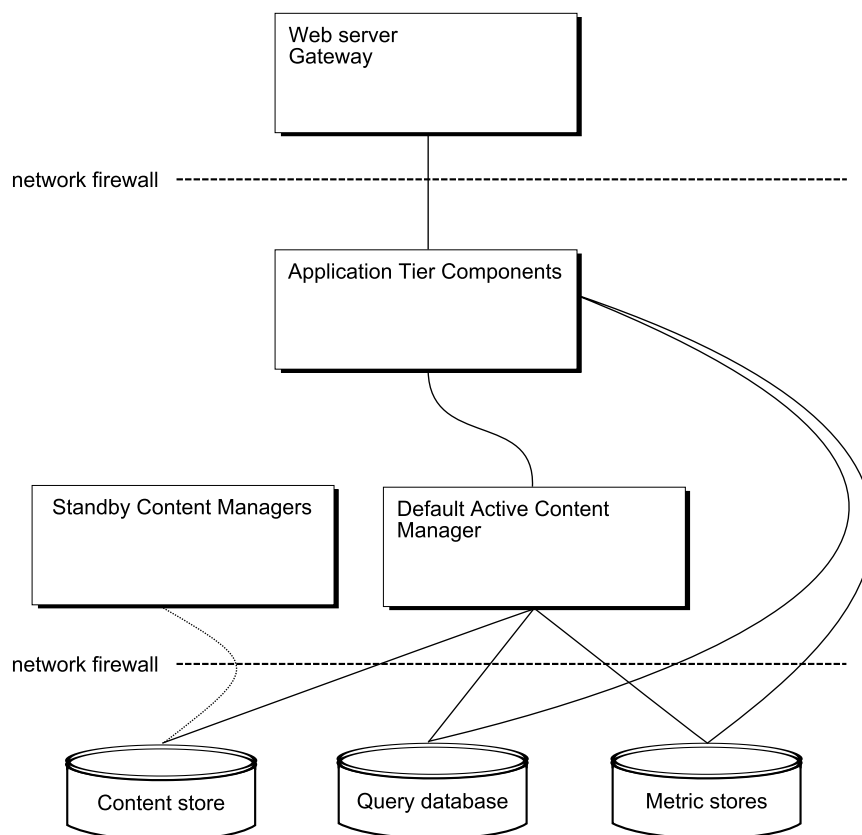


Figure 28. Installing application tier components and content manager on separate computers

The following diagram shows a more detailed view of an IBM Cognos BI installation in which separate computers are used for Application Tier Components and the Content Manager. This example shows only one installation of Application Tier Components, however the IBM Cognos BI environment can include multiple Application Tier Components computers.

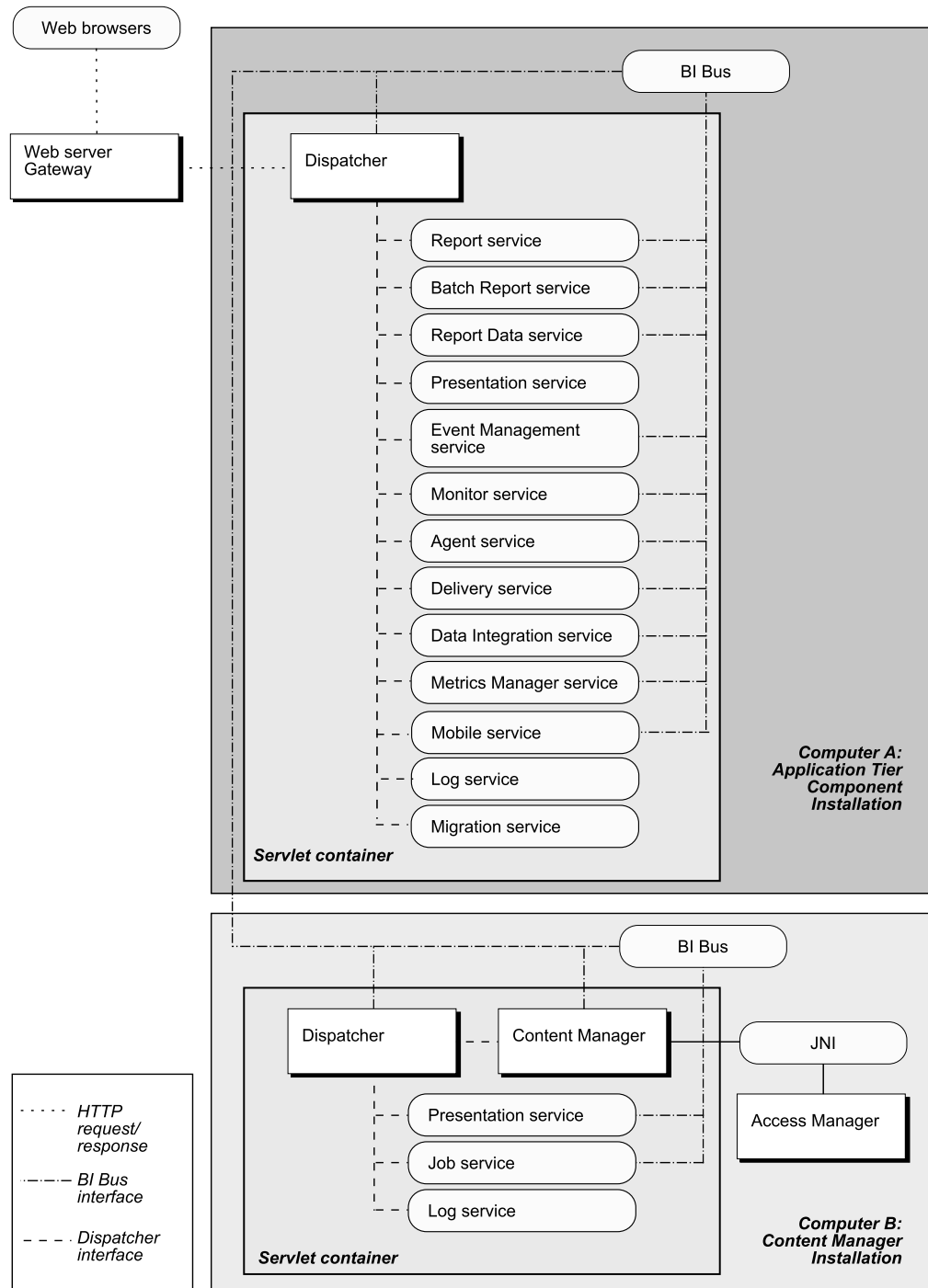


Figure 29. More detailed view of IBM Cognos Business Intelligence software installation

Multiple Installations of Content Manager

Your installation may include more than one Content Manager, each on a different computer. One Content Manager computer is active and one or more Content Manager computers are on standby.

Multiple Application Tier Components

To improve scalability in an environment in which there is typically a large volume of report requests to process, you can install Application Tier Components on multiple computers dedicated to processing incoming requests. By installing Application Tier Components on multiple computers, you distribute and balance loads among the computers. You also have better accessibility and throughput than on a single computer, as well as failover support.

Modeling Tool Installation Options

The IBM Cognos BI modeling tools, Framework Manager, Metric Designer, and Transformer, can be installed either on a computer containing other IBM Cognos BI components, or on a computer that is separate from these other components.

The modeling tools communicate with the Application Tier Components, which can be installed on one or more Web servers. Modeling tools can communicate with Application Tier Components using one of these routes:

- connect to the Application Tier Components dispatcher using the Internal dispatcher URI. This route is the preferred route.
- connect to an additional, dedicated gateway that is configured to connect to the dispatcher using the Internal dispatcher URI. You must configure appropriate security for this gateway. This method is useful when the modeling tool is outside a network firewall.

Important: Do not change your main gateway to use the Internal dispatcher URI. Doing so reduces the security of the IBM Cognos BI portal and studios.

To publish Framework Manager models, Metric Designer extracts, or IBM Cognos Transformer PowerCubes, you must configure the modeling tool to communicate with a dispatcher, either directly or through a dedicated gateway.

To ensure that the modeling tool can communicate with IBM Cognos BI components, on the computer where the tool is installed, configure cryptographic properties and the following environment properties:

- Gateway URI
- Dispatcher URI for external applications

For more information, see the *IBM Cognos Business Intelligence Installation and Configuration Guide*.

Web Servers Other Than Microsoft IIS

For Web servers other than Microsoft Internet Information Services (IIS), no functional difference exists between the two communication routes between the modeling tool and the Application Tier Components dispatcher. For either route, the modeling tool uses the BI Bus SOAP API. If you use the Web server route, and you have medium-sized and large models (approaching 1 MB in size), the models are broken into smaller pieces (chunked) for transmission.

If you use a Web server other than Microsoft IIS, configure the modeling tool to communicate through your Web server gateway (Route 1). This eliminates the need to set up additional communications channels if you use firewalls to separate the modeling tool, your Web server, and your Application Tier Components.

Network Firewall Considerations

When the modeling tool is outside a network firewall that protects the Application Tier Components, communication issues with the dispatcher can occur. For security reasons, the default IBM Cognos BI configuration prevents the dispatcher from accepting requests from the modeling tool when it is outside the network firewall.

A modeling tool that is outside a network firewall, for example Framework Manager, cannot send requests across a network firewall to the dispatcher on the IBM Cognos BI application server. To avoid communication issues when communicating across a network firewall, install the modeling tool in the same architectural tier as the Application Tier Components. The following diagram shows the Framework Manager computer inside the network firewall, successfully communicating with the dispatcher on the IBM Cognos BI application server.

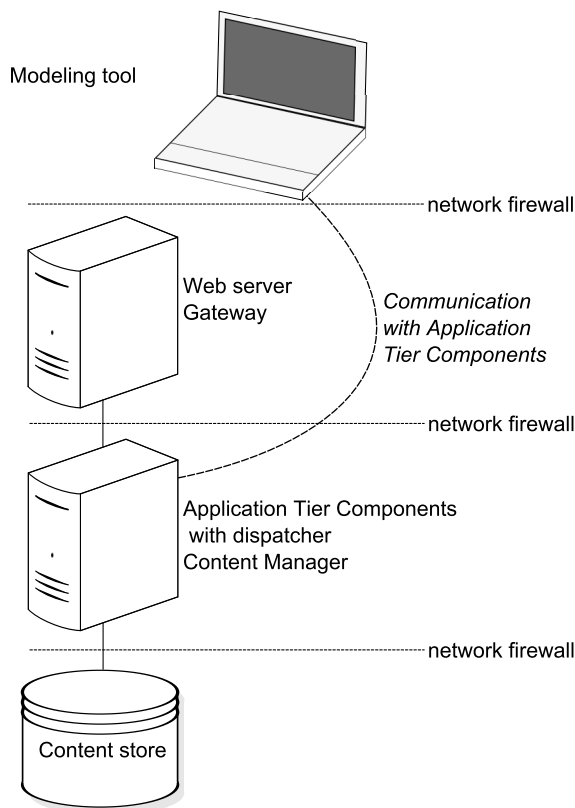


Figure 30. IBM Cognos components installed on different computers, with the modelling tools installed outside of the network firewall

Alternatively, you can install an additional gateway that is dedicated to communication with the modeling tool as shown in the following diagram. You then configure the modeling tool and its gateway such that the dispatcher accepts requests from the modeling tool.

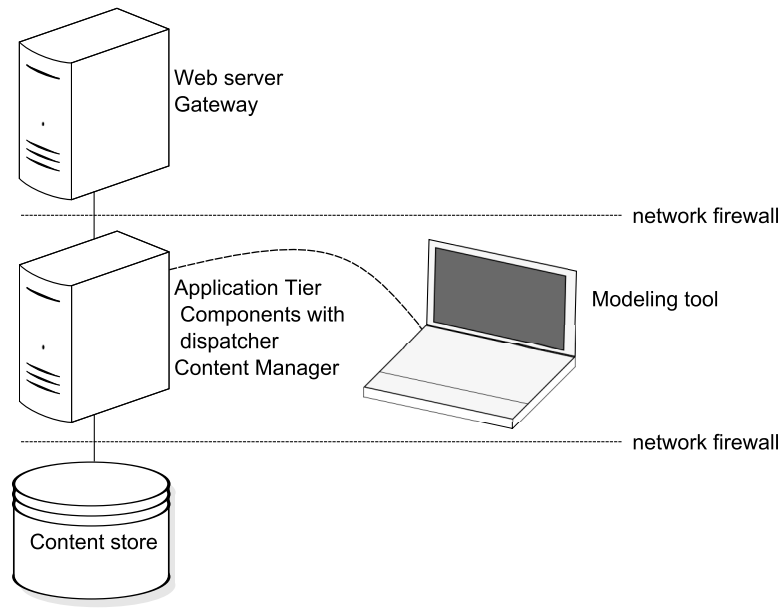


Figure 31. IBM Cognos components installed on different computers, with the modelling tools installed inside the network firewall

Alternatively, you can install an additional gateway that is dedicated for communication with the modeling tool. You then configure the modeling tool and its gateway such that the dispatcher will accept requests from the modeling tool. In addition to the environment properties that must be configured for the modeling tool, you must configure the Dispatcher URIs for gateway property on the dedicated gateway computer.

IBM Cognos Business Intelligence with other IBM Cognos products

You can install IBM Cognos BI in an environment that includes other IBM Cognos products.

The installation wizard for IBM Cognos BI can recognize compatible directories and shows a warning when conflicts occur. After IBM Cognos BI is installed, you can access objects that are created in another IBM Cognos product in IBM Cognos BI. The requirements for access depend on how you choose to run the two products.

Duplicated Services if Using Multiple Products

Many IBM Cognos products use similar services, such as the report service and the presentation service. If you are using multiple products, such as IBM Cognos Business Intelligence with IBM Cognos Metrics Manager or IBM Cognos PowerPlay, you must ensure that you disable some of the duplicated services to ensure your products work properly.

For example, you have IBM Cognos Business Intelligence and IBM Cognos PowerPlay installed. Both products have a reports service and a presentation service. If both products are accessed through the same gateway, reports that must be run on the IBM Cognos BI services could be routed to the IBM Cognos PowerPlay services. The result may be that your reports will display an error.

The following list shows an example of distributing components using three servers, where each server hosts one product. The fourth server hosts the common gateway.

- Server A - IBM Cognos Business Intelligence
 - Server B - IBM Cognos Metrics Manager
 - Server C - IBM Cognos PowerPlay
 - Server D - the Web server used for all products
1. On Server A, you must have the report service and the presentation service enabled.
 2. On Server B and Server C, you must disable the report service and the presentation service.
 3. On Server D, these services are not present.

IBM Cognos products that can be upgraded to IBM Cognos Business Intelligence

The following IBM Cognos products are earlier versions of components that are now within IBM Cognos BI ReportNet, IBM Cognos Metrics Manager, IBM Cognos DecisionStream, and IBM Cognos PowerPlay Web. When you upgrade these products to IBM Cognos BI, you can continue to run the earlier versions concurrently on the same computer until you are satisfied with the transition to IBM Cognos BI.

Cognos ReportNet

For ReportNet and IBM Cognos BI to run concurrently, each version must have unique ports, content stores, Web aliases, and cookie settings. If you use the default settings, configuration is required only to select new ports and a new content store for IBM Cognos BI.

You cannot use content from ReportNet directly in IBM Cognos BI until you upgrade ReportNet. When you upgrade to IBM Cognos BI, the content store is upgraded to use the IBM Cognos BI schema and cannot be used by previous versions. Therefore, you need to maintain both the old and new content stores to run both product versions. You can maintain both content stores using one of the following approaches:

- create a copy of the ReportNet content store database using database export utilities and use the copy with IBM Cognos BI
- use the embedded export feature in IBM Cognos Connection to export the ReportNet content store database and import the exported deployment into IBM Cognos BI

You can upgrade reports at the same time or upgrade them later if compatibility is required with some existing Software Development Kit applications.

For instructions about running concurrently and upgrading, see the upgrade chapter in the *IBM Cognos Business Intelligence Installation and Configuration Guide*.

Cognos Metrics Manager

To use data store content from IBM Cognos Metrics Manager in IBM Cognos BI, you upgrade by exporting the content from the data store to flat files, installing IBM Cognos BI, and then importing the flat files into the IBM Cognos BI metric

store. Note that the cube picker feature (the ability to map specific metrics to cube intersections) in IBM Cognos Metrics Manager is not available in other IBM Cognos BI studios.

For instructions about upgrading, see the upgrade chapter in the *IBM Cognos Business Intelligence Installation and Configuration Guide*.

Cognos DecisionStream

You can continue to run IBM Cognos DecisionStream Series 7 concurrently with IBM Cognos BI products. Catalogs that are created using DecisionStream Series 7 must be upgraded before you can use them with Data Manager.

For instructions about running concurrently and upgrading DecisionStream catalogs to the IBM Cognos BI Data Manager environment, see the chapter about upgrading a catalog in the *IBM Cognos Data Manager User Guide*.

Cognos PowerPlay Web

You can continue to use PowerPlay Web reports within the PowerPlay 7 user interfaces in the IBM Cognos BI portal. You can also drill through between PowerPlay Web and IBM Cognos BI. You can publish from PowerPlay Enterprise Server to IBM Cognos BI, provided that you use the same host name or IP address to identify the Series 7 namespace in IBM Cognos Series 7 and in IBM Cognos BI.

You can also upgrade the following reports to IBM Cognos BI reports by using IBM Cognos Migration Assistant:

- PowerPlay Windows reports
- PowerPlay Web Explorer reports
- PowerPlay for Excel reports
- PowerPlay for Windows reports published to PowerPlay Web

The tools are available at the IBM Cognos Customer Center (http://www.ibm.com/software/data/support/cognos_crc.html).

The last release of the migration tools was version 10.1.1. You can use these tools to migrate to IBM Cognos Business Intelligence version 10.1.1 (Report Studio or Analysis Studio), and then upgrade the migrated content to IBM Cognos BI version 10.2.0. You can also use the migration tools to migrate Series 7 PowerPlay content to IBM Cognos BI PowerPlay version 10.2.0.

IBM Cognos Series 7 products that can be migrated to IBM Cognos Business Intelligence

You can migrate metadata and applications from IBM Cognos Series 7 to IBM Cognos BI. Content that can be migrated includes Architect models from Windows, Impromptu client reports and catalogs from Windows, Upfront content, and Web-based content from Windows and UNIX.

For a list of supported IBM Cognos Series 7 versions and to download IBM Cognos Migration Assistant tools and documentation, see the IBM Cognos Customer Center (<http://www.ibm.com/software/data/cognos/customercenter>).

Architect

You can migrate Architect models for use as a metadata source for Framework Manager.

Impromptu

You can migrate Impromptu catalogs and reports to IBM Cognos BI. You use migrated catalogs as a metadata source for Framework Manager. After completing the catalog migration process, you can migrate and deploy Impromptu reports.

Upfront

You can migrate Upfront content to IBM Cognos BI. The migration process maps the Upfront content structure to an IBM Cognos Connection folder structure. By preserving the existing Upfront organization, it is easier to complete administrative tasks, such as applying security to the migrated content.

Impromptu Web Reports

You can migrate Impromptu Web Reports content, such as schedules and events, to IBM Cognos BI. You migrate Impromptu Web Reports content using an IBM Cognos Series 7 Deployment Manager package as the migration source. Before you migrate Impromptu Web Reports you must migrate the Impromptu catalog metadata used by the reports.

You cannot migrate Impromptu query definition files (.iqd), but you can continue to use existing .iqd files to build cubes in IBM Cognos BI Transformer 8.4. To do so, you must install the optional component, Series 7 IQD Bridge, which is available to install with IBM Cognos BI on IBM Cognos Series 7 supported platforms.

PowerPrompts are not migrated, but you can implement similar functionality using either the built-in administrator functionality or the IBM Cognos Software Development Kit.

IBM Cognos products that interoperate with IBM Cognos Business Intelligence

Some IBM Cognos products provide functionality that is not available in IBM Cognos BI. You can use these products in the same environment as IBM Cognos BI. With some products, you can access the different types of cubes or reports in the IBM Cognos BI portal. With other products, you can access unique features in the IBM Cognos BI portal.

