IBM Cognos Controller
Version 10.3.0

Architecture and Deployment
Product Information

This document applies to IBM Cognos Controller Version 10.3.0 and may also apply to subsequent releases.

Licensed Materials - Property of IBM

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

**Introduction** ................................................. v

Chapter 1. IBM Cognos Controller .................................. 1

Chapter 2. IBM Cognos Controller components ......................... 3

  Interfaces ................................................................ 4
    The IBM Cognos Controller interface ................................ 4
    IBM Cognos Connection ............................................ 5
    Cognos Viewer ...................................................... 5
    IBM Cognos Controller configuration ............................... 5
    IBM Cognos configuration ......................................... 5

  Gateway components .............................................. 5
    Gateways .......................................................... 5
    Controller Client Distribution Server ............................ 6
    Gateway Integration Enabler ...................................... 6

  Application Tier components ....................................... 6
    Controller Web Services Server .................................. 7
    Report Server ...................................................... 7
    IBM Cognos Connection Integration Enabler ..................... 8

  Content Manager components ..................................... 8
    Content Manager .................................................. 8
    Controller standard reports package............................ 9
    Controller Framework Manager model .......................... 10

  Modeling components ............................................. 10
    Framework Manager ............................................... 10

  Other components ................................................. 10
    Content store .................................................... 10
    Controller database ............................................. 11
    Controller data mart database .................................. 11

Chapter 3. Communications ........................................... 13

  Microsoft .NET Framework ...................................... 13
  COM+ application ................................................ 13
  Database connection management ................................... 14
  Log messages ..................................................... 15
  Port usage ......................................................... 15
  Request flow processing .......................................... 16

Chapter 4. Security ................................................... 19

  Microsoft .NET Framework security policies ....................... 19
  IBM Cognos authentication services ................................ 19
    Native security .................................................. 19
    IBM Cognos security ............................................ 20
    Windows authentication ......................................... 21
    Cognos namespace .............................................. 21
    Single signon .................................................... 21

  Content Manager authorization services ........................ 21
    Users ............................................................ 22
    Groups and roles .............................................. 22

  Cryptographic services .......................................... 22
    Using certificate authority by other providers .................. 23

  IBM Cognos Application Firewall .................................. 23
Introduction

IBM® Cognos® Controller is a Web-based financial consolidation tool that provides standard reports to support both statutory and management reporting.

The chapters one to five describe the IBM Cognos Controller architecture from the perspectives of structure, communications, security, and workflow. The chapters 6 to 9 provide information to help you plan to install and configure IBM Cognos Controller.

Audience

This document is for the solutions architect who oversees the setup, administration, and use of IBM Cognos Controller.

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

Finding information

To find product documentation on the web, including all translated documentation, access IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter).

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.

Accessibility features

Accessibility features help users who have a physical disability, such as restricted mobility or limited vision, to use information technology products. IBM Cognos Controller has accessibility features. For information on these features, see the accessibility section in Using Controller.

IBM Cognos HTML documentation has accessibility features. PDF documents are supplemental and, as such, include no added accessibility features.
Chapter 1. IBM Cognos Controller

IBM Cognos Controller is a Web-based solution designed to address financial consolidation needs and to support statutory and management reporting requirements. It supports leading relational databases.

IBM Cognos Controller uses Microsoft .NET Framework so that clients can interact with server-based components through the use of Web services. IBM Cognos Controller provides the zero-administration and zero-deployment benefits that are available for Microsoft .NET Framework applications.

IBM Cognos Controller supports multilingual reporting with components that are designed for scalability, availability, and openness. These components use platform independent, industry proven technology, such as Extensible Markup Language (XML), and Web Services Definition Language (WSDL).
Chapter 2. IBM Cognos Controller components

For description purposes, the components of IBM Cognos Controller can be organized into several groups.