Cognos Planning - Analyst

You can access published plan data in IBM Cognos BI by using the Generate Framework Manager Model wizard, which requires IBM Cognos Planning - Analyst 7.3 MR1 or later.

If you want to use this product with the IBM Cognos BI server, you must ensure that both products are the same version.

For more information, see the *IBM Cognos Analyst User Guide*.

Cognos Planning - Contributor

You can access unpublished (real-time) Contributor cubes in IBM Cognos BI by custom installing the IBM Cognos BI - Contributor Data Server component that is included with IBM Cognos Planning - Contributor 7.3 MR1 release or later. You can access published plan data in IBM Cognos BI by using the Generate Framework Manager Model administration extension in Contributor, which requires IBM Cognos Planning - Contributor 7.3 MR1 or later.

If you want to use this product with the IBM Cognos BI server, you must ensure that both products are the same version. You cannot install IBM Cognos Planning in the same path as 64-bit IBM Cognos BI.

For more information, see the *IBM Cognos Contributor Administration Guide*.

Cognos Finance

You can access IBM Cognos Finance cubes that are secured against a Series 7 namespace by using the IBM Cognos Finance Network API Service. You can also export data and metadata from IBM Cognos Finance for use in Framework Manager.

Cognos Controller

You can access IBM Cognos BI to create IBM Cognos Controller Standard Reports by using a predefined Framework Manager model that is created when IBM Cognos Controller is installed. You can also access published Controller data and structures in Framework Manager for custom reporting and analysis.

If you want to use this product with the IBM Cognos BI server, you must ensure that both products are the same version.

Cognos Transformer

You can use IBM Cognos PowerCubes and Transformer models that were generated by Transformer 7.3 or later directly in IBM Cognos BI. The cubes and models are upwards compatible and require no migration or upgrade tools. You can run reports and analyses in IBM Cognos BI against the IBM Cognos PowerCubes.

If you want to use the new integration features of Transformer with IBM Cognos BI, you can upgrade IBM Cognos Series 7.x Transformer models to IBM Cognos BI Transformer 8.4 or later. This allows you to use IBM Cognos BI data sources (such as published packages), list reports authored in Query Studio or Report Studio, authenticate using IBM Cognos BI security, and publish directly to IBM Cognos Connection.

Before you load the model, the IBM Cognos Series 7 namespace must be configured in IBM Cognos BI. The name ID that is used to configure the namespace in IBM Cognos BI must match the name used in IBM Cognos Series 7. For more information about configuring an IBM Cognos Series 7 namespace in IBM Cognos BI, see the *IBM Cognos Business Intelligence Installation and Configuration Guide*.

For more information about upgrading IBM Cognos Series 7 secured PowerCubes, see the *IBM Cognos Business Intelligence Transformer User Guide*.

For IBM Cognos Series 7 PowerCubes to be used in IBM Cognos BI, optimize the cubes for use in IBM Cognos BI by using the pcoptimizer utility, which is supplied with IBM Cognos BI. Otherwise, PowerCubes that were created with previous versions of Transformer may take too long to open in the IBM Cognos BI Web studios. This optimization utility is suitable for older PowerCubes created before Transformer 8.4 and does not require access to the model or data source. It is not necessary to run this command-line utility for cubes created in Transformer 8.4 or later. For more information about optimizing PowerCubes, see the *Transformer User Guide*.

You can publish PowerCubes using Transformer 8.4, Framework Manager, or directly in the IBM Cognos BI portal. You can publish single PowerCube data sources and packages to IBM Cognos Connection interactively in Transformer or in the command line. You can also publish silently using batch scripts after building a PowerCube. A user who has privileges to create data sources and packages in IBM Cognos Connection can publish PowerCubes in IBM Cognos Connection as well. The MDC file must be in a secured location that the IBM Cognos BI dispatcher and the report server process can access. Packages that use multiple PowerCubes from different PowerCube definitions or PowerCubes mixed with other data sources must be published using Framework Manager.

If you use an IBM Cognos Series 7 PowerCube as a data source, IBM Cognos BI converts the cube data from the encoding that was used on the system where the PowerCube was created. For a successful conversion, IBM Cognos Series 7 PowerCubes must be created with a system locale set to match the data in the PowerCube.

Cognos Data Manager

Data Manager is used to create data warehouses and data repositories for reporting, analysis, and performance management. When Data Manager is installed in your IBM Cognos BI environment, you can use the Data Movement Service to run builds and JobStreams in IBM Cognos Connection. You must install the Data Manager engine in the same location as your IBM Cognos BI Application Tier Components. Both Data Manager and IBM Cognos BI must be the same version.

Cognos Analytic Applications

IBM Cognos Analytic Applications is a performance management solution that includes a populated data warehouse, packages that describe the data available in the data warehouse, and a set of predefined reports.

IBM Cognos Analytic Applications Workbench is a performance management solution that includes sample business intelligence data with which you can build applications and documentation source files which you can modify to produce your own customized documentation for the product.

Some IBM Cognos Analytic Application components are available for installation on 64-bit systems. The default installation directories for 64-bit installations are different from the default installation directories for 32-bit installations. Whether you are installing all server components together on a single server or on multiple servers, 32-bit and 64-bit components must be in separate directories.

Cognos Lifecycle Manager

Lifecycle Manager is a Windows-based application for auditing upgrades from ReportNet 1.1 MR3 or MR4 and earlier versions of IBM Cognos BI to newer versions of IBM Cognos BI. It provides a verification feature that validates, executes, and compares report results from two different IBM Cognos BI releases. This helps to identify upgrade and compatibility issues between releases. User interface design and status reporting functionality provide both a proven practice process and support for upgrade project planning and status reporting. Lifecycle Manager also automates much of the process of bundling the required files, such as reports and models, for the test case.

For more information, see the *IBM Cognos Lifecycle Manager User Guide*.

Cognos BI Business Viewpoint Studio

IBM Cognos BI Business Viewpoint Studio helps to provide you with one version of the truth for dimensions used in an enterprise's performance management processes. With Business Viewpoint Studio, you have a controlled, collaborative, workflow-oriented business process to manage both manual and automated changes to all data related to how enterprises analyze and manage their business. Both IBM Cognos BI Business Viewpoint Studio and IBM Cognos BI must be at the same version.

Cognos Content Archival

With IBM Cognos Content Archival, you can store report output versions and their source report specifications to an external content archival repository. This enhances system performance and extends IBM Cognos product scalability by reducing the size of the Content Store, while helping to adhere to strict regulatory requirements. IBM Cognos Content Archival supports an IBM FileNet® Content Manager with IBM FileNet® CMIS external repository.

For more information, see the *IBM Cognos Business Intelligence Installation and Configuration Guide*.

Cognos TM1

IBM Cognos TM1 integrates business planning, performance measurement and operational data to enable companies to optimize business effectiveness and customer interaction regardless of geography or structure. Cognos TM1 provides immediate visibility into data, accountability within a collaborative process, and a consistent view of information, allowing managers to quickly stabilize operational fluctuations and take advantage of new opportunities.

For more information, see the *IBM Cognos TM1 User Guide*.

IBM Cognos Series 7 content that can be recreated in IBM Cognos Business Intelligence

Some IBM Cognos products cannot be programmatically migrated with the migration tools for IBM Cognos BI. IBM Cognos BI offers two options for duplicating content or functionality for the products described: use the Upfront portal within the IBM Cognos BI portal or use IBM Cognos BI studios to duplicate queries, visualizations, or objects.

The last release of the migration tools was version 10.1.1. You can use these tools to migrate to IBM Cognos Business Intelligence version 10.1.1 (Report Studio or Analysis Studio), and then upgrade the migrated content to IBM Cognos BI version 10.2.0.

Cognos Query

You can use IBM Cognos Migration Assistant to identify IBM Cognos Query objects in the IBM Cognos Series 7 migration source. You can then duplicate most IBM Cognos Query functionality in IBM Cognos BI. Foundation queries are available in IBM Cognos BI when you migrate an Architect model to Framework Manager. You can also manually replicate saved queries using SQL components in Report Studio.

Cognos Visualizer

You can duplicate some functionality by using the charting, layout, and formatting options in Report Studio and Analysis Studio.

Cognos NoticeCast

You can duplicate alert and notification functionality by using Event Studio and other IBM Cognos BI components.

Cognos Web Services

You can duplicate most IBM Cognos Web Services functionality using the IBM Cognos Software Development Kit.

CognosScript

You can duplicate automation functionality using the IBM Cognos Software Development Kit.

Cognos Portal Services

You can duplicate most IBM Cognos Portal Services functionality using IBM Cognos Connection.

Chapter 7. Performance Planning

Performance is a measure of how effectively a system completes the tasks it was designed to accomplish. It is a function of processing capacity and workload.

A system that performs well

- has the capacity to process requests quickly

Decide how much hardware you need to run IBM Cognos Business Intelligence, given your expected processing workload.

- scales to accommodate an increasing workload

Decide how much hardware you need to run IBM Cognos BI, given your expected processing workload.

- is available, even in exceptional situations

Decide how much hardware you need to run IBM Cognos BI, given your expected processing workload.

To ensure that IBM Cognos BI performs optimally, plan your IBM Cognos BI implementation with performance in mind. Planning for performance is part science, part art. It involves assessing the needs of different types of users, making decisions based on available resources, and developing a solution that considers security, application integration, and other factors.

This section does not provide absolute rules for planning IBM Cognos BI performance. It describes variables that affect performance, and ways to consider them when implementing IBM Cognos BI. The variables include the following:

- capacity

Decide how much hardware you need to run IBM Cognos BI, given your expected processing workload.

- scalability

Decide how to install and configure IBM Cognos BI components to take advantage of the ability of IBM Cognos BI to scale to meet increasing demand.

- availability

Decide how to implement IBM Cognos BI to take advantage of its ability to provide failover support in the event of a hardware failure or another system anomaly.

Maintaining IBM Cognos BI performance is an ongoing task. After implementing IBM Cognos BI, monitor and tune performance regularly. For information, see Chapter 8, “Performance Monitoring and Tuning,” on page 85.

Capacity Planning

Planning for capacity means determining the hardware needed for your system to perform well under its anticipated workload.

Capacity planning is a challenge, because it involves many variables, some of which are difficult or impossible to measure. It is the science of measuring known variables and developing an educated estimate of resource requirements on the basis of those measurements. It is also the art of allowing for unknown variables and assessing their impact on the estimates derived from the known variables.

To determine your IBM Cognos BI capacity requirements, gather information about the following:

- IBM Cognos BI users
Estimate the number of IBM Cognos BI users you expect to have, and when you expect them to use IBM Cognos BI.
- application complexity
Assess the complexity of the processing that your users will demand of IBM Cognos BI.
- your infrastructure
The characteristics of your environment and infrastructure.

Capacity planning is an ongoing process. After implementing IBM Cognos BI, monitor and modify your capacity as necessary to meet your performance expectations.

Estimating IBM Cognos BI User Load

In general, the greater the number of users, and the more concentrated their requests over time, the more hardware you need for a system to perform effectively. As a result, when planning adequate capacity for IBM Cognos BI, you should estimate the number of people who will use IBM Cognos BI and determine when they will use IBM Cognos BI. This can help you decide not only how much hardware you need, but also how to make the best use of the hardware you have.

Estimating Concurrent Users

The only users placing load on IBM Cognos BI are those who are actually performing processing. These are concurrent users. You can estimate the number of concurrent users, based on your total user population, by distinguishing between named, active, and concurrent users:

- named users
Named users are all of the users authorized to use IBM Cognos BI; that is, your total user population.
- active users
A subset of named users, active users are logged on to IBM Cognos BI and can demand system resources.
- concurrent users
A subset of active users, concurrent users are simultaneously demanding system resources. This includes users submitting requests and users waiting for a response to a request.

As a general rule, the ratio of named to active to concurrent users for business intelligence applications is about 100:10:1. In other words, for every 1000 named users there are 100 active users and 10 concurrent users.

The concurrency ratio can vary over time, and is affected by many factors. For example, the number of concurrent users relative to active and named users tends to be higher when the user population is small. However, the most important determinant of the concurrency ratio is how processing demand is distributed over time.

Estimating Load Distribution

In IBM Cognos BI, load is generated by

- user navigation and processing requests, such as requests to run or view reports

- requests made through automated or event-driven processes, including scheduled and burst reports

By determining when users are most likely to be using IBM Cognos BI and submitting processing requests, you can decide when to schedule automated processes. This allows you to distribute the processing load evenly over time, so that you make the best use of your system resources to maintain optimal performance. The key to doing this is estimating the number of concurrent users that will be applying load to your IBM Cognos BI system at any time.

Factors such as business hours, business practices, and the geographic distribution of users can determine how the concurrency rate changes over time, and how you choose to ensure adequate capacity.

A business intelligence application in which requests are spread evenly throughout the day has a lower peak concurrency ratio than an application in which the majority of requests are limited to a specific time of day. For example, if users are concentrated in one time zone, there will likely be heavy demand during business hours, followed by a period of low demand after hours. In this situation, you may be able to manage peak and non-peak time periods by sharing hardware resources between interactive and noninteractive processes. You would schedule automated activity to run in non-peak times to produce content for retrieval by interactive users in peak times.

On the other hand, if your user population is distributed across several time zones, user load on the system tends to be spread out over more hours, and there are fewer available non-peak hours for scheduled activities. In this situation, you may choose to dedicate separate hardware resources for interactive and noninteractive use.

Scheduling Processing to Distribute Load

Knowing how user load is distributed helps you decide when to schedule automated processes. Scheduling can be applied to two types of reports:

- scheduled reports

These reports often depend on updated, event-driven information, such as sales data for the previous day.

- burst reports

These are reports for which multiple users require filtered data based on a predetermined schedule. Burst reports are used when a common report format is applicable to more than one recipient, but each recipient requires customized information.

Scheduling is most useful for reports based on data that is updated on a predictable and cyclical basis. For example, an organization may need to produce sales reports based on information from the previous day, and make them available to users at the start of each business day. If users generate these reports at the beginning of each day, it creates considerable load on the system. By scheduling the reports to be triggered by data refresh, and run during non-peak times, the capacity required at peak times is reduced.

For information about tuning report scheduling and bursting after IBM Cognos BI is implemented, see “IBM Cognos BI Tuning” on page 88. For information about how to schedule reports, see the *IBM Cognos Administration and Security Guide*.

Assessing Application Complexity

Load is not only determined by the number of concurrent users, but by the complexity of their processing requests. The greater the complexity of a request, the more time is needed to process the request. In general, hardware resources can process more requests in a given time period when the requests are simple rather than complex. As a result, application complexity is an important determinant of the number of concurrent users that can be supported on a given hardware infrastructure.

The complexity of an IBM Cognos BI application depends on such things as the amount of work required to process the result set returned from the database query, and the size and layout of the report output. Size is determined by the number of pages in a report and the presence of elements, such as charts.

By identifying reports run at peak times, and improving their efficiency while meeting user requirements, you can improve performance during peak times. Because reporting patterns change over time, assessing application complexity, and improving reporting efficiency, should be ongoing activities. For more information, see Chapter 8, “Performance Monitoring and Tuning,” on page 85.

Planning Infrastructure Components

IBM Cognos BI performance also depends on the characteristics of your infrastructure.

Ideally, IBM Cognos BI server components should be connected by a network with 100 Mb of available capacity. Network bandwidth between a Web browser and a Web server does not affect system scalability, but does affect user performance.

Use true server computers, rather than fast workstations. True server computers run business applications faster and provide systems that are less likely to fail.

Will Web and application servers be dedicated solely for use by IBM Cognos BI, or shared by other software products? If other applications are sharing the resources, these applications must be taken into account when determining capacity requirements.

Install only gateway components on server computers that are dedicated to Web server processing. Web servers are designed to handle many small requests. Application servers often handle larger requests.

Use the gateway type most appropriate for your environment. For example, for some environments, ISAPI or Apache may provide better performance than CGI.

The complexity of your security infrastructure can increase response time. As your security infrastructure becomes more complex, a user request must be validated more frequently. For example, if you implement multiple network firewalls, each firewall must validate every request that passes through it. This can increase the time taken to complete the request. In addition, if you use SSL, the overhead of SSL encryption adds both processing overhead and size to the response.

Because notification service generates additional email traffic, ensure that your mail server can scale to support the increased load.

Sizing Your Content Store

The content store is used by Content Manager to store all IBM Cognos BI information that is visible in, or managed through, IBM Cognos Connection or your third-party portal. The content store is at the heart of IBM Cognos BI, and must have sufficient resources to operate effectively. To maximize IBM Cognos BI performance and scalability, ensure that your content store has the resources required to ensure that it does not become a bottleneck.

The size of the IBM Cognos BI content store you need depends on the number and size of the IBM Cognos BI items, such as reports, packages, and schedules, that you will create and store. Over time, as users create more items, the amount of space needed for the content store typically increases.

When determining the amount of space to allocate for your content store, consider the following:

- number of users

The greater the number of users, the greater the number of reports typically run and stored, and the larger the content store needed.

- number of saved reports

The greater the number of reports saved, the larger the content store needed. Reports designed for use throughout an organization, and stored in public folders, are often duplicated by users in private folders. This increases the number of reports stored and the space required for them.

- number of saved views

The greater the number of report views saved, the greater the space required.

- number of folders

IBM Cognos BI typically uses public folders as well as one or more private folders for each user. The number of characters in the name and description of each folder can increase the folder size.

- number of schedules

Schedules can exist for daily, weekly, and monthly print runs. The greater the number of schedules, the greater the content store space required.

- number of Framework Manager packages

The greater the number of packages, and the number of tables and query subjects in those packages, the greater the space required.

- additional storage items

Additional storage items, such as transaction logs and temporary space requirements, increase the size of the content store required.

Example - Estimating Content Store Size

The size of an empty content store hosted in a Microsoft SQL Server database is approximately 2 to 3 Mb. Depending on your size allocation strategy, this may vary for other supported databases.

The number of concurrent users affects the size of the content store because temporary disk space is allocated to serve report run requests, even if the requests are not saved.

Out of 50 concurrent users, approximately 25% will be executing reports and 75% will be viewing saved outputs. As a result, approximately 12.5 of the 50 users will be running reports (50 concurrent users * 0.25 executing reports = 12.5 concurrent users).

The following table provides an example of how to estimate the size of the content store you need.

*As a rule of thumb, the ratio of named to active to concurrent users is 100:10:1. However, the ratio varies with the environment. For more information, see “Estimating Concurrent Users” on page 70.

Table 3. Example of factors that affect the size of a content store

Factor	Number	Estimate of content store requirements (Kb)
Named users	1000*	not applicable
Active users	250*	not applicable
Concurrent users (temp space requirements)	50*	5,000,000
Saved reports: 1-10 pages (2 per user for Public and Myfolder copies at 340 Kb per report)	1001	340,340
Saved reports: 10-100 pages (9 per user for 4 Public and 5 Myfolder copies at 440 Kb per report)	5,004	2,201,760
Saved custom views: 1-100 rows (3 per user, all Myfolders at 250 Kb per view)	3,000	750,000
Saved custom views: 100-1000 rows (8 per user, all Myfolders at 350 Kb per view)	8,000	2,800,000
Folders (Public and Myfolders)	1,025	500
Framework Manager models	15	100,000
Framework Manager models (tables)	25	-
Framework Manager models (query subjects)	50	-
Schedules (day and week)	175	5,000
Empty content store	--	3,000
Database transaction logs	--	3,000,000
Total	--	14,200,600

Scalability Planning

Scalability is the ability of a system to adapt to increased processing demands in a predictable way, without becoming too complex, expensive, or unmanageable. As you deploy a system to larger numbers of users, often in different locations and time zones and with different language requirements, scalability becomes increasingly important.

IBM Cognos BI was designed for scalability. It scales vertically using more powerful computers, and horizontally using a greater number of computers. How you install and configure IBM Cognos BI components can enhance its scalability.

Web Server and Gateway Scalability

All Web communication in IBM Cognos BI is through an IBM Cognos BI gateway installed on a Web server. To increase the scalability of your IBM Cognos BI system, you can run your Web server on a larger computer. You can also install the IBM Cognos BI gateway on more than one Web server and configure your servers to leverage load balancing features.

Load Balancing

Load balancing spreads tasks among all available processors. It is important in any system, and is a key to processing capacity and scalability. In IBM Cognos BI, load balancing means ensuring that processing requests are distributed appropriately among all the available IBM Cognos BI servers. IBM Cognos BI does this automatically, but you can configure load balancing as well.

Automatic Load Balancing

In a distributed environment, IBM Cognos BI balances request load automatically. By default, as servers are added to the system, each server dispatcher processes the same number of requests. If there is more than one instance of a given service, the dispatcher distributes requests to all the enabled instances of the service that are registered in Content Manager.

Configuring Load Balancing

While automatic load balancing may be appropriate when hardware resources are identical throughout a server topology, it may not be ideal in environments containing a mix of hardware resources with different capacity characteristics. In a hardware environment that contains servers with varying degrees of processing capacity, it is desirable to balance the processing load according to the server's capacity.

In IBM Cognos BI, you can set process capacity settings using server administration options. For example, if you have two servers, one of which has twice the capacity of the other, you might assign the more powerful server a weight of two and the less powerful server a weight of one. IBM Cognos BI then submits twice as many requests to the more powerful server.

For more information about IBM Cognos BI dispatcher settings, see the *IBM Cognos Business Intelligence Administration and Security Guide*.

Load Balancing Dispatchers

Without a software or hardware load balancing mechanism, each IBM Cognos BI gateway is aware of only one dispatcher, and distributes all requests to that dispatcher. The dispatcher then distributes the requests among IBM Cognos BI servers. Because every request initially goes through the same dispatcher on one server, the load on that server is increased. An extra step is needed to automatically balance the load, as shown in the following diagram.

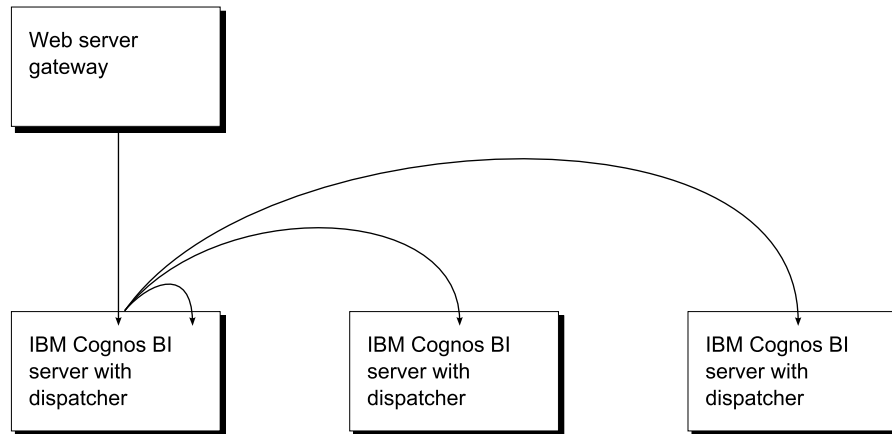


Figure 32. Load balancing dispatchers

This extra step can be avoided by either implementing load balancing without an external load balancing mechanism, or by using a router or other load balancing mechanism.

Load Balancing Without an External Mechanism

Since gateway servers often have less load than IBM Cognos BI servers, you may achieve better performance by configuring dispatchers together with the gateways, as shown in the following diagram.

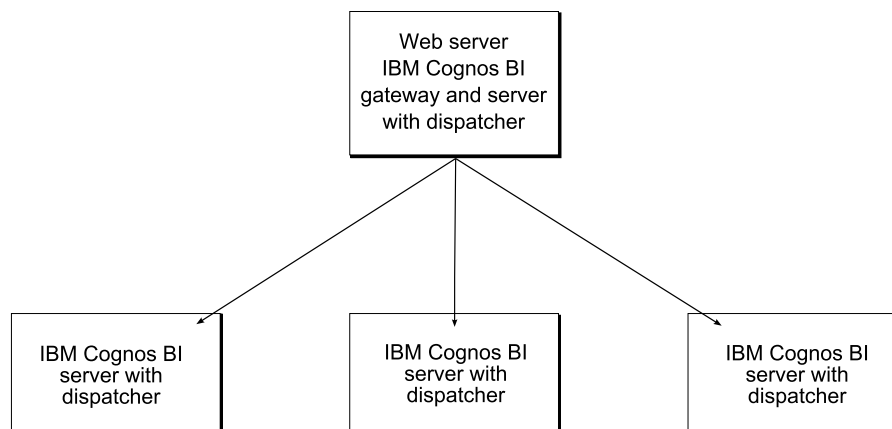


Figure 33. Load balancing by configuring dispatchers with gateways

This ensures that the processing capacity of the IBM Cognos BI servers is directed toward serving report requests rather than load balancing requests.

You can also achieve load balancing by having gateways direct all traffic to an IBM Cognos BI server computer that is dedicated to dispatching, as shown in the following diagram.

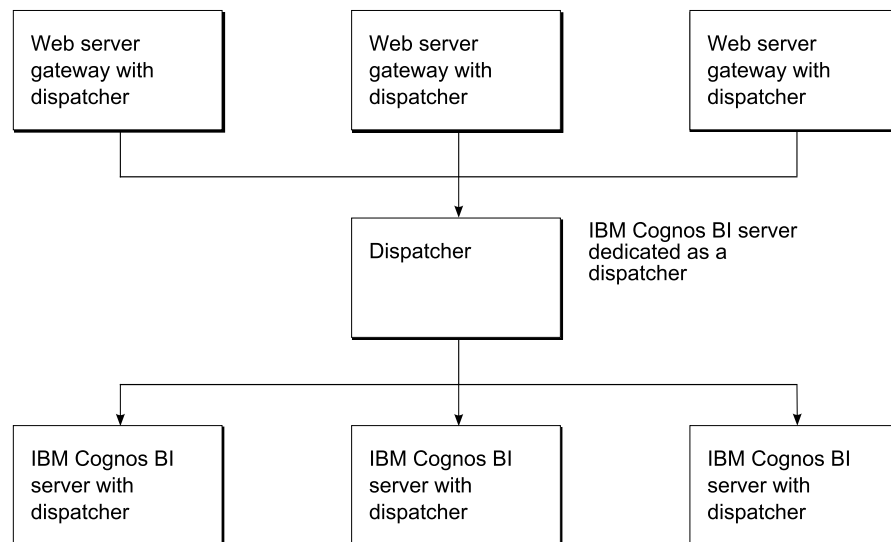


Figure 34. Load balancing by configuring gateways to direct traffic to a dedicated IBM Cognos BI server used for dispatching

This configuration also removes dispatching load from the IBM Cognos BI servers. However, it does require separate dispatching computers.

Using External Load-Balancing Mechanisms

You can use external load-balancing mechanisms, such as routers, to further distribute tasks in IBM Cognos BI. Load-balancing routers can be used in either or both of these locations:

- between the browser and Tier 1: Web Server
- between Tier 1: Web Server and Tier 2: IBM Cognos BI Server

You can use an external load-balancing mechanism to distribute requests to dispatchers across all available servers, as shown in the following diagram.

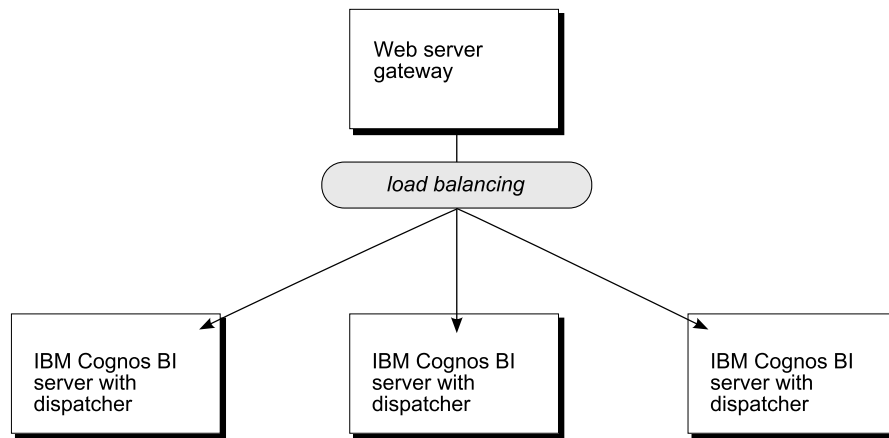


Figure 35. Using external load-balancing mechanisms to distribute requests to dispatchers across all available servers

You can also use routers with multiple gateways, as shown in the following diagram.

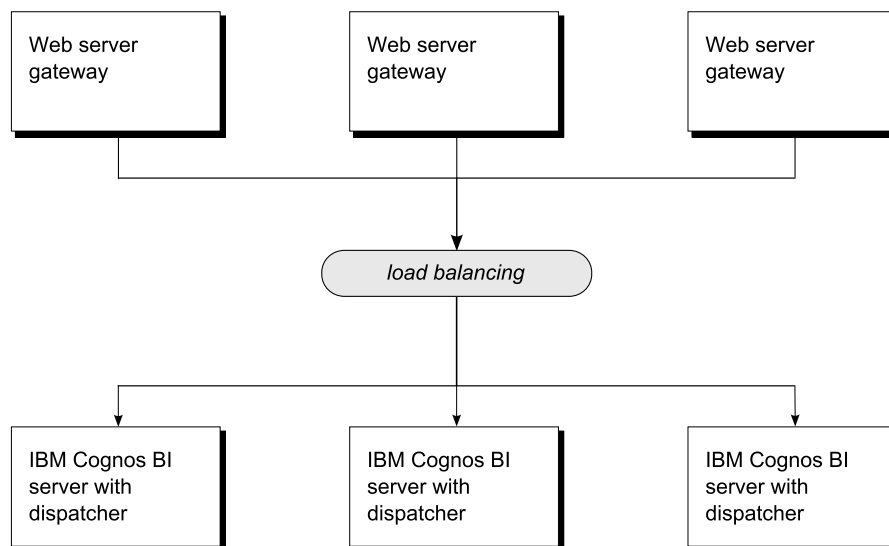


Figure 36. Using external load-balancing mechanisms to use routers with multiple gateways

An ideal load-balancing mechanism provides the same capacity awareness as an IBM Cognos BI dispatcher.

To ensure that requests are not distributed by both an external load-balancing mechanism and the dispatcher, you must configure the dispatchers to not use their built-in load balancing for low affinity requests. This ensures that requests remain at the server where the hardware load balancer directed them.

Request Affinity

Affinity refers to whether a request is assigned to a specific server or whether a load-balancing mechanism can assign it to another server. Affinity between request and server ensures that requests are routed to an appropriate computer for processing. IBM Cognos BI uses the following types of affinity: absolute, control, high, low, session, and server. The cancel operation is handled with a dedicated connection and does not have an affinity type.

To ensure that requests are managed efficiently and load is balanced, IBM Cognos BI uses request affinity to route some requests. For example, requests are routed back to the IBM Cognos BI server that handled earlier, related requests. IBM Cognos BI does this automatically. The use of one or more load-balancing mechanisms does not disrupt request affinity processing.

ReportService connections can be defined as AffineConnections or NonAffineConnections. AffineConnections accept only absolute and high affinity requests. NonAffineConnections accept all types of reportService requests.

Absolute Affinity

Absolute affinity requests are always routed back to the server that processed the original request. If the server is not available, the request fails. For example, when a user cancels a running report, absolute affinity routes the cancel request back to the executing process. Absolute affinity is used to create an association between the client and the executing server to ensure that long-running requests do not time out.

IBM Cognos BI routes absolute affinity requests to a specific server, regardless of the load balancing used. An absolute affinity request is used with operations such as `getOutput` and `release`.

Control Affinity

Control affinity requests are routed in the same way as absolute affinity requests. A control affinity request is reserved for system operations such as `wait` and `cancel`.

High Affinity

High affinity requests can be processed on any of a number of servers, but resource consumption is minimized if the request is routed back to the executing process. The dispatcher routes a high affinity request to the server that is specified by the conversation context node ID. If the specified server is not available, the request is routed to any available server.

For example, when a `pageDown` command is run while reading a report, the command can be run most efficiently by using the process that served up the page that is shown. If that process is not available because the administrator shut down the computer or there was a network failure, the request is routed to another available process. The next page can still be served up, although the process will be slower.

IBM Cognos BI routes high affinity requests to a specific server regardless of the load balancing used. A high affinity request is used with the following operations: `back`, `email`, `firstPage`, `forward`, `lastPage`, `nextPage`, `previousPage`, `print`, `render`, `save`, and `saveAs`.

Low Affinity

Low affinity requests will operate just as efficiently on any computer. For example, a report request can run on any computer in the IBM Cognos BI system.

A low affinity request is used with the following operations: add, collectParameterValues, execute, getMetadata, getParameters, query, testDataSourceConnection, update, and validate.

For more information about affinity in IBM Cognos BI, see “Setting Affinity Connections” on page 90.

Session Affinity

Session affinity requests are routed according to the conversation context node ID. If the node ID is present, they are routed in the same way as a high affinity request. If the node ID is absent, they are routed in the same way as a low affinity request. Session affinity is used with the query reuse feature: when query reuse is turned on and you run a report for the first time, the query is stored in the cache of your current session and reused the next time you run the report. For more information, see the Framework Manager *User Guide*.

Server Affinity

Server affinity requests are routed in the same way as absolute affinity requests. Server affinity is used for data source testing in administration: an administrator can test the connection to a new data source. For more information, see the topic about creating a data source in the *IBM Cognos Business Intelligence Administration and Security Guide*.

IBM Cognos BI Server Scalability

The IBM Cognos BI application server has one or more IBM Cognos BI servers. Each IBM Cognos BI installation contains Content Manager to manage data stored in the content store. Each IBM Cognos BI server contains a dispatcher that runs the IBM Cognos BI presentation service, batch report and report services, job and schedule monitor service, and log service.

Only one Content Manager is active at a time. The others are on standby. A standby Content Manager becomes active only if the computer on which the active Content Manager is installed fails.

To improve scalability, you can enable or disable Content Manager and the dispatcher services on individual application servers to balance the load for a given computer by request type. For example, if you have three application server computers, you might dedicate one to running interactive report requests, another to Content Manager, and the third to the other IBM Cognos services.

By targeting processing at specific computers in this way, you can control the load on each computer. For example, putting Content Manager on its own computer ensures that other requests do not downgrade its performance by competing for resources. Because report runs tend to be resource intensive, isolate the report services from other activities, especially in larger IBM Cognos BI deployments. However, before making this type of tuning configuration, analyze your user requirements carefully.

IBM Cognos services scalability

IBM Cognos services operate as threads within the dispatcher. The report services differ from the other services in the way they contribute to scalability.

Report and Batch Report Services

The report and batch report services are multi-instance components of IBM Cognos BI. As a result, one or more instances can be configured to operate on each IBM Cognos BI computer.

The same program is used for both the report service, which handles interactive requests, and the batch report service, which handles scheduled tasks. For information about configuring the number of instances of the report services and the number of threads that each instance handles, see the *IBM Cognos Administration and Security Guide*.

Content Manager

Content Manager, which can be installed in Tier 2 or 3 of IBM Cognos BI, stores information in the content store. To allow fast retrieval, Content Manager builds an in-memory cache to service many requests. This ensures optimal performance and enhances scalability by limiting the number of database reads required to meet user requests.

In the single Content Manager process, multiple threads can concurrently service requests for content. Content Manager creates one or more threads for each user request. Performance depends on the power of the central processor unit (CPU) of the computer on which Content Manager is installed.

To increase scalability, use a larger computer capable of managing more concurrent request threads. When scaling up Content Manager, be sure to scale up the content store relational database management system so that it does not impede Content Manager performance.

Indexed Searching

Search performance is bound by the number of CPUs in your BI environment and can be scaled by having Application Tier Components installed on multiple computers. The index services are installed with Application Tier Components. Scaling the index data service speeds up the retrieval of search results in environments where multiple users run concurrent search queries. This approach requires the use of a shared file system for the index data. For more information, see the topic about configuring the index data services in the *IBM Cognos Business Intelligence Installation and Configuration Guide*.

Having multiple instances of the index search service has little impact on the scalability of the search function. However, this approach does add redundancy to the environment.

The quality of the search results is dependent upon the quality of the index content. Indexing updates should be run regularly to index new and updated content. Unfortunately, indexing processes can take a significant amount of time to run.

Because the indexing services and processes rely heavily on the report service, we recommend that you schedule index updates for off-peak times. The initial indexing process, as with any full-text indexing process, can take several hours depending on the size of the IBM Cognos BI content store and related data. However, there may only be a limited amount of time in which the index update can occur due to other server processes. You may want to scale the index update

service for improved indexing performance.

Other Services

The scalability of the presentation service, job and schedule monitor service, and log service, is primarily dependant on the CPU size and the available memory. These components can be scaled in two ways:

- vertically, by using a larger computer capable of managing more concurrent request threads
- horizontally, by running the services on additional computers

There is no specific configuration to tune these components. However, you can view the load-balancing configuration set by the server administrator to determine how much load is given to each computer running these services.

Availability Planning

Availability is the ability of a system to withstand or recover from exceptional situations, such as a computer failure. All IBM Cognos BI components have built-in failover features to ensure that IBM Cognos BI handles exceptions well.

You can configure components in each of the IBM Cognos BI tiers to enhance availability. As a general rule, make all IBM Cognos BI components available on at least two computers. If the computer on which a IBM Cognos BI component is running fails, another computer takes over.

If, for tuning reasons, you are not running all IBM Cognos BI components on every IBM Cognos BI server, ensure that each component is running on at least two servers. In the event of a computer failure, the remaining component processes requests. Performance may degrade, but there will be service.

IBM Cognos Business Intelligence Gateway Availability

All Web communication in IBM Cognos BI is through an IBM Cognos BI gateway installed on a Web server. Each gateway can communicate with a single dispatcher in the applications tier.

Use two or more Web servers with IBM Cognos BI. This ensures that the failure of a single server does not result in the loss of IBM Cognos service. You can also use an external load-balancing mechanism, such as a router, to distribute requests across all available dispatchers.

In the unlikely event of a failure, the IBM Cognos BI gateway and IBM Cognos Application Firewall are restarted automatically by the Web server.

IBM Cognos Business Intelligence Server Availability

The IBM Cognos Business Intelligence server contains Content Manager to store and manage information, and a dispatcher to start IBM Cognos services and route requests.

The dispatcher manages the IBM Cognos BI presentation service, batch report and report services, job and schedule monitor service, and log service. To ensure that the failure of one computer or service does not cause IBM Cognos BI to become

unavailable, install two or more IBM Cognos BI servers. You can distribute services across IBM Cognos BI servers, and you do not need to enable all services on all IBM Cognos BI servers.

The Java technology of the IBM Cognos BI server provides Content Manager and the dispatcher with built-in failover support. Both components are multithreaded, and the threads are isolated from each other. If a failure occurs, it affects only a single request thread. If that thread is lost, no other threads are affected, and the failure does not affect the service as a whole.

If Content Manager or the dispatcher fails, the IBM Cognos BI server restarts it automatically. If you use the IBM WebSphere Application Server Liberty Profile provided with IBM Cognos BI, the IBM Cognos service monitors and restarts the application server. If you use an application server other than WebSphere, the administration services for that application server restart it.

Content Manager Availability

By default, the first Content Manager installed with IBM Cognos BI is the active one. An IBM Cognos BI server administrator can change the default Content Manager and the active Content Manager at any time. When IBM Cognos BI is started, the default Content Manager locks the content store from access by all other installations of Content Manager. These other Content Manager installations enter standby mode.