The following functional groups are available:

- “Interfaces” on page 4
- “Gateway components” on page 5
- “Application Tier components” on page 6
- “Content Manager components” on page 8
- Modeling components

Within the functional groups, the following components are used:

**Interfaces**
- Cognos Controller
- Cognos Connection
- Cognos Viewer
- Cognos Configuration
- Cognos Controller Configuration

**Gateway components**
- Gateway
- Controller Client Distribution Server
- Gateway Integration Enabler

**Application Tier components**
- Controller Web Services Server
- Report Server
- IBM Cognos Connection Integration Enabler

**Content Manager components**
- Content Manager
- Controller Standard Reports Package
- Controller Framework Manager Model

IBM Cognos Controller also uses other components “Other components” on page 10.
This architecture enables you to choose a single-server installation or a distributed installation. For more information, see Chapter 7, “Installation options,” on page 33.

**Interfaces**

Several interfaces are available for using and configuring IBM Cognos Controller:

- Cognos Controller interface
- Cognos Connection
- Cognos Viewer
- Cognos Controller Configuration
- Cognos Configuration

**The IBM Cognos Controller interface**

IBM Cognos Controller provides the user interface for financial consolidation.

It is a zero deployment, zero administration interface that uses Microsoft .NET Framework.

IBM Cognos Controller is accessible through IBM Cognos Connection, as well as through a URL. To access IBM Cognos Controller, users click the Controller link that appear in the IBM Cognos Welcome page. Users can also click the Controller link that appears on their home page, if one is defined. When the users click the Controller link, the Controller Client Distribution Server uploads Controller client components to the user's computer and then IBM Cognos Controller runs.

Within IBM Cognos Controller, the IBM Cognos Controller Link for Microsoft Excel extends the functionality of Microsoft Excel for creating individual forms and provides templates for manual data entry.

For information about using IBM Cognos Controller, see *Using Controller*. 
IBM Cognos Connection

IBM Cognos Connection is a Web portal provided with IBM Cognos Business Intelligence (BI), 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 URLs to other applications, can be integrated with IBM Cognos Connection.

Cognos Viewer

IBM Cognos Viewer is a portlet in which you can view and interact with any type of published IBM Cognos content.

It is accessible through IBM Cognos Connection and any existing enterprise portal.

IBM Cognos Controller configuration

IBM Cognos Controller Configuration is a Windows interface that you use to configure IBM Cognos Controller data sources, set security, and administer system-wide IBM Cognos Controller settings.

For information about using Controller Configuration, see Using Cognos Configuration Controller.

IBM Cognos configuration

IBM Cognos Configuration is a tool that you use to configure IBM Cognos Business Intelligence (BI), and to start and stop its services.

For information about using IBM Cognos Configuration, see the IBM Cognos Business Intelligence Installation and Configuration Guide.

Gateway components

The IBM Cognos Controller gateway components provide Web communication and access for client computers.

The gateway components include the following:
- “Gateways”
- “Controller Client Distribution Server” on page 6
- “Gateway Integration Enabler” on page 6

Gateways

Web communication in IBM Cognos Controller 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 the Controller Web Services Server “Controller Web Services Server” on page 7 or Report Server dispatcher “Dispatcher” on page 7. This may provide improved performance in environments where the gateway is not required for security purposes.
If you install the gateway component on a different computer from IBM Cognos Controller server components, you must configure the gateway computer so that it knows the location of a Controller Client Distribution Server.

The gateway supports several types of Web gateways, including

- CGI
  
  The default gateway, CGI, can be used for all supported Web servers. However, for enhanced performance or throughput, you may choose one of the other supported gateway types.

- ISAPI
  
  ISAPI can be used for the Microsoft Internet Information Services (IIS) Web server. It delivers faster performance for IIS.

The Controller Client Distribution Server and Web Services Server support only IIS. If a Controller Client Distribution Server is on the same computer as the gateway, you must use CGI or ISAPI.

When a gateway receives a request, it

- encrypts passwords to ensure security
- extracts information needed to submit the request to the appropriate IBM Cognos Controller 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 the appropriate server for processing

For information about configuring gateways, see Installing and Configuring Controller.