Your installation may include more than one Content Manager, each on a different computer. One Content Manager computer is active and one or more Content Manager computers are on standby.

This failover mechanism works because dispatchers and the active Content Manager routinely communicate with each other. If a dispatcher can no longer reach Content Manager, the dispatcher signals a standby Content Manager, which becomes the active Content Manager. The other installations of Content Manager remain in standby mode for continuing failover support. The standby Content Managers retrieve cryptographic settings, such as the common symmetric key (used to encrypt and decrypt data), from the active Content Manager.

Content Store Availability

Content Manager stores IBM Cognos BI information in the content store RDBMS. Content Manager writes to the content store using proper relational transactions. You can use standard database tools for backing up and restoring the content store.

Chapter 8. Performance Monitoring and Tuning

Over time, an IBM Cognos Business Intelligence environment changes. User populations grow, processing requests tend to increase in number and complexity, and network capacity and other aspects of infrastructure may be modified.

These changes can affect IBM Cognos BI performance. As a result, it is important to monitor and tune performance regularly.

Monitoring performance means regularly checking the status of your IBM Cognos BI installation and its resources. IBM Cognos BI provides metrics for checking the performance of the system, servers, dispatchers, or services. You can set thresholds for metrics to identify when the performance exceeds or falls short of expected ranges. You can configure the system to notify anyone who should be made aware of the problem when a performance issue occurs. You should conduct regular and targeted monitoring of the IBM Cognos BI servers. This is important to assess the occurrence and impact of paging, memory use, and other measures of an efficient system.

Tuning can involve adjustments in the following areas:

- databases
Keep your databases optimized for querying and reporting.
- application servers
Adjust your application server memory and connection settings as required for better performance.
- Web servers
Tune your Web server for maximum performance.
- IBM Cognos BI
Monitor and tune various aspects of your IBM Cognos BI system.

Perform additional tuning as required. This can involve modifying PDF rendering settings, changing low bandwidth connections, performing regular disk maintenance, and other tasks.

After a certain point, performance tuning efforts yield diminishing returns. A growing user population, and increased processing demands, will eventually require you to consider increasing system capacity. To improve IBM Cognos BI performance, you can scale vertically by using more powerful servers, or scale horizontally by adding servers and balancing the processing load among your servers. For more information about determining IBM Cognos BI capacity requirements, see “Capacity Planning” on page 69. For information about other tuning and maintenance tasks, see the *IBM Cognos Business Intelligence Administration and Security Guide*.

Performance Metrics

You can monitor current system performance using metrics. You can assess the status of the system as a whole, as well as the status of individual servers, dispatchers, and enabled services.

For example, you check the performance metrics and notice that the report service shows a red square indicator, which identifies poor performance. You view the metrics for the report service and determine that the number of requests waiting in the queue exceeds the number that can be processed in a specified length of time. You can then take action to reduce the number of requests waiting in the queue.

Metrics are grouped using the following categories:

- session metrics for monitoring the number of sessions in your system
These metrics are collected by Content Manager.
- queue metrics for monitoring the ability of dispatchers and services to keep up with requests that are waiting in queues
For example, queue metrics for services may identify that requests are waiting too long in a queue for processing. There are two types of queue metrics. Global queue metrics, which include the JobQueue, SMTP Queue, and Task Queue, are collected by the monitor service. Service queue metrics are collected by individual services.
- Java Virtual Machine metrics for monitoring status information such as the length of time a JVM in the IBM Cognos BI environment has been running and how much memory it is using
These metrics are collected by the Java Virtual Machine.
- service request metrics for monitoring processing times, volume of requests, operational status of services, and response times
These metrics are collected by the dispatcher that manages the service.
- report service metrics for monitoring report service processes
These metrics are collected by the dispatcher that manages the report service.

The availability of a metric depends on the resource with which the metric is associated. For example, some metrics are available for the system, servers, dispatchers, and services. Other metrics may be available for only a subset of these resources.

You define the threshold values that determine whether the status for a resource indicates excellent performance (a green indicator), average performance (a yellow indicator), or poor performance (a red indicator). There are no default threshold values. If you define thresholds, the values are stored in the content store.

You can also create an agent that monitors the metrics and notifies you when threshold values are exceeded. For example, you can create an agent that sends you an email when a threshold value is exceeded.

When a threshold is exceeded, the dispatcher writes an entry to the logging database.

For information about system metrics, including how to define threshold values and notifications, see the *IBM Cognos Business Intelligence Administration and Security Guide*.

Database Tuning

The data source used by IBM Cognos BI is usually a relational database management system, such as IBM DB2, Microsoft SQL Server, or Oracle. To ensure that IBM Cognos BI continues to perform well, it is important to maintain the performance of your database.

This means optimizing it for querying, reporting, and analyzing. If IBM Cognos BI and other applications demand more of a database than it can provide, or queries are too large for a database to handle efficiently, you may experience increased response times and degradation in IBM Cognos BI performance and scalability.

For information about tuning your database, see its documentation.

Application Server Tuning

The Java application server contains the Content Manager servlet and dispatcher servlet. By default, IBM Cognos BI installs and uses IBM WebSphere Application Server Liberty Profile as the default application server. You can also configure IBM Cognos BI to use another Java application server.

Regardless of the application server you use, to enhance and maintain IBM Cognos BI performance, you should monitor memory settings and connection limits and tune them based on IBM Cognos BI usage characteristics.

Changing Memory Settings

The memory settings of your application server dictate the memory that is available to IBM Cognos BI dispatchers and services managed by the Java servlet.

In IBM Cognos Configuration, the default memory allocation is 768 Megabytes. If you expect many users and report requests, you may want to increase the memory allocation beyond the default.

The memory allocation strategy for your application server depends on the available capacity of your resources, and on the resource needs of other applications running on the server. In general, configure your application server with a minimum of 512 Megabytes of memory for multi-user applications. You may be able to reduce application server memory to 256 Megabytes, but you should only consider this for single users, or for proof of concept or demonstration applications.

To configure IBM WebSphere Application Server Liberty Profile memory settings, use IBM Cognos Configuration or alternative methods. For information about using IBM Cognos Configuration, see the *IBM Cognos Business Intelligence Installation and Configuration Guide*. If you use an application server other than IBM WebSphere Application Server Liberty Profile, consult the documentation for that product.

Setting Connection Limits

For the IBM Cognos BI dispatcher to service the expected number of requests, it is important to configure the connection limits of your application server. Depending on your application server, connections may be referred to as threads. The setting applied will determine the number of available connections, or threads, that can be handled simultaneously by the application server process.

If the value of this application server setting is too low, users may encounter difficulties when making IBM Cognos BI requests. It is a good practice to monitor the application server process and its use of connections.

To configure IBM WebSphere Application Server Liberty Profile, use the `server.xml` file located in the `<clt_location>/wlp/usr/servers/cognosserver` directory. For details see the IBM WebSphere Application Server Knowledge Center.

To configure Apache Tomcat connection settings, use the `\conf\server.xml` file located in the Tomcat directory in your IBM Cognos BI installation location. IBM Cognos BI uses the settings for the coyote connector.

Web Server Tuning

The default IBM Cognos BI gateway is CGI, which can be used with all supported Web servers. For improved performance, consider using a scalable gateway, such as Apache mod for Apache and IBM HTTP servers, or ISAPI for IIS Web servers.

For information about Web server scalability in IBM Cognos BI, see “Web Server and Gateway Scalability” on page 75. For information about tuning your Web server, see its documentation.

IBM Cognos BI Tuning

The way that you use and configure IBM Cognos BI can affect its performance. For example, you can design models and reports with performance in mind, configure IBM Cognos BI dispatchers and services for performance, and schedule jobs to make the best use of system resources.

Designing Models and Reports for Performance

Designing and creating models in Framework Manager is an important step in the IBM Cognos BI workflow. A model specifies, structures, adds to, and manages the metadata used to create reports. For optimal IBM Cognos BI performance, a modeler can design models that specify default prompting, and that set the query processing type.

Specifying Default Prompting

To improve query performance, models can include reports that prompt a user for a descriptive name, as well as perform filtering on a code or key value.

You can modify a model to ensure that queries sent to the data source are efficient, well formed, and secure. To ensure optimal performance, the Framework Manager modeler can

- specify the rules governing query generation
- restrict user access to specific rows or columns of data
- model data relationships to hide the complexity of data from report authors

For more information, see the *IBM Cognos Framework Manager User Guide*.

Setting Query Processing Type

For relational metadata, you can improve performance by selecting the appropriate type of query processing.

There are two types of query processing:

- limited local

The database server does as much of the SQL processing and execution as possible. However, some reports or report sections use local SQL processing.

- database only

The database server does all the SQL processing and execution. An error appears if any reports or report sections require local SQL processing.

Although the database server can usually run the SQL and run reports much faster, local processing is sometimes necessary. For example, choose limited local processing if you want to create cross database joins or if you want report authors to use unsupported SQL99 functions.

Some complex queries, such as a query that must generate an At clause to avoid double-counting, require limited local processing. In this case, the query automatically uses limited local processing even if the package was published with database only processing.

For more information, see the *IBM Cognos Framework Manager User Guide*.

Tuning IBM Cognos BI Dispatchers

IBM Cognos BI dispatchers manage the distribution of requests.

You can monitor IBM Cognos BI dispatchers using administration options. For more information, see “IBM Cognos Connection” on page 4.

In a distributed IBM Cognos BI environment, there are two or more servers, each with a dispatcher to manage the IBM Cognos BI request flow. The dispatcher is responsible for routing requests to the services configured on a particular IBM Cognos BI server.

An IBM Cognos BI server can be configured to handle a specified proportion of requests. This is especially important if you have servers of different capacity and must make granular changes to specific servers in your environment.

Setting the Process Capacity

Each IBM Cognos BI dispatcher is assigned a process capacity. It dictates the number of requests that will be handled by a server. By default, request distribution uses a weighted round-robin algorithm that distributes requests equally among all configured dispatchers. In this case, the process capacity for each dispatcher is assigned a weight of 1.0.

The process capacity should be configured according to the relative performance of each server. For example, consider a two-server topology. If all other variables are constant, a quad-processor server should be configured with a processor capacity of 2.0, and a dual-processor server given a processing capacity of 1.0. This means that in the two-server topology, one server receives twice the number of requests as the other.

For more information, see the *IBM Cognos Administration and Security Guide*.

Specifying Advanced Dispatcher Routing

Depending on how your system is set up, you may want to control how reports are distributed among servers. For example, you have different departments that maintain their own servers, or you have specific servers set up for specific data

access, such as Microsoft Windows operating system servers for Microsoft SQL Server databases and Linux operating system servers set up for DB2 access. You can set up IBM Cognos BI so that report requests are processed by specific servers by applying routing rules to specific packages, groups, and roles.

For more information, see the *IBM Cognos Administration and Security Guide*.

Tuning the Report Service, Batch Report Service, and Report Data Service

The report service, batch report service, and report data service have several settings that you can configure to optimize the use of resources.

There are a number of processes associated with the report service and the batch report service. For a complete list, see “IBM Cognos services” on page 11. When these services receive requests from the dispatcher, they start processes to handle the requests. You can specify the maximum number of processes that these services can start at any one time.

The number of processes should be configured based on the amount of available capacity provided by IBM Cognos BI servers. In general, report processing is a CPU-bound process. As a result, the number of CPUs in a server, and the clock rates of those CPUs, are the main variables to keep in mind when adjusting this setting from the default value of 2.

For example, a server with four available CPUs should generally be configured to use more batch report service processes than a server with only two available CPUs. Similarly, given two servers with an equal number of CPUs, the server with a significantly faster CPU clock rate should be configured to use more batch report and report service processes.

For the report data service, you can specify the maximum report size that can be sent.

For more information about server administration settings, see the *IBM Cognos Administration and Security Guide*.

Setting Affinity Connections

You can specify the maximum number of high affinity and low affinity connections that the dispatcher can open to handle requests. High affinity connections are used to process absolute and high affinity requests from the report services, while low affinity connections are used to process low affinity requests.

High Affinity Connections

A high affinity connection is used to handle a high affinity request, and each connection handles one request at a time. A high affinity request is a transaction that can benefit from a previously processed request. It can be processed on any of a number of servers, but resource consumption is minimized if the request is routed back to the report service process that was used to execute the original process.

Each report process has a configurable number of high affinity connections. The number of high affinity connections to set should be based on the number of low affinity connections set for each report process, as well as the capacity required for other services on the same server.

The distribution decision between high and low affinity connections per batch report process should be a function of the anticipated distribution of request types. For example, an HTML reporting application may have a greater likelihood of high affinity requests than a PDF reporting application. The page down request for an HTML report uses a high affinity connection whenever possible.

In general, the number of batch report service and report service processes should be the primary parameter to be optimized when deploying an IBM Cognos BI application. After system resource use is configured to operate efficiently, the number of affinity connections can be tuned for further optimization.

Note: If the number of affinity connections per process is set too high, the process may be overburdened with managing connections. This will result in competition for system resources, and requests will take longer to complete due to inefficient use of server resources.

Low Affinity Connections

A low affinity connection is used to handle a low affinity request. Each connection handles one request at a time. A low affinity request will operate just as efficiently on any server.

Both the report service and batch report service are capable of handling low affinity requests. Low affinity requests that have been initiated by scheduled activity will make use of the low affinity connections configured for a batch report service. Low affinity requests that have been initiated by user-driven activity will make use of the low affinity connections configured for a report service.

Each report and batch report process has a configurable number of low affinity connections. The number of low affinity connections per report service process should be set in coordination with the settings specified for the batch report service.

The distribution decision between high and low affinity connections per process should be a function of the anticipated distribution of request types. For example, an HTML reporting application may have a greater likelihood of high affinity requests than a mainly PDF reporting application. The page down request for an HTML report uses a high affinity connection whenever possible.

In general, the number of report service and batch report service processes should be the primary parameter to be optimized when initially deploying an IBM Cognos BI application. Once system resource use is configured to operate efficiently, the number of affinity connections can be tuned for further optimization.

Note: If the number of affinity connections per process is set too high, the process may be overburdened with managing connections. This will result in competition for system resources and requests will take longer to complete due to inefficient use of server resources.

Affinity Level of IBM Cognos BI Activities

IBM Cognos BI includes the following high affinity activities:

- Report Viewer links
 - Run again
 - Return

- HTML report navigation
 - Top page
 - Page up
 - Page down
 - Bottom page
- delivery options
 - Save
 - Save As
 - Print
 - Email
 - Viewing

IBM Cognos BI includes the following low affinity activities:

- report querying
 - reporting
 - report processing
- report authoring
 - metadata retrieval
 - query validation
- administrative
 - testing data source connections
 - adding objects (folders, jobs, schedules, etc.)
 - refreshing portal page

For more information about affinity, see “Request Affinity” on page 78. For information about setting affinity connections, see the *IBM Cognos Administration and Security Guide*.

Best Practices for Scheduled Reporting

The IBM Cognos Business Intelligence architecture differentiates between the processing of interactive and noninteractive requests. All requests that are initiated through user activity are processed by the report service, while scheduled or event-driven activity is processed by the batch report service.

Scheduled reporting is a critical aspect of any large-scale enterprise reporting solution. The effective management of low or noninteractive usage time periods, in combination with an organization's data refresh cycles, provides an opportunity for administrators to prepare as much information as possible during off-peak times for later retrieval by the greater business intelligence user community.

Use Jobs to Schedule Reports

Reports can be scheduled on an individual basis. However, if you have many reports to schedule, scheduling on a one-by-one basis can become burdensome. As an alternative, you can use jobs to execute scheduled activities.

A job is a container of processing activities that operates in a coordinated manner. Instead of scheduling individual reports, a job allows multiple reports to execute using the same schedule.

Each activity or step within a job can run concurrently, or be given a sequence ordering. The job service submits steps to the monitor service. The monitor service queues the job steps, and manages how many reports are forwarded to the batch report service depending on how it is configured.

All scheduled activity is managed by the monitor service. This service forwards tasks to different target services for processing and monitors their execution. For example, reports are forwarded to the batch report service.

Job Service Settings

The job service is responsible for retrieving job definitions from the Content Store, inspecting those definitions, and forwarding step execution requests to the monitor service.

Settings for the job service include the following:

- Maximum connections for job services during non-peak period
The maximum number of jobs during non-peak periods identifies a configurable limit to the number of jobs that can simultaneously execute during the specified non-peak period range.
- Maximum number of job service connections during peak period
The maximum number of jobs during peak periods identifies a configurable limit to the number of jobs that can simultaneously execute during the specified peak period range. If an application does not perform scheduled activity during the specified peak period range, this setting is inapplicable.

For information about these and other job and schedule service settings, see the *IBM Cognos Administration and Security Guide*.

Using Report Bursting

Report bursting is a method of producing a set of reports containing personalized content that is based on a common report definition. Bursting performs a single execution of a report; sections the content as required, typically based on security access; and distributes the sections to the appropriate users based on report content.

Bursting is a critical aspect of any large-scale enterprise reporting solution. The effective management of low or noninteractive usage time periods, in combination with an organization's data refresh cycles, provides an opportunity for administrators to prepare as much information as possible for later retrieval by the greater business intelligence user community. Report bursting in IBM Cognos BI streamlines information distribution. A report is created once, and separated out into multiple filtered report outputs that contain individualized content.

Report bursting offers scalability benefits and helps in the effective management of resources. It also reduces network traffic, minimizes database queries, and enables IBM Cognos BI to process multiple personalized reports in parallel.

For more information about bursting reports, see the *IBM Cognos Report Studio User Guide* or the *Software Development Kit Developer Guide*.

PDF Rendering

You can change PDF rendering settings to improve response time. If a user views a one-page document on an idle system, the CPU time is often less than one second. However, PDF files vary in size, and response time is limited by your network speed.

To improve response time, you can do the following:

- Turn off font embedding.

Embedding fonts can add 100 Kilobytes or more to each report. Where connection speeds are 56 Kbps or less, turn off font embedding.

- Avoid uncommon fonts.

When you turn off font embedding, report authors should avoid using any fonts that report consumers may not have installed on their computers. If report consumers do not have the font set used by report authors installed on their computers, a default font is substituted.

- Enable linearized PDF documents.

You can enable linearized PDF viewing, known as byte serving, which delivers documents to your users as the pages become available. This is enabled by default in the PDF rendering settings and Adobe Acrobat Reader.

For more information about PDF documents, see the documentation provided with Adobe Acrobat.

Low Bandwidth Connections

If you have users who access IBM Cognos BI using a dial-up connection, change PDF rendering settings to improve performance.

You can also reduce default page sizes in Query Studio and Report Studio. In heavy volume installations, the amount of HTML generated can be high. You can improve performance by lowering the default page size to reduce the amount of HTML initially passed back to the Web server and on to your users.

Disk Maintenance

Over time, data on a physical disk becomes fragmented, which can cause performance degradation when writing to or accessing from the disk. Disk defragmentation should be a regular system maintenance activity.

Performance for IBM Cognos Mobile

You can use various methods to estimate and control the performance of your IBM Cognos Mobile environment.

Estimate the bandwidth required by IBM Cognos Mobile

IBM Cognos Mobile sends compressed versions of reports from the server to the mobile device. The size of a compressed report might range from 2 KB for a single-page report that contains text and a crosstab, up to possibly 500 KB for a 10-page report that contains multiple detailed charts on every page.

Each version of a report is sent only once. It is then stored in a cache on the mobile device. A mobile user can then view the report any number of times on the device without consuming any additional bandwidth.

Other operations, such as browsing the content store and answering prompts, also consume bandwidth. The bandwidth consumed is proportional to that used by a desktop browser performing the same action, but smaller because extraneous formatting information would not be exchanged.

IBM Cognos Mobile engages in intelligent polling to detect changes on the server. In an idle state, each mobile device sends a small data message to the server every 24 hours. (Note that this value is configurable). If there is heavy usage, where a mobile device user runs many reports throughout the day and schedules many reports for delivery to the mobile device, the device automatically checks in with the server more frequently.

To estimate bandwidth costs, an administrator can use the following formula as a guide:

$(\text{number of users}) \times (\text{average size of a report}) \times (\text{number of adhoc reports run each day per user} + \text{number of scheduled reports sent to each user per day})$.

Estimate the required number of servers

The load generated by one user using IBM Cognos Mobile on a server (dispatcher) is similar to the load generated by the same user using the IBM Cognos desktop products.

The resources needed by a desktop user to browse folders, run reports, answer prompts and view the resulting report are approximately the same as the resources needed by a mobile user to perform the same actions. As a result, to estimate the number of servers needed for your mobile users you can use the same formula that you use to estimate the number of servers needed for your desktop users.

Estimating the size of a report

You can use typical reports to determine the size of the content that is transferred over the wireless carrier's network to the mobile device.

Procedure

1. Remove all reports from the mobile device.
2. Run the report that you want to know the size of.
3. On your desktop browser, type the following request: `http://servername/alias/cgi-bin/cognos.cgi/mobileService?mob_op=about`
4. If you have security enabled, log on.

Ensure that you log on as the same user that ran the report on the mobile device.

A small XML document appears. Within the document there is a section that looks like the following example showing the number 28. The actual number you see depends on your report:

```
<s2><inbox>28</inbox></s2>
```

Tip: Because you have only one report, only one number should appear. If you see multiple numbers separated by colons, this means that you did not delete all reports. You must delete all reports and repeat steps 1 to 3.

5. Type the following request, replacing the number 28 with the number that you obtained in step 4: `http://servername/alias/cgi-bin/cognos.cgi/mobileService?mob_op=downloadDB&mob_ir=28`

The response to this request is the actual report contents.

6. Save this response as a file, and record its size.
This file is what is transferred over the network.
7. Repeat these steps for a number of typical reports to get an idea of the amount of data that your mobile users use.

Advanced Report Processing Configuration Settings

By default, IBM Cognos BI is configured to process reports and other business intelligence transactions using a standard model applicable to all applications. You can change the default processing behavior for the IBM Cognos BI server by modifying entries in the `rsvpproperties` file.

Setting `rsvpproperties.xml` properties

The `rsvpproperties.xml.sample` file is located in the `c10_location/configuration` directory. Depending on your specific IBM Cognos BI application and on the demands placed on it, changing settings in the `rsvpproperties.xml` file may benefit performance.

To enable the `rsvpproperties.xml.sample` file, you must rename the file `rsvpproperties.xml` and restart IBM Cognos BI. This activity must be conducted on all IBM Cognos BI servers.

Settings in the `rsvpproperties.xml` file are very sensitive to change. Changing these properties may greatly impact the behavior of IBM Cognos BI. As a result, you should use discretion when changing these values. For more information, contact Cognos Software Services.

Chapter 9. Globalization Considerations

Many businesses perform transactions in the global market. In this environment, users speak different languages, work in different currencies, use different date and time formats, and expect different sorting orders.

IBM Cognos Business Intelligence provides a multinational reporting environment in which users can create reports and access data in different languages. Users can work in the IBM Cognos BI user interface using their preferred supported language and regional settings, or any combination of supported languages.

IBM Cognos BI supports both Unicode and non-Unicode data sources. A single installation of IBM Cognos BI supports multiple languages, and reports can be generated once for use in different languages.

If you will use IBM Cognos BI in a global environment, decide how to configure IBM Cognos BI so that interface elements and report contents appear in the languages that users need.

To configure IBM Cognos BI for a global environment, do the following:

- Ensure that all strings that appear in the IBM Cognos BI user interface are translated into the required languages.
- Add fonts to your IBM Cognos BI environment.
Ensure that the appropriate language packs were installed on all computers in the distributed installation to support the character sets you use.
- Customize language support to the user interface.
Add or remove user interface language support. You can also specify the language used in the user interface when the language specified in the user locale is not available.
- Ensure that users see reports, data, or metadata in their preferred language.
You can also specify the language a report is viewed in if the preferred language of the user is not available.
- Customize currency, numbers, dates, and times.
Ensure that these variables are formatted correctly for users in different locations.
- Configure your database.
Certain databases require specific configuration of the client or server software to enable multilingual reporting.

For information about installing and configuring IBM Cognos BI, see the *IBM Cognos Business Intelligence Installation and Configuration Guide*.

Locales

IBM Cognos BI supports various types of locale. By default, IBM Cognos BI ensures that all locales, which may come from different sources and in various formats, use a consistent format. That means that all expanded locales conform to a language and regional code setting.

In IBM Cognos BI, a locale specification consists of the following parts, separated by a dash (-):

- The first part is a two-character-set code, such as en, that specifies a language.
- The second part is a two-character-set code, such as us, that specifies a regional setting.

A locale specifies linguistic information and cultural conventions for character type, collation, format of date and time, currency unit, and messages. More than one locale can be associated with a particular language, which allows for regional differences.

Product Locale

The product locale controls the language of the user interface and all messages, including error messages.

Content Locale

The content locale consists of the language and region combinations that are supported for Content Manager objects, Framework Manager objects, Content Manager data formatting, report data formatting, report text (titles), and database data (if the database tool is configured to use locale).

Server Locale

The server locale ensures that all log messages are in one language. It is configured during installation. In a distributed environment, each IBM Cognos BI server obtains the server locale from Content Manager.

Do not change the server locale after specifying any IBM Cognos groups or roles as part of security modeling within your environment. As well, if more than one Content Manager exists in your IBM Cognos BI installation, ensure that the server locale is set to the same value for all Content Managers.

Author Locale

The author locale is based on content locale and is the locale used when a report or query specification is created. It determines model binding and literal data formats. Author locales must be supported by the metadata model on which the report is based.

User Locale

Determining the language and locale preferences of users and enforcing an appropriate response locale are important issues when you distribute reports in different languages.

A user locale specifies the default settings that a user wants to use for formatting dates, times, currency, and numbers. IBM Cognos BI uses this information to present data to the user.

IBM Cognos BI obtains a value for user locale by checking these sources, in the order listed:

1. authentication provider

If the authentication provider has locale settings that are configured, IBM Cognos BI uses these values for the user product and content locale.

2. user preference settings

If the user sets the user preference settings in IBM Cognos Connection, IBM Cognos BI uses these settings for the user product and content locale and for default formatting options. The user preference settings override the values obtained from the authentication provider.

3. browser cookie

Anonymous and guest users cannot set user preference settings. For these users, IBM Cognos BI obtains a user locale from the browser cookie stored on the computer.

Run Locale

Run locale refers to a user product and content locales for a specific IBM Cognos BI session. IBM Cognos BI obtains a value for run locale by checking these sources, in the order listed:

1. URL

2. user account object in the content store

3. account information from the authentication provider

Product locale is used, if specified. Otherwise, content locale is used.

4. language settings in the browser

Each entry in the locale list for the browser is checked against the product mapping table, and then against the content locale mapping table. For more information, see “Mapping Content Locale” on page 102.

5. server locale for the Content Manager computer

Adding Fonts to the IBM Cognos BI Environment

IBM Cognos BI uses fonts to render PDF reports on the IBM Cognos BI server and to render charts used in PDF and HTML reports.

To show output correctly, fonts must be available where the report or chart is rendered.

In the case of charts and PDF reports, the fonts must be installed on the IBM Cognos BI server. For example, if an IBM Cognos Report Studio user selects the Arial font for a report, Arial must be installed on the IBM Cognos BI server to properly render charts and PDF files. If a requested font is not available, IBM Cognos BI substitutes a different font.

Because HTML reports are rendered on a browser, the required fonts must be installed on the personal computer of each IBM Cognos BI user who will read the HTML report. If a requested font is not available, the browser substitutes a different font.

When creating reports, you must select fonts that your IBM Cognos server or users have installed. Microsoft delivers a broad selection of fonts with different language packs, so this will likely not be an issue in Microsoft Windows operating systems. However, UNIX operating system servers rarely have fonts installed. You should be prepared to purchase and install the fonts you need on both the server and browser clients.

When generating a PDF, IBM Cognos BI embeds only the glyphs that are used in the report.

If you plan to use different fonts, you must license and install those fonts on each server computer in your authoring environment and production system. You must also ensure that the fonts used in the authoring environment match the fonts used on your Windows and UNIX server computers.

For information about configuring fonts and about mapping substitute fonts, see the *IBM Cognos Business Intelligence Installation and Configuration Guide*.

Embedded Fonts

To ensure that PDF reports appear correctly in Adobe Reader, IBM Cognos BI embeds required fonts in reports by default. To minimize the file size, IBM Cognos BI embeds only the characters (also called glyphs) used in the report rather than all characters in the font set. IBM Cognos BI embeds fonts only if they are licensed for embedding. The license information is stored in the font itself and is read by IBM Cognos BI.

If you are confident that the fonts used in reports are available on users' computers, you can limit or eliminate embedded fonts to reduce the size of PDF reports. When limiting fonts, you specify whether a font is always or never embedded, using an embedded fonts list in IBM Cognos Configuration.

For more information about limiting embedded fonts, see the *IBM Cognos Business Intelligence Installation and Configuration Guide*.

IBM Cognos BI Default Font

If a requested font is not found, the IBM Cognos server renders PDF files and charts using a default font. The default font, Andale WT, is a sans serif font. While it has most of the Unicode characters for many languages, it is not necessarily complete for all languages and does not have the attractive appearance of most purchased fonts. Also, this font has no Glyph Substitution (GSUB) and Ligature support in most languages.

IBM Cognos Report Studio Fonts

IBM Cognos Report Studio is an HTML and Java-based application that runs in a browser. Because of the browser design, IBM Cognos Report Studio operates within the browser security sandbox and has no access to the list of fonts installed on the local computer. As a result, the list of fonts presented in IBM Cognos Report Studio depends on the fonts installed in the `c10_location\bin\fonts` directory of the IBM Cognos BI server. If the IBM Cognos BI server is installed on a Windows computer, IBM Cognos Report Studio also uses the fonts installed in the Windows font directory.

Changing the Language of the User Interface

In IBM Cognos BI, the product locale controls the language of the user interface and all messages, including error messages. By default, the language you choose to run the installation program becomes the product language. Users can choose another language at run time.

The product locale is different from the content locale. The language in the user interface does not control the language or content of reports, or the object names, descriptions, or tips in Content Manager.

To change the language of the user interface, do the following:

- Determine which languages will be supported in the user interface
- Ensure that translations exist for all strings that appear in the IBM Cognos BI user interface, in the languages you require.
- Install language files on all computers in your distributed environment.
- Add or remove user interface language support using the Product Locale table on each Content Manager computer.

By default, the user sees the product interface in the language that matches the language setting of the user locale.

For more information, see the *IBM Cognos Business Intelligence Installation and Configuration Guide*.

- Map unsupported languages to supported languages using the Product Locale Mappings table on each Content Manager computer.

You can then select the language to be used in the user interface when the language specified in the user locale is not available.

You can ensure that all regions for a locale use the same language, or that a specific, complete locale (language-region) uses a particular language.

Changing the Language of Reports, Data, or Metadata for Users

To ensure that users see reports, data, or metadata in their preferred language, or in a language specific to their region, add and remove partial locales (language) or complete locales (language-region) in the Content Locales table.

Adding incomplete locales (languages) to the IBM Cognos BI environment does not guarantee that your computer has a font that can show Web pages in your preferred languages. Ensure that you install the appropriate language packs to support the character sets you use. For more information, see “Adding Fonts to the IBM Cognos BI Environment” on page 99.

Content locale consists of the language and region combinations that are supported for the following:

- Content Manager objects
- Framework Manager objects
- Content Manager data formatting
- report data formatting
- report text (titles)
- database data, if the database tool is configured to use locale

Content locale does not apply to PowerCubes, whether they are created in IBM Cognos BI Transformer or IBM Cognos Series 7 Transformer. Each PowerCube is created with a single language encoding. For multiple languages, a separate PowerCube is required for each language.

If you have a multilingual model, you can specify the content locale of query data.

Users can create reports and access data using one of the supported languages, which include: English, French, German, Japanese, Dutch, Finnish, Swedish, Spanish, Italian, Portuguese, Traditional and Simplified Chinese, Korean, Czech, Hungarian, Polish, Romanian, Slovak, Greek, Turkish, Norwegian, Danish, and Russian.

The architecture is capable of supporting locales as well as additional languages. Therefore, it is possible to show data in two versions of English, each using a locale, such as en-us (English, United States) and en-ca (English, Canada).

User preferences allow the user to specify a locale or use the Web browser locale for both the product and content locale.

Mapping Content Locale

Some content is language-specific, such as names, and is called a partial locale. Some content is specific to language and region, such as date formats, and is called a complete locale. Use the Content Locale Mappings table to do the following:

- Ensure that users can access content that is language sensitive, but not locale sensitive.

For example, map a complete locale, such as en-us (English, United States), to a partial locale, en, to ensure that users can access content in English that is not subject to regional variation. For example, names and descriptions are usually specified by language, not locale.

- Ensure that users can access content that is locale sensitive.

For example, map a partial locale, such as en, to a complete locale, en-us, to ensure that users can access content that is locale sensitive, such as data format of dates and numbers. Data formatting is set by the combination of language and region and so requires a complete locale.

- Map a user-preferred language to another language.

For example, a report is not available in the preferred language, Vietnamese, but is available in French and German. You can use the Content Locale Mappings table to map Vietnamese to French or German. You then see the report in the mapped language.

- Map unsupported content locales to supported locales.

When you map partial locales, IBM Cognos BI does the mapping after checking for a user locale. If all users are using the same Web browser types, mappings behave the same way for all users. However, if you have multiple browsers, results vary.

For example, on Internet Explorer, locale identifiers for many European regions do not exist. In other words, the user locale of fr-fr (French, France) cannot be selected. Only the fr (French language identifier) is available. To correct the problem, fr can be mapped to fr-fr, so that the language-region value is returned. Netscape provides region identifiers, so locale mapping is not required to return a value of fr-fr. This distinction may produce inconsistent results for different browser users. On Internet Explorer, where fr is mapped to fr-fr, users receive content that is region specific (fr-fr). On Netscape, where fr does not return a value of fr-fr, users receive content that is not region specific.

User Choices

In a Framework Manager model, users can specify the column titles and column descriptions that they want to see in their own language. A report automatically switches to the user preferred language. No action is required by the author.

In Report Studio, users can specify a language or locale for

- report data items, such as calculations, that do not exist in the metadata model
- text in a report, such as the page title
- report layouts

Customizing Currency, Numbers, Dates, and Times

IBM Cognos BI provides a complete set of default locale formats for number, dates (short, long, complete, and abbreviated), times, intervals, and currencies across almost 200 locales. You can control whether all formatting or a selected subset of data is linked to the user locale.

For example, data in US currency can be shown with the US currency symbol (\$) and the format that is appropriate for the user locale. A French user may see 123,45 \$, and a US user \$123.45.

By default, IBM Cognos BI shows only a subset of supported currencies in the user interface. You add or remove currencies in the Currency table on each Content Manager computer.

When users are prompted for numerical data, IBM Cognos BI automatically accepts the data in the user locale format.

Support for Japanese Users

Dates in an Imperial calendar are entered and shown using the year, which can be specified as a year or a given emperor's reign.

Users have the option of using English year and month names for either the Imperial or Gregorian calendar.

IBM Cognos BI supports Sankaku negative signs. In the following table, a triangle is used in place of the western negative sign (-).

Table 4. Sankaku negative signs

Symbol	Shift-JIS	Unicode
△	0x81A2	U+25B3
▲	0x81A3	U+25B2
▽	0x81A4	U+25BD
▼	0x81A5	U+25BC

Setting up a Multilingual IBM Cognos BI Environment

You can create reports that show data in more than one language and use different regional settings. This means that you can create a single report that can be used by report consumers anywhere in the world.

You can combine data sources from multiple locales. If you use an IBM Cognos Series 7 PowerCube as a data source, IBM Cognos BI converts the cube data from the encoding that was used on the system where the PowerCube was created. For a successful conversion, IBM Cognos Series 7 PowerCubes must be created with a system locale set to match the data in the PowerCube. After conversion in IBM Cognos BI, PowerCubes from multiple locales can be combined with no concern about server locale.

The samples databases provided with IBM Cognos BI store a selection of text fields, such as names and descriptions, in more than 25 languages to demonstrate a multilingual reporting environment. For information about how data is stored in the samples databases and how the samples databases are set up to use multilingual data, see the *IBM Cognos Administration and Security Guide*.

Here is the process for creating a multilingual reporting environment:

- Use multilingual metadata.

The data source administrator can store multilingual data in either individual tables, rows, or columns.

For more information about configuring your database for multilingual reporting, see the *IBM Cognos Administration and Security Guide*.

- Create a multilingual model.

Modelers use Framework Manager to add multilingual metadata to the model from any data source type except OLAP. They add multilingual metadata by defining which languages the model supports, translating text strings in the model for things such as object names and descriptions, and defining which languages are exported in each package. If the data source contains multilingual data, modelers can define queries that retrieve data in the default language for the report user.

For more information, see the *IBM Cognos Framework Manager User Guide*.

- Create multilingual maps.

Administrators and modelers use a Microsoft Windows operating system utility named Map Manager to import maps and update labels for maps in Report Studio. For map features such as country or region and city names, administrators and modelers can define alternative names to provide multilingual versions of text that appears on the map.

For more information, see the *IBM Cognos Map Manager User Guide*.

- Create a multilingual report.

The report author uses Report Studio to create a report that can be viewed in different languages. For example, the report author can specify that text, such as the title, appears in German when the report is opened by a German user. Report authors can also add translations for text objects, and create other language-dependent objects.

For more information, see the *IBM Cognos Report Studio User Guide*.

- Specify the language in which a report is viewed.

You can use IBM Cognos Connection to do the following:

- Define multilingual properties, such as a name, screen tip, and description, for each entry in the portal.
- Specify the default language to be used when a report is run.

Tip: You can specify the default language on the run options page, in the report properties, or in your preferences.

- Specify a language, other than the default, to be used when a report is run.
- For more information, see the *IBM Cognos Connection User Guide*.

The data then appears in the language and with the regional settings specified in

- the user's Web browser options
- the run options
- the IBM Cognos Connection preferences

Any text that users or authors add appears in the language in which they typed it.

Configuring a Database for Multilingual Reporting

IBM Cognos BI is a Unicode product capable of querying and encoding data in many languages. IBM Cognos BI typically queries the database using the native data encoding of the database, such as Latin-1, Shift-JIS, and Unicode. IBM Cognos BI translates this data to Unicode as required.

When querying databases with two or more data encodings, Report Studio requests the data in Unicode. Some databases require specific configuration of the client or server software to enable this capability. For more information, see the database documentation.

Round Trip Safety Configuration of Japanese Characters

Shift-JIS is the Japanese character encoding system. If characters are converted from Unicode to Shift-JIS and back to Unicode, round trip safety issues can arise. These can be avoided by using the Round Trip Safety Configuration utility. This utility is located in *c10_location\bin* and is named *rtsconfig.exe*.

The Round Trip Safety Configuration utility ensures the round trip safety of Shift-JIS characters only when it is used to convert the characters both from Shift-JIS to Unicode and from Unicode to Shift-JIS. If data is requested from a database that has its own conversion mechanism to convert the Shift-JIS characters to Unicode automatically, IBM Cognos BI does not call the Round Trip Safety Configuration utility to convert the characters back to Shift-JIS. In this situation, the round trip safety of characters in the data cannot be ensured.

Chapter 10. Security Architecture

IBM Cognos Business Intelligence provides a security architecture that is flexible and compatible with your existing security model. It is easily integrated with authentication and cryptographic providers.