**Controller Client Distribution Server**

Controller Client Distribution Server provides access to IBM Cognos Controller for client computers. When a user starts IBM Cognos Controller within a Web browser, Controller client components are downloaded from Controller Client Distribution Server (if necessary) and then IBM Cognos Controller runs.

**Gateway Integration Enabler**

The Gateway Integration Enabler updates the gateway to make it aware of all server components.

---

### Application Tier components

Application Tier components provide the user interface for reporting and the server functionality for routing and processing requests.

The IBM Cognos Controller application tier components include:

- "Controller Web Services Server" on page 7
- "Report Server" on page 7
- "IBM Cognos Connection Integration Enabler" on page 8
Controller Web Services Server

Controller Web Services Server processes all IBM Cognos Controller requests, except for downloading IBM Cognos Controller components to the user's computer.

Controller Web Services Server handles requests for activities within IBM Cognos Controller, such as working with accounts, consolidations, companies, and dimensions. Controller Web Services Server also manages data source connections and security information, as well as preparing data in the IBM Cognos Controller database for reports.

Depending on how you have configured security, the Web Services Server may access other components before processing requests, such as authenticating users.

A COM+ application is created when the Web Services Server is installed. This application runs within the Microsoft component services and provides most of the IBM Cognos Controller business logic, such as retrieving report templates and preparing data in the Controller database for reports.

Report Server

The Report Server renders IBM Cognos Controller reports, in PDF and HTML formats. It includes a dispatcher and several services.

Dispatcher

The dispatcher operates Report Server services and routes requests to these services. If more than one Report Server is included in your installation, the dispatcher routes requests to other Report Server dispatchers, as required.

The dispatcher starts all Report Server services configured and enabled on a computer. 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 reporting. For more information, see “IBM Cognos Application Firewall” on page 23.

When a dispatcher starts, it registers itself with Content Manager. As a result, if more than one Report Server is included in your installation, 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.

When you configure 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 Installing and Configuring Controller.

Services

The dispatcher manages the following Report Server services:

- presentation service
The presentation service handles requests for IBM Cognos Connection and Cognos Viewer.

- report service
  The report service handles interactive requests to run reports and provides output in Cognos Viewer.

- log service
  The log service manages all logs generated by the dispatcher and other services. You can configure the log service to record log information in a file, a database, a remote log server, or a Windows Event Viewer. For more information, see “Log messages” on page 15.

- Content Manager service
  The Content Manager service performs object manipulation functions in the content store, such as add, query, update, delete, move, and copy.

**IBM Cognos Connection Integration Enabler**

The IBM Cognos Connection Integration Enabler activates the links in IBM Cognos Connection that users click to access IBM Cognos Controller. These links are available from the IBM Cognos Connection Welcome page and the home page.

---

**Content Manager components**

The IBM Cognos Controller Content Manager components support the data functionality for the content store and Controller database.

The components include:

- “Content Manager components”
- “Controller standard reports package” on page 9
- “Controller Framework Manager model” on page 10

**Content Manager**

Content Manager is a service that manages the storage of IBM Cognos data, including customer application data. 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.

The information stored by Content Manager includes

- report packages
  Packages contain metadata, reports, and folders.
- server configuration
  Server configuration contains directory information, the Cognos namespace “Cognos namespace” on page 21, and information about contacts, distribution lists, the content store database, 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 multilingual capabilities for reporting components.

Content Manager stores information in a content store “Content store” on page 10 database.
Content Manager contains Access Manager, the Cryptographic service, and the Authentication service.

![Content Manager components and architecture](image)

**Access Manager**

Content Manager contains Access Manager, the primary security component of IBM Cognos Controller. Access Manager leverages your existing security providers for use with IBM Cognos Controller. It provides IBM Cognos Controller 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 Controller but are exposed to IBM Cognos Controller by Access Manager. Other capabilities, such as authorization, are internal to IBM Cognos Controller, 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 Controller uses its own certificate authority service to establish the root of trust in the IBM Cognos Controller security infrastructure. If you use a other certificate authorities, you can configure IBM Cognos Controller to use it instead of the default IBM Cognos Controller certificate authority. For more information, see Chapter 4, "Security," on page 19.