IBM Cognos BI security involves the following:

- IBM Cognos Application Firewall
- IBM Cognos authentication services
- IBM Cognos authorization services
- Cryptographic services

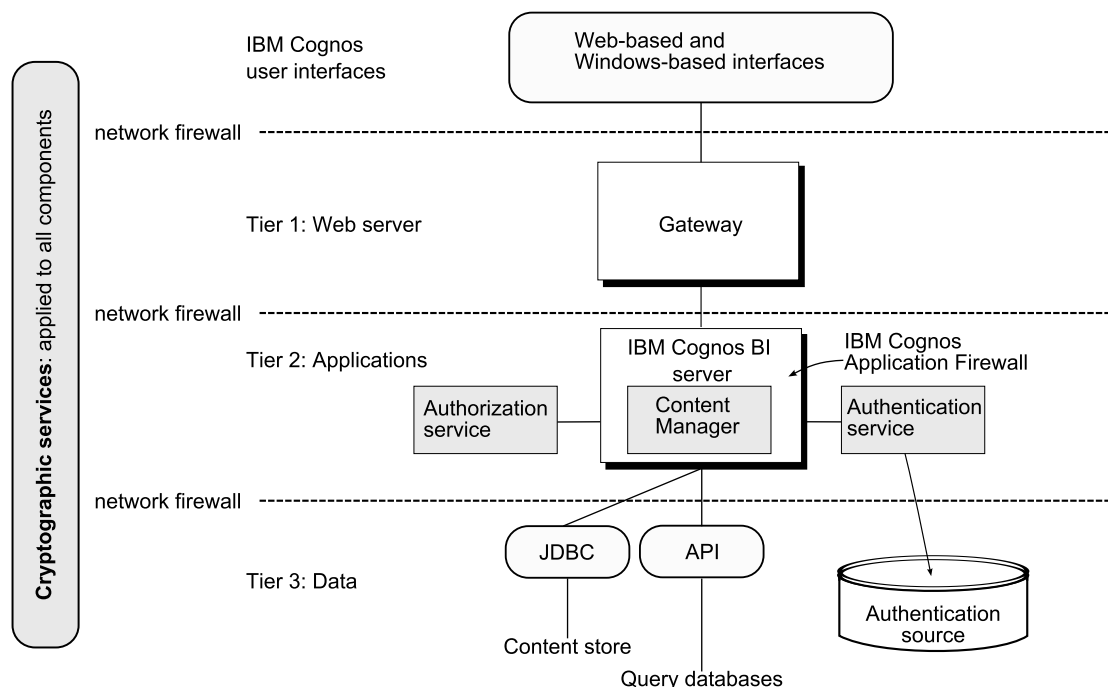


Figure 37. A graphic showing the IBM Cognos architecture and highlighting the security components

For information about setting up security in IBM Cognos BI, see Chapter 11, "Securing the Deployment," on page 113.

IBM Cognos Application Firewall

IBM Cognos Application Firewall validates and filters incoming and outgoing traffic at the dispatcher layer.

IBM Cognos Application Firewall features include request validation, SecureError, and parameter signing. It also has a flexible architecture that can be updated to keep your IBM Cognos BI security current.

IBM Cognos Application Firewall is an essential component of IBM Cognos BI security, helping to provide protection against penetration vulnerabilities such as cross-site scripting. Disabling the IBM Cognos Application Firewall will remove

this protection, and should not be done under normal circumstances. For more information, see “Recommendation - Use IBM Cognos Application Firewall” on page 118.

For information about configuring IBM Cognos Application Firewall, see the *IBM Cognos Business Intelligence Installation and Configuration Guide*.

IBM Cognos Authentication Services

Authentication is the process of identifying individuals before allowing them to log on.

Authentication in IBM Cognos BI is integrated with third-party authentication providers. Authentication providers define users, groups, and roles used for authentication. User names, IDs, passwords, regional settings, and personal preferences are some examples of information stored in the authentication source accessed by the provider. An authentication namespace is an instance of a configured authentication provider.

To set up authentication for IBM Cognos BI, you must configure IBM Cognos BI using one or more of these authentication providers:

- LDAP
- Microsoft Active Directory
- IBM Cognos 7 namespaces created using IBM Cognos 7 Access Manager and available with other IBM Cognos products
- eTrust SiteMinder
- Custom Java provider

For information about configuring third-party authentication providers, see the *IBM Cognos Business Intelligence Installation and Configuration Guide*. For information about creating a custom authentication provider, see the *Custom Authentication Provider Developer Guide*, available when you purchase the IBM Cognos software development kit.

For information about anonymous access and authenticated access, see “Request Flow Processing” on page 26.

Cognos Namespace

IBM Cognos BI has its own namespace that exists regardless of any additional namespaces that are configured based on third-party authentication providers. The Cognos namespace does not replicate the groups and roles defined in your authentication provider. Instead, you may want to use the Cognos namespace to define groups and roles that can span multiple third-party authentication providers. This practice can add value to your existing groups and roles by reorganizing them for IBM Cognos BI without changing them in your authentication provider.

You can use the Cognos namespace to set up security that links easily with client security systems. For an example, see “Using the Cognos Namespace to Restrict Access” on page 123. For more information, see the *Administration and Security Guide*.

Single Signon

You can configure IBM Cognos BI for single signon. Users can then sign on once to an environment that includes IBM Cognos BI and other programs, without having to sign on each time they move between programs. Implementation of a single signon solution depends on the environment and authentication provider configuration.

For more information, see the *IBM Cognos Business Intelligence Installation and Configuration Guide*.

IBM Cognos Authorization Services

Authorization is the process of granting or denying access to data, and specifying the actions that can be performed on that data, based on a user identity. For example, IBM Cognos BI administrators can set up folders in which reports are stored. They can then secure those folders so that only authorized users can view, change, or perform other tasks using the reports in the folder.

Authorization services are provided in Content Manager.

Distributed Administration

The IBM Cognos BI security model supports the distribution of security administration.

Because objects in Content Manager, such as folders and groups, can be secured separately, security administration can be assigned to individuals in separate functional areas of the organization. Security administration does not have to be centralized with an Information Technology group or other overall administration group.

Permissions

Permissions define access rights to objects, such as directories, folders, and other content, for each user, group, or role. Permissions also define the activities that can be performed with these objects.

IBM Cognos BI authorization assigns permissions to

- groups and roles created in the Cognos namespace in Content Manager. These groups and roles are referred to as IBM Cognos groups and IBM Cognos roles.
- entire namespaces, users, groups, and roles created in third-party authentication providers.

Users

A user entry is created and maintained in a third-party authentication provider to uniquely identify an account belonging to a person or a computer. You cannot create user entries in IBM Cognos BI.

The user entry stored in the authentication provider may include information such as first and last names, passwords, IDs, locales, and email addresses. However, IBM Cognos BI may require additional information, such as the location of the users' personal folders or their format preferences for viewing reports in the portal. This additional information is stored in IBM Cognos BI.

You can assign users to groups and roles defined in the authentication provider and in IBM Cognos BI. A user can belong to one or more groups or roles. If users are members of more than one group, their access permissions are merged.

For more information about users, see the *IBM Cognos Administration and Security Guide*.

Groups and Roles

Groups and roles represent collections of users who perform similar functions, or have a similar status in an organization. Members of groups can be users and other groups. Members of roles can be users, groups, and other roles.

Both groups and roles are used to assign access permissions in IBM Cognos BI. Users always log on with all the permissions associated with the groups and roles to which they belong.

For more information about groups and roles, see the *IBM Cognos Administration and Security Guide*.

Cryptographic Services

Cryptographic services ensure that IBM Cognos BI communications and sensitive data are secure.

Encryption is used to secure

- static data
- temporary data
- transient data

You can use the built-in IBM Cognos BI certificate authority (CA) or a supported third-party CA, such as Entrust. To use a third-party CA, you must purchase and install appropriate software before you configure the new cryptographic resource. To use encryption with Entrust, you must purchase and install an Entrust Public Key Infrastructure (PKI), which includes its own CA. The PKI must be available before you configure the a new cryptographic resource for use with the Entrust security infrastructure.

For more information, see “Configuring the Cryptographic Environment” on page 119.

Using a Third-party Certificate Authority

IBM Cognos BI relies on the functionality of a certificate authority (CA) to provide cryptographic services.

By default, IBM Cognos BI provides a simple built-in CA. You may choose to disable it and use a third-party CA. You can use any third-party CA that generates Base-64 encoded X.509 certificates. For more information, see the *IBM Cognos Business Intelligence Installation and Configuration Guide*.

IBM Cognos Cryptographic Provider

The IBM Cognos cryptographic provider is included with IBM Cognos BI.

It includes the following:

- secure sockets layer (SSL) services

The SSL protocol is used to secure communication between IBM Cognos BI components installed on the same computer or on different computers.

- trusted requests on BI bus messages

Signatures are used to digitally sign some messages to ensure that they come from a recognized IBM Cognos service.

- encryption of the deployment process

Symmetric algorithms are used to encrypt and decrypt data in the export and import processes.

- encryption of temporary files

Symmetric algorithms are used to encrypt and decrypt temporary files.

Data stored in the database depends on database security to protect it.

The IBM Cognos cryptographic provider can be used with the built-in certificate authority (CA) or with a third-party CA.

Chapter 11. Securing the Deployment

The primary goals of the IBM Cognos Business Intelligence security strategy are

- to limit access to authorized data to the intended users
- to prevent modification of the data, or data presentation, by unauthorized users
- to prevent the theft or destruction of information
- to ensure that the application is available

You must ensure that users cannot, either through inadvertent or malicious actions, view data that they are not authorized to view, bypass authentication and authorization mechanisms, steal or violate session states to assume the identity of another user, or escalate existing privileges. You must also prevent users from causing disruptions in service for the application.

This information will help you configure an IBM Cognos BI installation for maximum security. The issues discussed include the environment security, which involves the operating system and network security, and the application security. All of these areas were considered during the security audit that was conducted on IBM Cognos BI as part of the developmental cycle.

Each customer's installation and configuration of IBM Cognos BI is unique. As a result, the security requirements for each installation and configuration are also unique. This section does not contain complete information about issues involved in securing an IBM Cognos BI environment. However, it provides guidelines and recommendations that supplement the more detailed information in the *IBM Cognos Business Intelligence Installation and Configuration Guide*.

The IBM Cognos BI security framework is based on the industry standard approach to securing Web applications. This involves addressing security issues during the design and development of functional areas that are vulnerable to security threats.

The following IBM Cognos BI functional areas were developed with special attention to security.

Authentication and Authorization

User authentication and authorization prevent unauthorized users from accessing system components and data.

The effectiveness of the security strategy depends on the type of authentication and authorization.

Web Request and Content Validation

Web request and content validation checks the data before the data is processed.

The effectiveness of the security strategy depends on the validation techniques, such as bounds checking that prevents buffer overflow and variable assignment violations, and format checking that prevents data encoding and format string violations.

Session Management

Session management supports appropriate access control. It relies on strong session identifiers that are difficult to guess.

The effectiveness of the security strategy depends on the type of session management systems used, the information that they include, and where in the program cycle the sessions are validated.

Transport Security

Transport security is used during transmission to secure transactions that contain sensitive information when untrusted networks are used.

The effectiveness of the security strategy depends on how data is encrypted.

Encryption

Encryption protects sensitive data, such as account credentials and personal information.

The effectiveness of the security strategy depends on how data is encrypted and stored.

Logging and Monitoring

Application logs identify when errors occur or when sensitive transactions are complete. In addition, application logs record error messages that provide system information. Error messages should expose the minimum amount of information to meet business requirements.

The effectiveness of the security strategy depends on where the log files are stored, and whether auditing capabilities are built into the application.

Administration

Administrative access includes the right to add and remove users, provide group and role-based access, and configure application components. Administrative access should be restricted to appropriate individuals.

The effectiveness of the security strategy depends on how the application is administered, the configuration of administrative options for security, and how these options are protected.

Techniques for Securing the Operating System

The operating system is the physical environment where your application runs. Any vulnerability in the operating system could compromise the security of the application. By securing the operating system, you make the environment stable, control access to resources, and control external access to the environment.

The physical security of the system is essential. Threats can come through the Web, but they can also come from a physical terminal. Even if the Web access is very secure, if an attacker obtains physical access to a server, breaking into a system is much easier.

Review security policies and recommendations for your operating system. Consider implementing the following security best practices.

User Accounts

- Limit the number of user accounts on the server computers.
Unnecessary and legacy user accounts increase system complexity and may present system vulnerabilities.
Fewer user accounts reduces the amount of time administrators spend on account administration.
- Ensure that only a few trusted users have administrative access to the server computers.
Fewer administrators make it easier to maintain accountability. The administrators must be competent.
- Assign the minimum required access permissions for the account that runs the application.
If attackers obtain access to the application, they have the permissions of the user who runs the application.

Account Policies

- Develop and administer password policies that promote operating system security.
Examples of such policies are the strong password rule and the password change schedule.
- Test the strength of users' passwords by breaking the passwords.
The users who do not comply with the strong password rule receive a notification to update their passwords according to the organization password policy.
Software is available to help you with this task.
- On a UNIX operating system, activate the shadow password file.
On UNIX, passwords are stored in the `/etc/passwd` file. This file is open to everyone, which presents a security risk. To enhance password security, activate the shadow password file named `/etc/shadow`. If this file is available, passwords are stored in it instead of the `passwd` file. Because permissions for the `/etc/shadow` file are more restrictive, the security risk is lower.

File System

- Grant the users read-only permissions for required directories.
If attackers obtain access to an application, they have the user permissions.
- Deny access by default.
Access to resources is denied for everyone except for the users to whom access is granted explicitly.
You can deny read and write permissions for all directory structures for all users. Only users to whom these permissions are granted explicitly have access to the directories and files. This policy also protects any resources that were overlooked by an administrator.

Network Services

- Provide the minimum number of required services on the server computer.
Use only the services that you need to run the application. Each service is a potential entry point for a malicious attack. Reducing the number of running services also makes your system more manageable.

For example, you may not need the ftp, rlogin, or ssh services.

- Reduce the level of access permissions for the network services users.

Network services are exposed to the public.

- Ensure that the user accounts that have access to the Web server do not have access to the shell functions.
- Ensure that unused services do not exist in the rc files, rc0 through to rc6, in the /etc directory on UNIX and Linux operating systems.
- Ensure that unused services are not running, and that they do not start automatically on Microsoft Windows operating systems.
- Ensure that required services are running on UNIX.

You can use the ps and netstat utilities to see the running services. The ps utility gives a list of processes currently running on the computer. The netstat utility provides a list of ports that are currently in use.

- Reduce the number of trusted ports specified in the /etc/services file.
Delete or comment out the ports that you do not plan to use to eliminate possible entry points to the system.
- Protect your system against NetBIOS threats associated with ports 137, 138, and 139.

These ports are listed in the /etc/services file.

- Use wrapper services, such as iptables.
- Ensure that the services are current by checking often for security updates.
- Avoid using services that have a graphical user interface (GUI), if possible.

Such services introduce many known security vulnerabilities.

System Patches

- Run the latest, vendor-recommended patches for the operating system.
The patches may be core OS patches, or patches required by additional applications.
- Schedule regular maintenance of security patches.

Operating System Minimization

- Remove nonessential applications to reduce possible system vulnerabilities.
- Restrict local services to the services required for operation.
- Implement protection for buffer overflow.

You may need third-party software to do this.

Logging and Monitoring

- Log security-related events, including successful and failed logons, logoffs, and changes to user permissions.
- Monitor system log files.
- Use a time server to correlate time for forensics.
- Secure the system log files by restricting access permissions to them.
Logs are important for daily maintenance and as a disaster recovery tool. Therefore, they must be protected from system failures and user tampering.
- Use IPF logging to build a more sophisticated logging system.

To increase the security of the log file system, you can

- place all log files in one location, on one server

This simplifies the administration of log files.

- set up multiple logging servers for redundancy
- use a remote server for logging

This protects the logs if the system is compromised and, for example, the hard drive is destroyed.

Because an IPF server is accessed through the network, it can be located anywhere in the world.

- Secure the logging configuration file.

The configuration file contains settings that, if changed, can compromise the reliability of the log system. For example, setting the log level incorrectly may cause some failures not to be logged.

- Enable logging of access requests on the Web server.

This can be useful in identifying malicious activity.

System Integrity

- Build production systems from a known and repeatable process to ensure the system integrity.
- Check systems periodically against snapshots of the original system.
- Use available third-party auditing software to check the system integrity.
- Back up the system resources on a regular basis.

Techniques for Securing the Network

The network is the entry point to an application. Therefore, the network security mechanisms are the first line of defense against potential threats from the outside. Network security involves protecting the protocols and the communication channels, as well as devices, such as the router, the firewall, and the switch.

Consider implementing the following best practices to enhance your network security:

- Use a firewall.

This will allow only legitimate access to the network.

- Ensure that the firewall provides packet forwarding and filtering.

These firewall features introduce an additional layer of protection. Forwarding packets prevents the outside world from direct contact with the computers inside the protected network. Filtering can block some types of requests, or requests that come from some domains or IP addresses. These techniques help to reduce the number of illegitimate requests that can be passed to the internal network.

- Limit the number of accessible ports.
- Limit the traffic direction on some ports.
- Limit some network protocols, such as ping.

Web Servers

Consider implementing the following security best practices for all types of Web servers:

- Remove any unused virtual directories.
- Remove or disable example default cgi-bin or ASP scripts provided with your web server application. For example: Apache: cgi-bin/printenv.pl.
- Grant read, write, and execute permissions explicitly for each Web site and virtual directory.

- Create a root directory for the Web server.
For Apache, this is known as chrooting.
For Microsoft Internet Information Services (IIS), you can assign the root Web site to a specific directory. The user who runs IIS can be given read and write permissions for this directory. All other user permissions can be removed.
- Ensure that access permissions for the physical files are set up properly.
Only some users require read and write permissions for these files.
- Remove unwanted default mappings, such as for applications with the .httr, .idc, .stm, .printer, and .htw file extensions.
- Enable secure sockets layer (SSL) on the Web server.
SSL is used to encrypt a user's communication with the Web server. For more information, see the section about configuring the Web server in the *IBM Cognos Business Intelligence Installation and Configuration Guide*.

For Apache, also implement the following best practices:

- Enable only the required modules.
- Ensure that your Apache installation hides version information and other sensitive information.
- Turn off directory browsing.
- Configure the Web server to restrict access by IP address.
- Ensure that error logging and access logging are enabled.

These types of logging are controlled by the ErrorLog and mod_log directives in the configuration file.

For IIS, also implement the following best practices:

- Disable protocols, such as ftp, if they are not used.
- Enable logging in the configuration tool.
- Disable Remote Data Service if it is not required.
- Remove sample applications, such as \IISamples, \IISHelp, and \MSADC.
- Set access permissions for the winreg registry key.
Only administrators require access to this key.

Securing the Application

Using the built-in security features, you can configure an IBM Cognos BI installation for maximum security.

The best practices provided here are not a complete list of all configuration tasks required to secure your application. However, they address the most critical issues that include IBM Cognos Application Firewall, the cryptographic environment, the SSL protocol, and the temporary files. They also address securing access to IBM Cognos Connection, IBM Cognos PowerCubes, data source signons, and the content store.

Recommendation - Use IBM Cognos Application Firewall

IBM Cognos Application Firewall (CAF) supplements the existing IBM Cognos BI security infrastructure. By default, this supplemental security is enabled. To ensure that the IBM Cognos BI solution is secure, CAF should never be disabled in a production environment.

In a distributed environment, all CAF settings must be the same for all computers where IBM Cognos BI Application Tier Components are installed. If CAF is disabled on some computers and enabled on others, unexpected behavior and product errors may result.

CAF protects the IBM Cognos BI components from processing malicious data. The most common forms of malicious data are buffer overflows and cross-site scripting attacks (XSS links), either through script injection in valid pages or redirection to other Web sites.

Using IBM Cognos Configuration, you can change settings for third-party XSS tool support, and add host and domain names to the IBM Cognos list of valid names.

You can also track firewall activity by checking the log file, which contains rejected requests. By default, log messages are stored in the *c10_location\logs\cogserver.log* file.

Configuring the Cryptographic Environment

Assess the level of security required for your environment before setting up the system.

Typical factors that influence the decision how secure a system must be, include

- external exposure

Who are the users? Are there internal users as well as external or guest users?

- use of the public Internet

Is the system accessible by the Internet? Does a virtual private network (VPN) exist?

- data sensitivity

Departments such as human resources, finance, and accounting likely want the data protected the best way possible.

For more information about cryptography in IBM Cognos BI, see “Cryptographic Services” on page 110. For more information about configuring the cryptographic settings, see the *IBM Cognos Business Intelligence Installation and Configuration Guide*.

Cryptographic Providers and Cipher Strength

IBM Cognos BI components require a cryptographic provider to run. If you delete the default cryptographic provider, you must configure another provider.

You can configure cryptographic providers for use with a supported certificate authority, such as Entrust.

When choosing the cryptographic provider, cipher strength should not be the main concern. The encryption provided by the IBM Cognos provider is secure enough for most applications. A high-security setup relies not only on the cipher strength, but on the security of the whole system, which includes physical access to directories, password policies, and so on. If your environment is exposed to the Internet and deals with highly sensitive data, you should consider using a third-party certificate authority.

The Certificate Authority (CA)

When you implement the IBM Cognos cryptographic provider, the IBM Cognos BI certificate authority, AutoCA, is used by default. AutoCA signs the internal certificates and provides all the functionality needed to establish the root of trust in the IBM Cognos security infrastructure.

AutoCA is sufficient for simple setups and test environments, but has limitations in development and production environments. For example, it cannot provide full administration capabilities for issued and revoked certificates, issue certificates based on purpose, such as mail, server, and private certificates, or sign the Web server and client certificates.

If you intend to enable SSL for the Web server or application server, or use client certificates, you need a third-party CA. This can likely be a CA that your organization already implemented as part of its security infrastructure. When using a third party CA, the necessary certificates must be generated and imported. For more information, see the section about configuring IBM Cognos BI components to use a third-party certificate authority in the *IBM Cognos Business Intelligence Installation and Configuration Guide*.

For internal systems that are not exposed to the Internet, you can set up your own CA using the open source software OpenSSL.

IBM Cognos BI does not support self-signed certificates because they do not adhere to the public key infrastructure (PKI) principles.

Supported Cipher Suites and Application Servers

In distributed installations, you must specify the same set of cipher suites for all installation components. Mixing ciphers, especially high-numbered ciphers with low-numbered ciphers, can cause problems. The sets must contain at least one common suite. Otherwise, the SSL negotiation fails and the connection cannot be established.

The cipher suites are also affected by the application server that is used to run IBM Cognos BI. If WebSphere Application Server is used, the IBM Cognos code generates the server certificates and switches WebSphere Application Server to SSL listeners. The cipher suites configured in IBM Cognos BI are the only ciphers that can be used. If an application server other than WebSphere Application Server is used, SSL must be enabled on the application server before the cipher suites are configured in IBM Cognos BI. Ensure that the set of cipher suites you specify in IBM Cognos Configuration contains at least one of the cipher suites configured on the application server. Otherwise, the SSL connection will not initialize.

Specify the list of cipher suites in priority sequence where the higher-numbered ciphers appear first.

Enabling SSL

When you use secure sockets layer (SSL), you protect the data crossing between the Web servers, application servers, and LDAP servers. Except for the Web servers, the servers are internal and protected by a firewall. You can usually rely on the network security for external network links. If this security is not enough, SSL should be enabled for communications between IBM Cognos BI components and other servers.

Enabling SSL requires a certificate authority (CA), and an administrator with a good knowledge of the public key infrastructure (PKI) technology and SSL.

You can configure IBM Cognos components to use the SSL protocol for:

- internal connections

If you configure SSL only for internal connections, IBM Cognos components on the local computer communicate using this protocol. The dispatcher listens for secure connections on a different port than for remote, HTTP requests. Therefore, you must configure two dispatcher URIs.

If you use WebSphere Application Server to run IBM Cognos BI, you configure the SSL protocol in IBM Cognos Configuration. If you use a different type of application server, the SSL protocol must be configured on the application server.

- external connections

If you configure SSL only for external connections, communications from remote IBM Cognos components to the local computer use the SSL protocol. You must configure the dispatcher to listen for secure remote requests on a different port than local HTTP requests. You must also configure the Content Manager URIs and the dispatcher URI for external applications to use the same protocol and port as the external dispatcher.

For externally accessible Web servers, SSL should always be enabled. For more information, see the *IBM Cognos Business Intelligence Installation and Configuration Guide*.

- internal and external connections

If you configure SSL for all connections, the dispatcher can use the same port for internal and external connections. Similarly, if you do not use SSL for local or remote communication, the dispatcher can use the same port for all communications.

You must also update the Content Manager URIs, dispatcher URI for external applications, and Gateway URI to use SSL, if required.

- LDAP connections

If you use an LDAP directory server, you can enable LDAPS, the secure LDAP protocol, for communications between the Access Manager component of Content Manager and the LDAP directory server. Unsecured LDAP traffic is transmitted as clear text.

To enable LDAPS, you must install a server certificate that is signed by a certificate authority (CA) in your directory server, create a certificate database to contain the certificates, and configure the directory server and the IBM Cognos BI LDAP namespace to use LDAPS.

For more information, see the sections about configuring LDAP authentication providers in the *IBM Cognos Business Intelligence Installation and Configuration Guide*.

For more information about configuring the SSL protocol, see the *IBM Cognos Business Intelligence Installation and Configuration Guide*.

Choosing a Location for the Common Symmetric Key

The common symmetric key (CSK) is used to encrypt and decrypt data between components in your IBM Cognos BI installation. The CSK can be stored locally or it can be requested each time a cryptographic operation is made. The default is to store the key locally.

Requesting the CSK for each cryptographic operation provides more security, but it may affect performance. Storing it locally provides better performance, but it may also expose it if the computer's security is compromised.

Requesting the CSK for each cryptographic operation is intended only for the gateway computer in cases where you have installed the IBM Cognos BI gateway separately from Content Manager or the Application Tier Components. Storing the CSK locally on your Content Manager and Application Tier Component computers is adequate as those components would be behind your firewall, while the gateway may not be.

Securing Temporary Files

IBM Cognos BI uses temporary files during reporting activities to store recently viewed reports. The files are not encrypted. Because the reports can contain sensitive data, they should be secured.

Implement the following measures:

- Restrict access to the temporary files directory.
Grant read and write permissions for the temp directory only to the IBM Cognos service account. Deny all other accounts any access.
The temp directory can be in the default *c10_location\temp* location, or in a different location, as specified in IBM Cognos Configuration.
- Enable encryption of temporary files.
Because encrypted content is unintelligible, it is useless for potential attackers.
Encrypting temporary files may affect performance.

For more information, see the section about configuring temporary files properties in the *IBM Cognos Business Intelligence Installation and Configuration Guide*.

Securing IBM Cognos BI Files

To protect the files that IBM Cognos BI uses, ensure that only authorized users have access to the directories that are used. This includes the installation directory (*c10_location*) and directories where files may be stored as backups or exported deployment archives.

To further secure your IBM Cognos BI files, follow these guidelines:

- Apply execute permission only to the *c10_location\cgi-bin* directory.
- Remove the *cm_tester.htm* file from the *c10_location\webcontent* directory.
- Edit the properties of the *cogstartup.xml* file in the *c10_location\configuration* directory to only allow Read and Write access for the user account under which IBM Cognos BI runs.

Protecting CAM password cookies

Setting the HTTPOnly attribute instructs a user's web browser to block scripts from being able to read or manipulate the CAM Passport cookie. CAM Passport identifies a user's session to the server. Setting HTTPOnly helps mitigate against malicious scripts attempting to steal a user's session identity.

Such scripts may be inserted into the browser using a Cross Site Scripting (XSS) attack on the same server or web application that the user has authenticated to.

Administrators who want to enable this feature should ensure that users have a browser that supports the HTTPOnly attribute.

Techniques for Securing Access to IBM Cognos Connection

When you add an authentication provider in IBM Cognos Configuration, all users in the directory have access to IBM Cognos Connection. To secure IBM Cognos BI, you must restrict this access.

The methods and best practices discussed in this section apply mostly to the LDAP authentication providers, Oracle directory server and Active Directory.

Use whichever of the following methods applies to your organization:

- the Cognos namespace
Use this method with any type of authentication provider when you want to grant access only to the members of the Cognos namespace.
- LDAP groups or roles
Use this method with Oracle directory server or Active Directory when the user accounts are located in different branches of the directory tree.
- LDAP OUs
Use this method with Oracle directory server or Active Directory when the user accounts are located in a specific Organizational Unit (OU) in the directory tree.
An Organizational Unit (OU) is a type of container in an LDAP directory structure. OU can contain user accounts, groups, roles, and other OUs.

Using the Cognos Namespace to Restrict Access

You can restrict access to IBM Cognos Connection only to users who belong to any group or role defined in the Cognos namespace. This is a quick method of securing access to IBM Cognos Connection that can be used with any type of authentication provider. Several built-in groups and roles in the Cognos namespace can be used. You can also create new groups and roles.

Tip: In IBM Cognos Configuration, set the value of the **Restrict access to members of the built-in namespace** property to **True**.

Before you use this method, you must

- ensure that authorized users and groups belong to at least one IBM Cognos group or role
Add the user accounts, groups, and roles created in your authentication provider to the Cognos namespace.
- remove the group Everyone from the built-in and predefined IBM Cognos groups and roles
By default, the group Everyone is a member of all built-in and predefined groups and roles in the Cognos namespace.

For more information about managing groups and roles in IBM Cognos BI, see the *Administration and Security Guide*. For more information about configuring IBM Cognos BI to use an authentication provider, see the *IBM Cognos Business Intelligence Installation and Configuration Guide*.

Administer BI environments with multiple tenants

Multitenancy provides the capability to support multiple customers or organizations (tenants) by using a single deployment of an application, while

ensuring that members of each tenant can access only the data that they are authorized to use. Multi-tenant applications minimize the extra costs associated with these environments.

IBM Cognos BI provides built-in multitenancy capabilities. Before you can use IBM Cognos multitenancy, you must configure an advanced property within Cognos Configuration which maps the path within your authentication source that can be used to identify the tenant ID for a user.

To configure multitenancy, you can perform the following tasks:

- Identify tenancy information.
- Enable multitenancy.
- Disable multitenancy.

For more information about multitenancy, see the *IBM Cognos Business Intelligence Administration and Security Guide*.

Using LDAP Groups or Roles to Restrict Access

Not all users in your LDAP directory must use IBM Cognos BI. Grant only designated users access to IBM Cognos Connection. This can be done by creating an IBM Cognos BI-specific group or role in your directory server, adding the required users to its membership, and granting the group or role access to IBM Cognos Connection.

An alternative method is based on using the LDAP organizational units (OUs).

Whether you must create a group or a role depends on your authentication provider. If you use Oracle directory server, you must create roles because this provider uses role membership as part of its user account information. If you use Active Directory, you must create groups because this provider uses group membership as part of its user account information.

Using Roles

The roles for this technique are created using Oracle directory server. For more information about creating this type of roles, see the Oracle directory server documentation.

Ensure that the following parameters are properly defined in IBM Cognos Configuration, in the **Security, Authentication** category.

- **User lookup**

Configure the user lookup string to contain the attribute that will be used to authenticate against the `${userID}` variable. This variable takes the user name entered at logon and substitutes the variable with the value before passing the search string to the directory server. The distinguished name (DN) of the role must also be included in the string.

Here is an example of the lookup string:

```
(&(uid=${userID})(nsrole=cn=Cognos,ou=people,dc=cognos,dc=com))
```

In this example, all members of the IBM Cognos BI role located in the organizational unit (ou) named people have access to IBM Cognos Connection.

- **Use external identity?**

Set the value to **True** if single signon is enabled.

- **External identity mapping**

Specify this property if **Use external identity?** is set to **True**.

Construct a string to locate a user in the LDAP directory server. At logon time, the environment variable `${environment("REMOTE_USER")}` in this string is replaced by the user name.

In the following example, the Web browser sets the environment variable `REMOTE_USER` that matches the user's uid attribute:

```
(&(uid=${environment("REMOTE_USER")})(nsrole=cn=Cognos,ou=people,dc=cognos,dc=com))
```

In some cases, the `REMOTE_USER` variable, which is typically in the `DOMAIN\username` format, may not match any of the user's uid attributes. To solve this problem, include the replace function in the string, as in the following example:

```
(&(uid=${replace("${environment("REMOTE_USER")},"ABC\\", "")})(nsrole=cn=Cognos,ou=people,dc=cognos,dc=com))
```

If the replace function is included, the domain name, `ABC` in this example, is replaced with a blank string, and only the user name is passed to the directory server.

The domain name is case sensitive in this context.

After the role is created, configure it for access to IBM Cognos Connection using IBM Cognos Configuration. The role can also be added to the Cognos namespace.

Using Groups

The groups for this technique are created using Active Directory. This technique involves modifications to the user lookup string. Because Active Directory does not have this property, it cannot be used. Instead, the associated LDAP provider is used.

Ensure that the following parameters are properly specified in IBM Cognos Configuration, in the **Security, Authentication** category.

- **User lookup**

Configure the lookup string to contain the attribute that will be used to authenticate against the `${userID}` variable. This variable takes the user name entered at logon and substitutes the variable with the value before passing the search string to the directory server. The distinguished name (DN) of the group must also be included in the string.

Here is an example of the lookup string:

```
(&(sAMAccountName=${userID})(memberOf=cn=ReportNet,ou=Groups,dc=cognos,dc=com))
```

- **Use external identity?**

Set the value to **True** if single signon is enabled.

- **External identity mapping**

Specify this property if **Use external identity?** is set to **True**.

Construct a string to locate a user in the LDAP directory server. At logon time, the environment variable `${environment("REMOTE_USER")}` in this string is replaced by the user name and then the string is passed to the directory server.

In the following example, the Web browser sets the environment variable `REMOTE_USER` that matches the user's uid attribute. Instead of substituting the hard-coded `sAMAccountName` value with `${userID}`, the environment variable is read from the browser session.

```
(&(sAMAccountName=${environment("REMOTE_USER")})(memberOf=cn=Cognos,cn=Groups,dc=cognos,dc=com))
```

After the group is created, configure it for access to IBM Cognos Connection using IBM Cognos Configuration. The group can also be added to the Cognos namespace.

Using LDAP OUs to Restrict Access

You can grant access to IBM Cognos Connection for a particular Organizational Unit (OU) or children of a particular OU in an LDAP directory. An OU usually represents a segment of an organization.

For this method to work, you must properly set up the **Base Distinguished Name** and **User lookup** properties in IBM Cognos Configuration, under the **Security, Authentication** category. By using different values for these properties, you can grant access for different OUs in your LDAP directory structure.

Consider the following directory tree:

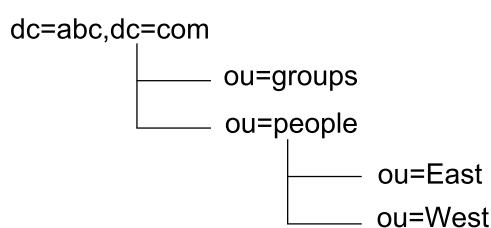


Figure 38. Tree of organizational units of a fictitious company broken down by east and west

If users from only the East OU need access to IBM Cognos Connection, the values can be specified as listed in the following table.

Table 5. The Base Distinguished Name and User Lookup values for the East Organisational Unit

Property	Value
Base Distinguished Name	ou=East, ou=people, dc=abc, dc=com
User lookup	uid=\${userID}

If users from both East and West OUs require access, the values can be specified as listed in the following table.

Table 6. The Base Distinguished Name and User Lookup values for the East and West Organisational Units

Property	Value
Base Distinguished Name	ou=people, dc=abc, dc=com
User lookup	(uid=\${userID})

The parentheses () in the **User lookup** property are used as a filter that can search all OUs located under the specified Base DN. In the first example, only the East OU is searched for user accounts. In the second example, both the East and West OUs are searched.

However, in both of the above examples, groups are excluded from access to IBM Cognos Connection because they are located in a different branch of the directory tree than users. To include both the groups and users, the Base DN must be the root of the directory tree. The values would then be as listed in the following table.

Table 7. The Base Distinguished Name and User Lookup values for groups and users located at the root of the directory tree

Property	Value
Base Distinguished Name	dc=abc, dc=com
User lookup	(uid=\${userID})

As a result, all users in the directory have access to IBM Cognos Connection.

The last example shows that using OUs may not always be the most efficient way of securing access to IBM Cognos Connection. You can use this method if you want to grant access for all users in a particular OU. If you want to grant access only for specific users, you may want to consider creating a designated IBM Cognos BI group or role in your directory server, and granting this group or role access to IBM Cognos Connection.

Securing IBM Cognos PowerCubes

IBM Cognos Series 7 PowerCubes are secured using the user class views based on the user classes that exist in the Series 7 namespace. After the PowerCubes are deployed into IBM Cognos BI, the MDC files continue to reside in the file system.

As an additional security measure,

- set up restricted access to PowerCube data sources
- use a third-party file encryption system for the PowerCube data sources
- set up permissions for the IBM Cognos BI directory that contains the cubes
- grant read and write permissions for the users who must add or remove cubes from the directory
- grant read permissions for the domain user account that is used to start the IBM Cognos service

To use secured PowerCubes from IBM Cognos Series 7 in IBM Cognos BI, you must have a Series 7 namespace configured as an available authentication provider. PowerCubes that you create in IBM Cognos BI can be secured against any available authentication provider.

For more information, see the *IBM Cognos Transformer User Guide* or the *IBM Cognos Administration and Security Guide*.

Securing Data Source Signons

IBM Cognos BI uses data source signons to access the underlying data located in the reporting databases.

To protect against unwanted access to the data,

- grant execute permissions for users and groups that need the signons
Other types of permissions are not required.
- deny execute permissions explicitly for all users, groups, and roles that do not need the signons

This ensures that access is not permitted through an unknown membership.

For more information about data source signons, see the *IBM Cognos Administration and Security Guide*.

Securing the content store

To ensure its security and integrity, the content store is accessed by the Content Manager service using single database signon specified in IBM Cognos Configuration. The database signon is encrypted according to your encryption standards. However, the content store security relies not only on the IBM Cognos BI security but also on the native database security, operating system security, and network security.

For securing your database, follow these guidelines:

- Secure the database and the database API using the mechanisms provided by the database, the network, and the operating system.
- Assign a limited number of users to maintain the database.
- Use your database native security to grant only minimum permissions to the user accounts that access the database, as follows:
 - Microsoft SQL Server
Users must have create and drop table permissions for the database. Ensure that the user account is a member of the db_ddladmin, db_datareader, and db_datawriter roles, and the owner of their default schema.
 - ORACLE
Users must have permissions to connect to the database. Also, they must be able to create, alter, and drop tables, triggers, views, procedures, and sequences, as well as insert, update, and delete data in the database tables. The permissions must be granted to the user account directly, and not through a group or role membership.
 - DB2
Users must have the create, drop table, CREATETAB, CONNECT and IMPLICITSCHEMA permissions for the database. Also, they must have USE permissions for the USER TEMPORARY tablespace and other appropriate tablespaces associated with the database.
 - Sybase Adaptive Server Enterprise
Users must have create, drop table, create default, create procedure, create rule, create table, and create view permissions for the database.
- Limit the number of users who have read or write access for the Content Manager tables.
- Follow other recommendations on securing the database. For information, see the database documentation.

Security Audit

A methodical security audit was conducted on IBM Cognos BI to check the effectiveness of the implemented security strategy.

The following distributed installation was used during the audit.