**Controller standard reports package**

Report Server uses information in the Controller standard reports package, a Framework Manager package provided with IBM Cognos Controller, to determine the structure of data in the Controller database.
The package contains preformatted templates that are used to obtain the data necessary for rendering the standard reports that are available with IBM Cognos Controller. You do not need to install IBM Cognos Framework Manager to use the standard reports package.

After installing IBM Cognos Controller, you must import the package into Content Manager using IBM Cognos Connection. You must have Controller user or administrative privileges (defined within IBM Cognos Connection) to import this package.

**Controller Framework Manager model**

You can use the Framework Manager model provided with Controller to author custom reports.

You can use the Framework Manager model provided with Controller to author custom reports. This Publish to Data Mart Framework Manager model is provided as a template for reporting against a Controller data mart database. You can also customize the model in IBM Cognos Framework Manager before creating the reports in IBM Cognos Report Studio.

To use this model, you must install IBM Cognos Framework Manager from the CD provided with IBM Cognos Controller, or use Framework Manager from your IBM Cognos Business Intelligence installation.

### Modeling components

Modeling components model data within data sources to structure and present data in a way that is meaningful to users. IBM Cognos Controller uses the following modeling components:

**Framework Manager**

Framework Manager is the IBM Cognos Business Intelligence (BI) 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.

To author custom reports using the Controller Framework Manager model, you must have access to Framework Manager. You can access Framework Manager in an existing IBM Cognos Business Intelligence environment, or you can install Framework Manager using the CD that is provided with IBM Cognos Controller.

### Other components

IBM Cognos Controller requires some other components for its databases: the content store, the Controller database, and the Controller data mart.

**Content store**

The content store is a relational database that contains data that IBM Cognos Controller needs to operate, such as report packages and connection information about the external namespace and the Cognos namespace.

Content Manager uses a JDBC (Java™ DataBase Connectivity) API to access the content store. IBM Cognos Controller comes with
the JDBC drivers for Microsoft SQL Server access from a Windows or UNIX operating system. JDBC drivers for Oracle, IBM, and Sybase, which are required for their respective databases, are available from their vendors.

The IBM Cognos application does not publish the content store schema, but updates the schema periodically, isolating changes from the user through stable user interfaces and APIs.

Much of the information in the content store is stored as binary large object (BLOB) fields.

**Controller database**

The Controller database is a relational database that contains the data that clients work with in IBM Cognos Controller.

The Controller Web Services Server uses data source connections to access Controller databases. One data source connection is defined for each Controller database. Data source connections are defined by administrators using Controller Configuration.

At least one database and its data source connection must be available before users can use IBM Cognos Controller. If more than one Controller database is available, each database must be the same Controller database version. For more information about database versions, see *Installing and Configuring Controller*.

If more than one Controller database is available, the administrator determines whether users can select the database they want to use or whether one is provided by default. Administrators can choose to let users select a database from a list that appears when IBM Cognos Controller starts. If no selection is allowed, users can access only the default database.

To enable the Web Services Server to connect to the Controller database, ensure that you install the database API software on each Web Services Server computer.

**Controller data mart database**

A Controller data mart database is required if you use the Publish to Data Mart Framework Manager model provided with IBM Cognos Controller. By using the Publish to Data Mart functionality in Controller, you can publish data and structures from a Controller database to the data mart database. After it is populated, you can use the Controller data mart database for custom reporting using the Controller Publish to Data Mart Framework Manager model.
Chapter 3. Communications

Several forms of communication are used among IBM Cognos Controller components.

IBM Cognos Controller is deployed to users’ computers using Microsoft .NET Framework. As well, Controller Web Services Server and Controller Client Distribution Server communicate using the Hypertext Transfer Protocol (HTTP) while Report Server and Content Manager communicate using the Business Intelligence (BI) Bus. The BI Bus is an open, documented, Simple Object Access Protocol (SOAP) API that supports Web Services Definition Language (WSDL).