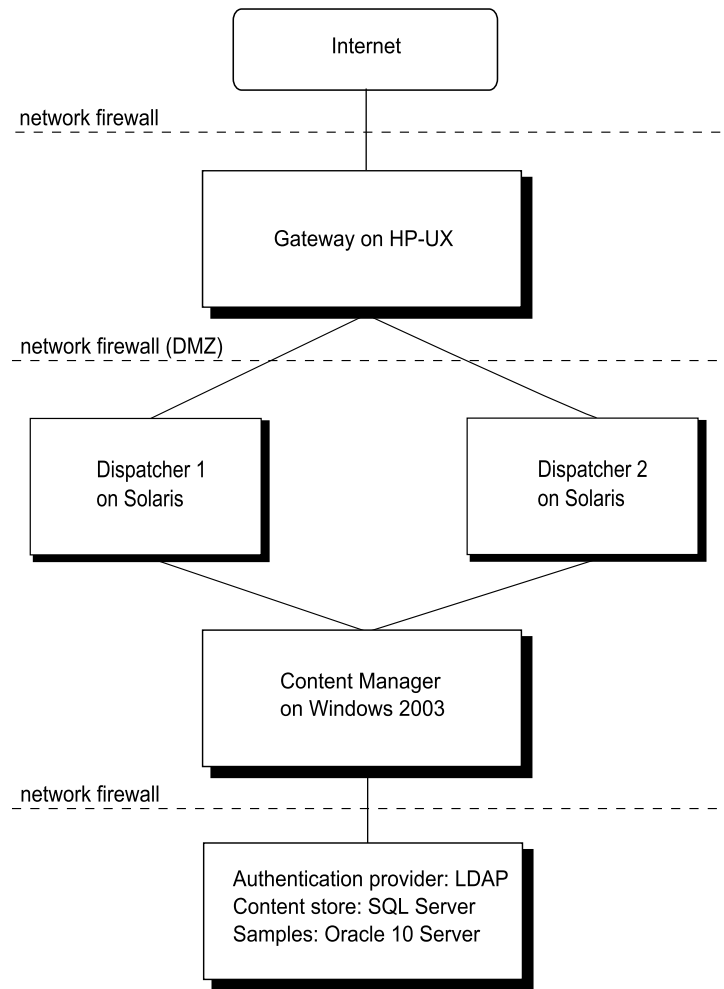


Figure 39. A representation of the IBM Cognos installation that was used for audit testing

Notices

This information was developed for products and services offered worldwide.

This material may be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service. This document may describe products, services, or features that are not included in the Program or license entitlement that you have purchased.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Software Group
Attention: Licensing
3755 Riverside Dr.
Ottawa, ON
K1V 1B7
Canada

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Depending upon the configurations deployed, this Software Offering may use session and persistent cookies that collect each user's

- name
- user name
- password

for purposes of

- session management
- authentication
- enhanced user usability
- single sign-on configuration
- usage tracking or functional purposes other than session management, authentication, enhanced user usability and single sign-on configuration

These cookies cannot be disabled.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM's Privacy Policy at <http://www.ibm.com/privacy> and IBM's Online Privacy Statement at <http://www.ibm.com/privacy/details> in the section entitled "Cookies, Web Beacons and Other Technologies" and the "IBM Software Products and Software-as-a-Service Privacy Statement" at <http://www.ibm.com/software/info/product-privacy>.

Trademarks

IBM, the IBM logo and [ibm.com](http://www.ibm.com) are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at " Copyright and trademark information " at www.ibm.com/legal/copytrade.shtml.

The following terms are trademarks or registered trademarks of other companies:

- Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.
- Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
- Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.
- UNIX is a registered trademark of The Open Group in the United States and other countries.
- Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Index

Special characters

.xml configuration files 44

A

- absolute affinity 79
- Access Manager 16
- accessing IBM Cognos BI 26
 - anonymous access 27
 - authenticated access 28
- Active Directory 123
- ActiveX 4
- administration 45
 - distributed 109
 - IBM Cognos Connection 45
- affinity
 - high 90
 - IBM Cognos BI activities 91
 - low 91
 - request 79
 - setting 90
- agent service 11
- agents
 - running 34
- analysis
 - Analysis Studio 6
 - running 30, 31
 - viewing 29
- Analysis Studio 6
- annotation service 11
- Apache Web server 117
- application servers
 - SSL 120
 - tuning 87
- Application Tier Components 10
 - installing 57
 - log server 20
- applications tier 10
- Architect models
 - migration to IBM Cognos BI 64
- architecture
 - communications 19
 - scalability 75
 - security 107
 - workflow 41
- audience of document vii
- audit logs
 - See also* log messages
 - See also* troubleshooting
 - log destinations 20
- authenticated access 28
- authentication 108
- authentication providers
 - Active Directory 123
 - Oracle directory server 123
 - Series 7 namespace 127
- author locale 98
- authorization services 109
- availability 69
 - Content Manager 83

- availability (*continued*)
 - content store 85
 - IBM Cognos BI gateway 82
 - IBM Cognos BI server 82
 - maximizing 82
 - planning 82

B

- balancing loads 20
- bandwidth
 - estimating 94
- batch report service 11
- batch report services
 - tuning 90
- best practices
 - security 113
- BI Bus API,
 - See* IBM Cognos BI Bus API
- browsers
 - configuring 45, 99
 - fonts in HTML reports 99
- builds
 - running in IBM Cognos Connection by using Data Movement service 66
- bursting reports 93
- Business Viewpoint Studio 67

C

- CAM password cookies, protecting 122
- capacity planning 69
 - infrastructure components 72
- certificate authority 110, 120
- CGI,
 - See* common gateway interface
- cipher strength 119
- cipher suites 120
- coglocale.xml files 44
- Cognos namespace 44, 108
 - securing IBM Cognos Connection 123
- cogstartup.xml files 44
- common gateway interface 9
 - in encryption 110
- common symmetric key settings 121
- communications 19
- components
 - IBM Cognos BI 53
 - installing 53
 - startup configuration 43
- Composite Information Server,
 - See* IBM Cognos Virtual View Manager
- compressing PDF reports 16
- configuration
 - browsers 99
 - fonts 99
 - multi-lingual reporting 45
 - planning 51
 - security 44

- configuration (*continued*)
 - startup 43
 - Web browsers 45
- configuration files 44
- connecting to database 24
- connection limits
 - setting 88
- connections
 - low bandwidth 94
- content locale 98
- content locales 101
 - mapping 102
- Content Manager 10, 14
 - availability 83
 - installing 57
 - log server 20
 - scalability 81
 - standby 10, 81
- Content Manager service 11
- content providers 16
- content store 16
 - availability 85
 - securing 128
 - sizing 73
- control affinity 79
- cookies
 - browser settings 99
- creating
 - models 46
 - packages 46
 - reports 47
- creating the index
 - request flow 35
- cryptographic keys
 - common symmetric key 110
 - encryption key pair 110
 - signing key pair 110
- cryptographic providers 119
 - cipher strength 119
 - standard 110
- cryptographic services 110
- cryptography
 - configuring 119
- CSK settings 121
- CSK,
 - See* common symmetric key
- currency 103

D

- data
 - data sources 16
 - multilingual 104
 - securing 122
- data integration service 11
- Data Manager
 - using in IBM Cognos BI 66
- Data Movement service
 - using in IBM Cognos Connection 66
- data source signons
 - securing 127
- data tier 16
- database
 - configuring for multilingual reporting 105
 - modeling 47, 49
 - tuning 87
- database connection management 24

- database connection management (*continued*)
 - content store database 24
 - metric store databases 24
 - query databases 24
- dates 103
- DecisionStream
 - requirements to upgrade catalogs to IBM Cognos BI 63
- DecisionStream to IBM Cognos BI
 - upgrade consideration 62
- default settings
 - browsers 99
 - fonts 99
 - security disabled 107
- delivery service 11
- diagnostics
 - See* troubleshooting
- dimensional analysis 67
- disk maintenance 94
- dispatcher metrics 86
- dispatchers 10
 - load balancing 76
 - logging 107
 - tuning 89
- dispatching 20
 - local preferred 20
- distributed administration 109
- distributing
 - requests 20

E

- enabling SSL 120
- encryption
 - key pairs 110
- Enterprise Information Integrators 17
- event management service 11
- Event Studio 6
- Excel,
 - See* Microsoft Office

F

- firewalls 10, 107
 - Framework Manager installation 60
- fonts
 - configuration 99
 - installing 45
- formats
 - numbers 103
- Framework Manager 7
 - configuration requirements 59
 - installation options 59
 - modeling 47, 49
 - packages 47

G

- gateways
 - IBM Cognos BI 9, 55
 - installing 55
 - scalability 75
- globalization considerations 97
- graphics service 11
- groups 110
 - securing IBM Cognos Connection 124

H

- high affinity 79
- HTML reports
 - running 30
 - viewing 29
- human task service 11

I

- IBM Cognos Administration 5
- IBM Cognos Application Firewall 10, 107, 119
- IBM Cognos BI
 - accessing 26
 - communications 19
 - configuring 43
 - dispatchers 13
 - gateways 9
 - installing 42
 - performance tuning 85
 - scalability 75
 - security 107, 110
 - services 13
 - tuning 89
 - user interfaces 3
 - workflow 41
- IBM Cognos BI Bus API 19
- IBM Cognos BI files
 - securing 122
- IBM Cognos BI for Microsoft Office 8, 25, 49
- IBM Cognos BI servers 10
 - availability 82
- IBM Cognos Configuration 43
 - user interfaces 3
- IBM Cognos Connection 4
 - opening a folder 33
 - securing 123, 124, 126
- IBM Cognos Content Database 16, 17
- IBM Cognos Controller
 - data access in IBM Cognos BI 65
- IBM Cognos DecisionStream
 - requirements to upgrade catalogs to IBM Cognos BI 63
- IBM Cognos Finance
 - data access in IBM Cognos BI 65
- IBM Cognos Insight 8
- IBM Cognos Metrics Manager
 - requirements to upgrade to IBM Cognos BI 62
 - upgrading to IBM Cognos BI 62
- IBM Cognos NoticeCast
 - duplication of functionality in IBM Cognos BI 68
- IBM Cognos Planning - Analyst
 - data access in IBM Cognos BI 64
- IBM Cognos Planning - Contributor
 - data access in IBM Cognos BI 65
 - migration to IBM Cognos BI 64
- IBM Cognos Portal Services
 - migration overview 68
- IBM Cognos PowerPlay Web
 - requirements to upgrade reports to IBM Cognos BI 63
- IBM Cognos Query
 - duplication of functionality in IBM Cognos BI 68
- IBM Cognos Report Studio 47
- IBM Cognos Series 7
 - migration to IBM Cognos BI 63
- IBM Cognos Series 7 PowerCubes
 - requirements for successful language conversion 65

- IBM Cognos services
 - scalability 81
- IBM Cognos Virtual View Manager 17
- IBM Cognos Visualizer
 - duplication of functionality in IBM Cognos BI 68
- IBM Cognos Web Services
 - migration overview 68
- IBM Cognos Workspace 7
- IBM Cognos Workspace Advanced 7
- IBM CognosScript
 - migration overview 68
- IBM WebSphere Portal 4
- IIS Web server 117
- implementation planning 42
 - checklist 51
- Impromptu catalogs and reports
 - migration to IBM Cognos BI 64
- Impromptu Web Reports
 - migration to IBM Cognos BI 64
- index data service 12
- index search service 12
- index update service 12
- indexed search scalability 81
- installation
 - Application Tier Components 57
 - components 42
 - Content Manager 57
 - fonts 45
 - Framework Manager 59
 - gateways 55
 - Metric Designer 59
 - options 53
 - planning 51
 - setting up security 110
- interfaces 3
- Internet Server API 9
- ISAPI,
 - See* Internet Server API

J

- job service 12
- JobStreams
 - running in IBM Cognos Connection by using Data Movement service 66
- JVM metrics 86

L

- language
 - restrictions for PowerCubes 101
- languages
 - supported 101
 - user interface 101
 - user preferences 101
- LDAP
 - namespaces 123
- Lifecycle Manager 67
- load balancing 75
 - automatic in IBM Cognos BI 75
 - configuring 75
 - settings 20
 - with external mechanisms 77
 - without external mechanisms 76
- load distribution
 - application complexity 72

- load distribution (*continued*)
 - concurrent users 70
 - estimating 71
- local preferred dispatching 20
- locales
 - author 98
 - content 98, 101
 - content mapping 102
 - description 98
 - product 98, 101
 - run 99
 - server 98
 - user 98, 99
- log destinations
 - types of 20
- log messages
 - See also* audit logs
 - See also* troubleshooting
 - log destinations 20
 - remote log server 20
- logging
 - dispatcher 107
 - secure 107
- logging database
 - adding metrics 86
- logs
 - message processing 20
 - service 12
- low affinity 79

M

- maintaining disks 94
- Map Manager 8, 104
- maximizing availability 82
- memory settings
 - WebSphere Application Server Liberty Profile 87
- messaging 20
- metadata modeling 47, 49
- Metadata service 12
- Metric Designer 8
 - configuration requirements 59
 - installation options 59
- metric store 16
- Metric Studio 6
- Metrics Manager service 12
- metrics, performance 86
- Microsoft .NET Framework 8, 25, 49
- Microsoft Office
 - IBM Cognos BI report data 8
 - IBM Cognos BI report data in workbooks and presentations 49
 - report data service 14
- migration
 - from other IBM Cognos products to IBM Cognos BI 63
- Migration service 12
- mobile service 13
- modeling 7, 8
 - and IBM Cognos BI performance 88
 - databases 47, 49
 - metadata 47, 49
 - packages 47
 - users 47, 49
- models 47
 - creating 46
 - Framework Manager 47, 49
 - publishing 47

- monitor service 13
- multilingual
 - Map Manager 104
- multilingual reporting
 - configuring 45
- multitenancy 124

N

- namespaces
 - Active Directory 123
 - IBM Cognos 123
 - LDAP 123
 - multiple tenants 124
 - Oracle directory server 123
 - Series 7 127
- network
 - securing 117

O

- OLAP 7
- operating system
 - securing 114
- Oracle directory server 123
- organizational units (OUs) 126

P

- packages
 - creating 46
 - Framework Manager 47
- parameter signing 107
- PDF
 - report compression 16
 - running reports 30, 31
 - viewing reports 29
- PDF rendering 94
- performance
 - application complexity 72
 - dispatch times 20
 - estimating 94
 - estimating bandwidth 94
 - estimating load distribution 71
 - estimating servers 95
 - planning 69
- performance metrics 86
- performance tuning 85
- permissions 109
- planning
 - availability 82
 - checklist 51
 - configuration 51
 - implementation 42, 51
 - installation 51
 - performance 69
- planning data service 13
- planning job service 13
- planning Web service 13
- planning administration console service 13
- plug-ins 4
- port usage 25
- portal pages 39
- portal services 4
- portlets 39

- PowerCubes
 - access in IBM Cognos BI 65
 - combining cubes from multiple locales 104
 - conversion from IBM Cognos Series 7 104
 - language restrictions 101
 - requirements for successful language conversion 65
 - securing 127
- PowerPlay
 - considerations for upgrading to IBM Cognos BI 62
 - migrating PowerPlay Web reports to IBM Cognos BI 64
- PowerPlay Web
 - requirements to upgrade reports to IBM Cognos BI 63
- PowerPoint
 - See Microsoft Office 8
- presentation service 13
- presentations
 - using IBM Cognos BI data in Microsoft Office PowerPoint 8
- process capacity setting 89
- processing log messages 20
- product locales 98, 101
- prompts 88

Q

- query processing types 88
- query service 14
- Query Studio 6, 47
- queue metrics 86

R

- report bursting 93
- report data
 - using in Microsoft Office 8, 49
- report data service 14
 - tuning 90
- report service metrics 86
- report services 14
 - scalability 81
 - tuning 90
- Report Studio 6
- report types
 - capacity planning 70
- ReportNet
 - requirements to upgrade to IBM Cognos BI 62
 - upgrading 62
- reports
 - bursting 71, 93
 - creating 47
 - estimating sizes 95
 - multilingual 104
 - running 30
 - scheduling 32, 71, 92
 - viewing 29
- repository services 14
- request affinity 79
- request flow
 - creating the index 35
 - searching 36
 - updating the index 35
- requests
 - distributing 20
 - flow processing 26
 - managing 20

- requirements
 - modeling 47, 49
- robustness,
 - See availability
- roles 110
 - securing IBM Cognos Connection 124
- routers
 - using 77
- rsvpproperties.xml files 96
- run locale 99
- running
 - analysis 30
 - HTML reports 29, 30
 - reports 30

S

- scalability 69, 75
 - Content Manager 81
 - IBM Cognos BI gateway 75
 - IBM Cognos BI server 80
 - planning 75
 - Web server 75
- search capability scalability 81
- searching
 - access control list 37
 - request flow 36
 - security check methods 36
- secure logging 107
- secure sockets layer 110
- secure sockets layer,
 - See SSL
- SecureError 107
- securing
 - content store 128
 - data 122
 - data source signons 127
 - IBM Cognos Connection 123, 124, 126
 - network 117
 - operating system 114
 - PowerCubes 127
 - temporary files 122
 - Web servers 117
- security
 - See also cryptographic keys
 - access control list 37
 - audit 128
 - authentication providers 108
 - best practices 113
 - configuration 44
 - Content Manager 109
 - IBM Cognos BI 107, 110
 - keys, 110
- security check
 - Content Manager 36
 - internal 37
 - searching 36
- Series 7 namespace 127
- Series 7 PowerCubes
 - requirements for successful language conversion 65
- server
 - locales 98
- server affinity 80
- server metrics 86
- servers
 - estimating numbers 95

- service
 - graphics 11
 - human task 11
 - index data 12
 - index search 12
 - index update 12
- service request metrics 86
- services
 - agent 11
 - annotation 11
 - authorization 109
 - batch report 11
 - Content Manager 11, 14
 - data integration 11
 - delivery 11
 - event management 11
 - IBM Cognos BI 13
 - IBM Cognos Content Database 16
 - job 12
 - load balancing 20
 - log 12
 - Metadata 12
 - Metrics Manager 12
 - Migration 12
 - mobile 13
 - monitor 13
 - planning data 13
 - presentation 13
 - query 14
 - report 14
 - report data 14
 - repository 14
 - scalability 81
 - system 14
 - visualization gallery service 14
- services metrics 86
- session affinity 80
- session metrics 86
- signing key pair 110
- single signon 109
- sizing the content store 73
- SSL
 - application servers 120
 - enabling 120
 - enabling on Web servers 117
- SSL,
 - See* secure sockets layer
- standby
 - Content Manager 14
- standby Content Manager 10, 81
- startup configuration 43
 - files 44
- system metrics 86
- system service 14

T

- temporary files
 - securing 122
- thresholds, metrics 86
- tiers
 - applications 10
 - data 16
 - Web server 9
- TM1
 - business planning 67
- Transformer 8

- Transformer (*continued*)
 - data access in IBM Cognos BI 65
- troubleshooting
 - logging 20
- tuning
 - application servers 87
 - databases 87
 - dispatchers 89
 - IBM Cognos BI 85
 - report services 90

U

- UNIX servers
 - fonts 99
- updating the index
 - request flow 35
- Upfront
 - migrating content to IBM Cognos BI 64
- upgrading
 - from other IBM Cognos products to IBM Cognos BI 61
 - tools that support upgrading from IBM Cognos
 - ReportNet 67
- user community
 - size 70
- user interfaces 3
 - user interfaces
 - windows-based 3
 - web-based 3
- user load
 - estimating 70
- user locale 98, 99
- users 109
 - active 70
 - concurrent 70
 - named 70

V

- viewing
 - analysis 29
 - HTML reports 29
 - PDF reports 29
- Virtual View Manager 17
- visualization gallery service 14

W

- Web browsers
 - configuring 45
- Web portal 4
- Web server tier 9
- Web servers 59
 - Apache 117
 - enabling SSL 117
 - IIS 117
 - scalability 75
 - securing 117
 - tuning 88
- Web-based user interfaces 4
- WebSphere Application Server Liberty Profile 82
 - memory settings 87
- Windows-based user interfaces 7
- workbooks
 - using IBM Cognos BI data in Microsoft Office Excel 8
- workflow 41

workspaces 8

X

XML configuration files 44

XML support 16

Y

Year, in dates 103