Microsoft .NET Framework

Microsoft .NET Framework allows local applications to interact with server-based applications through the use of Web services.

IBM Cognos Controller uses Microsoft .NET Framework to enable users’ computers to interact with IBM Cognos Controller server components for access to IBM Cognos Controller and its features.

IBM Cognos Controller provides the zero-administration and zero-deployment benefits that are available for Microsoft .NET Framework applications. As a Microsoft .NET smart client, IBM Cognos Controller does not need to be installed or configured by users. To access IBM Cognos Controller, users click the Controller link in IBM Cognos Connection. The content for IBM Cognos Controller, which consists primarily of Microsoft .NET Windows Forms, and the IBM Cognos Controller Link for Microsoft Excel, is downloaded from Controller Client Distribution Server to a cache on the user’s computer. IBM Cognos Controller then opens on the user’s computer. When configuration information is required, such as the location of Controller Web Services Server and help files, IBM Cognos Controller communicates with Controller Client Distribution Server.

By default, Microsoft Windows does not allow smart clients to run outside of the browser. Therefore, Microsoft .NET Framework Security Policies on every client computer must be configured to allow IBM Cognos Controller to run. This configuration allows the client computer to trust the computer on which Controller Client Distribution Server is located. For information about configuring this trust, see Installing and Configuring Controller.

Microsoft .NET Framework must be installed on the client computers, the Controller Web Services Server computer, and the Controller Client Distribution Server computer. Microsoft .NET Framework Software Development Kit must also be installed on the Controller Web Services Server computer and the Controller Client Distribution Server computer. You do not need to configure trust on the Controller server computers unless you want to run IBM Cognos Controller on them.

COM+ application

The Microsoft Component Object Model (COM+) application requires that you configure an identity and users before it can run.
The COM+ application is installed automatically with Controller Web Services Server [“Controller Web Services Server” on page 7].

**COM+ identity**

The COM+ identity represents a dedicated user who has access rights to the applications and services required by the COM+ application. The account that is configured to represent this dedicated user can be a system account or a specific user account, depending on the security requirements for the computer that the COM+ application is running on.

For information about configuring the identity for the COM+ application, see *Installing and Configuring Controller*.

**COM+ users**

The COM+ application accepts requests submitted by anonymous IIS accounts on behalf of IBM Cognos Controller clients. You must identify these IIS accounts to the COM+ application before it will accept requests.

For information about configuring accounts for the COM+ application, see *Installing and Configuring Controller*.

### Database connection management

IBM Cognos Controller uses databases for the content store and the Controller data source.

**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 is determined by the number of requests accepted by the Java application server or Tomcat.

When other Report Server 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.

For some types of databases, such as Oracle, API client software must be installed and configured on each Report Server.

**Controller database**

Controller Web Services Server and Report Server access the Controller database. Controller Web Services Server interacts with the Controller database to respond to user requests, to process SQL commands against the database, and to create data views for reports. Report Server accesses the Controller database to retrieve data for reports.

Controller Web Services Server and Report Server use one database connection per request, creating new connections as required. Each server maintains its own
database connections for the duration of its operation. There is no limit to the number of connections that can be concurrently created or maintained.

The API connection type is used between Controller Web Services Server or Report Server and the Controller database. OLE DB in Microsoft ActiveX Data Objects (ADO) connections are used.

For some types of databases, such as Oracle, API client software must be installed and configured on each Controller Web Services Server or Report Server.

For information about defining database connections, see Installing and Configuring Controller.

Log messages

Log messages are an important diagnostic tool for investigating the behavior of IBM Cognos Controller components.

In addition to error messages, log messages provide information about the status of components. Log messages also provide a high-level view of important events, such as successful completion of processing requests and fatal errors.

Log messages for IBM Cognos Controller components are recorded in the Windows Event Log.

When you install reporting components, a log server is installed. The log server uses a different port from the other IBM Cognos Controller components, and continues to process events even if other services on the local computer, such as the dispatcher, are disabled.

By default, all local reporting services send events to the local log server. When you configure a log server, you can:

- Specify the level of detail to log for each logging category.
  For more information, see the IBM Cognos Business Intelligence Administration and Security Guide.
- Direct messages to an alternative destination, such as another database or the Windows Event Viewer.

Port usage

All communication among reporting components, except for log server communication, can take place through one incoming port.

This is true whether components are on the same computer or on different computers. The default port number is 9300.

Log server communication must take place through a unique port. The default port is 9362.

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

For information about specifying where to send log messages, see Installing and Configuring Controller.
Request flow processing

Request flow describes internal IBM Cognos Controller responses to user requests.

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

Users can request a report in HTML or PDF format.

When a user runs a report from IBM Cognos Controller, the following occurs:

1. The user clicks a report to run it, and the request goes to the gateway, which forwards the request to Controller Web Services Server. If a gateway is not part of your installation, the request is sent directly to Controller Web Services Server.

2. Controller Web Services Server forwards the request to the Controller COM+ application for processing.

3. The COM+ application prepares the data in the Controller database for Report Server to retrieve later.

   To prepare the data, the COM+ application inserts data for the report into the dedicated tables created during installation in the Controller database. When Report Server generates the report, SQL queries are run against these tables.

4. The COM+ application retrieves the report template, which is an XML file stored on the Controller Web Services Server computer. The COM+ application updates the report template based on selections made by the user when requesting the report. Updates include modifications to the data source, formatting, and SQL queries.
5. The modified report template is sent to IBM Cognos Controller (client).
6. IBM Cognos Controller (client) makes the request to the Report Server dispatcher. The request also specifies whether a PDF or HTML report is required.
7. The presentation service sends the request to the report service.
8. The report service uses the SQL queries in the report template to retrieve data from the dedicated tables for the report in the Controller database.
9. The report service returns one of the following results to the presentation service, and then to IBM Cognos Controller (client):
   • an error page
   • a not ready page
   • a page of an HTML or PDF report, depending on which format was requested, for display in Cognos Viewer
Chapter 4. Security

IBM Cognos Controller 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 Controller security involves the following:

- "Microsoft .NET Framework security policies"
- "IBM Cognos authentication services"
- "Content Manager authorization services" on page 21
- "Cryptographic services" on page 22
- "IBM Cognos Application Firewall” on page 23

Microsoft .NET Framework security policies

To access IBM Cognos Controller, users click the Controller links in IBM Cognos Connection.

The content required to run IBM Cognos Controller is downloaded from the Controller Client Distribution Server to the user's computer. Because IBM Cognos Controller is based on Microsoft .NET technology, all client computers must be configured to trust the Controller Client Distribution Server computer. This trust is configured using the Microsoft .NET Framework Configuration tool. For information about installing Microsoft .NET Framework and configuring this trust, see Installing and Configuring Controller.

IBM Cognos authentication services

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

Authentication in IBM Cognos Controller is managed using IBM Cognos Controller native security, IBM Cognos security with other authentication providers, or Windows authentication.

For information about configuring authentication, see Installing and Configuring Controller.

Native security

Native security is the default authentication method.

When users start IBM Cognos Controller, they are prompted to choose a database and log on. Only users who can provide the appropriate credentials are allowed to log on to IBM Cognos Controller.

If you use native security to secure the Controller database, you must configure anonymous access to the reporting components using IBM Cognos security.
IBM Cognos security

IBM Cognos security allows anonymous access to reporting components when native security is defined for the Controller components, or authenticated access to both Controller and reporting components.

For authenticated access, when users attempt to access IBM Cognos Controller, they are prompted to log on to the application. Only users who provide the appropriate application credentials are allowed access to IBM Cognos Controller.

Authentication providers determine the 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.

Figure 4. Security for Cognos Controller

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

- LDAP
- Windows NT LAN Manager (NTLM)
- Microsoft Active Directory
- IBM Cognos 7 namespaces created using IBM Cognos 7 Access Manager and available with other IBM Cognos products
- Netegrity SiteMinder
- Custom Java provider
**Windows authentication**

Windows Authentication is the built-in authentication provided through the configuration of Internet Information Services (IIS) and Microsoft .NET Framework.

When Windows Authentication is enabled, user connections established with IIS on the Controller Web Services Server are validated and authenticated against the Cognos Namespace. If users have met the logon requirements for Windows, they are not prompted to provide logon credentials when starting up IBM Cognos Controller.

**Cognos namespace**

IBM Cognos has its own namespace, which is in addition to the external namespaces that represent other 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 other authentication providers. This practice can add value to your existing groups and roles by reorganizing them for IBM Cognos Controller without changing them in your authentication provider or existing Controller security definitions.

You can use the Cognos Namespace to set up security that links easily with client security systems. For more information, see the *IBM Cognos Administration and Security Guide*.

**Single signon**

Depending on the type of authentication you implement, you can configure IBM Cognos Controller for single signon.

Users can then sign on once to an environment that includes IBM Cognos Controller 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 or IBM Cognos Controller native security configuration.

For more information, see *Installing and Configuring Controller*.

**Content Manager authorization services**

Authorization services are provided in Content Manager.

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. In IBM Cognos Controller, authorization is used to set permissions.

Permissions are related to the users, groups, and roles defined in other authentication providers. 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 Controller authorization assigns permissions to
- groups and roles created in the Cognos Namespace in the Content Manager for IBM Cognos Controller. These groups and roles are referred to as IBM Cognos groups and IBM Cognos roles.
• entire namespaces, users, groups, and roles created in other authentication providers

**Users**

A user entry is created and maintained in a other authentication source to uniquely identify an account belonging to a person or a computer.

You cannot create user entries in IBM Cognos Controller.

The user entry stored in the authentication source may include information such as first and last names, passwords, IDs, locales, and email addresses. However, IBM Cognos Controller 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 Controller.

You can assign users to groups and roles defined in the authentication provider and in IBM Cognos Controller. 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 tasks, or have a similar status in an organization.

Examples of groups are Employees, Developers, or Sales Personnel. Members of groups can be users and other groups. Group membership is part of a user basic identity. Users always log on with all the permissions associated with the groups to which they belong.

Roles differ from groups in several ways. Members of roles can be users, groups, and other roles. Role membership is not part of the user basic identity.

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

**Cryptographic services**

Cryptographic services ensure that sensitive data and communications in the gateway, Report Server, and Content Manager are secure.

Two categories of encryption strength are available for IBM Cognos Controller. Basic encryption using Standard OpenSSL is the standard IBM Cognos cryptographic service included with IBM Cognos Controller. It uses signatures to digitally sign some messages to ensure that they come from a recognized Report Server service.

If an assessment of your security risks indicates a need for stronger cryptographic services, you can replace the standard IBM Cognos cryptographic services with the Enhanced Encryption module available from IBM Cognos: the Enhanced Encryption Module for OpenSSL. It is packaged separately to adhere to government regulations controlling the export of cryptographic software.
You can add enhanced encryption after you start using IBM Cognos Controller with standard encryption. However, after you install enhanced encryption and configure IBM Cognos Controller to use it, you cannot return to standard encryption.

**Using certificate authority by other providers**

To provide encryption, certificates are required.

When you implement the standard or enhanced IBM Cognos encryption provider, the IBM Cognos certificate authority (CA) is used by default. You can also use any other CA that generates Base-64 encoded X.509 certificates. For more information, see *Installing and Configuring Controller*.

---

**IBM Cognos Application Firewall**

IBM Cognos Application Firewall validates and filters incoming and outgoing traffic for the Report Server dispatcher.

IBM Cognos Application Firewall does not affect non-reporting requests, which are not sent to the dispatcher.

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 Controller security posture current.

IBM Cognos Application Firewall helps provide protection against penetration vulnerabilities such as cross-site scripting. Disabling the IBM Cognos Application Firewall removes this protection, and should not be done under normal circumstances.

For information about configuring IBM Cognos Application Firewall, see *Installing and Configuring Controller*. 
Chapter 5. Workflow for IBM Cognos Controller

The workflow for IBM Cognos Controller is shown in the following diagram.

![Workflow Diagram](image)

Figure 5. Workflow for Cognos Controller

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

- **Planning for deployment**
  Deployment planning should be done before installing and configuring IBM Cognos Controller. It is typically carried out by a team assembled and led by the business intelligence solutions architect.

- **Installing and configuring IBM Cognos Controller.**
  Technical personnel install and configure IBM Cognos Controller, typically under the direction of the business intelligence solutions architect. The installation and configuration process is not complete until a Controller database is available and the Controller Framework Manager Model has been imported into Content Manager.

- **Administering IBM Cognos Controller.**
  Administrators must ensure that client computers are configured with the appropriate trust permissions to access IBM Cognos Controller. Administrators also establish and maintain security, set up multilingual capabilities, and perform ongoing administration.

- **Using IBM Cognos Controller.**
  Users can access IBM Cognos Controller and begin working with their data and viewing reports. For more information, see Using Controller.

Report users view and print reports through IBM Cognos Connection. For more information, see the IBM Cognos Connection User Guide.

**Planning for deployment**

Deploying IBM Cognos Controller means installing and configuring it to integrate effectively with your existing infrastructure.
To ensure that IBM Cognos Controller is deployed effectively, it is important to carefully plan your implementation. For information about deployment planning, including a deployment planning checklist, Chapter 6, “Deployment checklist,” on page 31.

Installing IBM Cognos Controller

Installing IBM Cognos Controller is typically done by information technology personnel under the direction of the business intelligence solutions architect.

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

- gateway components, including gateways "Gateway components” on page 5, Controller Client Distribution Server “Controller Client Distribution Server” on page 6, IBM Cognos Connection Integration Enabler “IBM Cognos Connection Integration Enabler” on page 8, and Gateway Integration Enabler “Gateway Integration Enabler” on page 6
- application tier components, which include Report Server “Report Server” on page 7 and Controller Web Services Server “Controller Web Services Server” on page 7
- Content Manager components, which include Content Manager “Content Manager” on page 8 and Controller Framework Manager Model “Controller Framework Manager model” on page 10

To deploy the Publish to Data Mart model that is provided with IBM Cognos Controller, you must also install Framework Manager.

You can install the components on one computer, or distribute them across a network. Before installing IBM Cognos Controller, choose the appropriate installation and configuration option Chapter 7, “Installation options,” on page 33

Configuring IBM Cognos Controller

IBM Cognos Controller uses two configuration tools: IBM Cognos Configuration and Controller Configuration.

You use these tools immediately after installation to set the initial IBM Cognos Controller configuration. You can configure the following:

- logging
  You can specify the destination log for messages generated by the gateway and reporting components “Log messages” on page 15.
  The Web Services Server records log messages in the Microsoft Windows Event Log.
- security
  You can run IBM Cognos Controller with or without security. By default, native security is configured for the Controller database and IBM Cognos Application Firewall is enabled for the Report Server. If you want to set up security, you should configure security settings immediately after installing IBM Cognos Controller Chapter 4, “Security,” on page 19.
- data access
  You must specify database connection information “Database connection management” on page 14 for the content store and at least one Controller database.
If you use a database from a previous version of IBM Cognos Controller, we recommend that you use the new consolidation model. The new model provides a more detailed method of handling complex ownership structure for all customers and facilitates migration to IBM Cognos Controller from Consolidator. Discuss available consolidation models with your IBM Cognos consultant to determine the one that is appropriate for your installation.

If you want to use the Publish to Data Mart model, you must specify connection information for an additional database used as the Controller data mart.

Following initial configuration, if a property changes or components are added, you can use the configuration tools to configure IBM Cognos Controller again.

For information about initial configuration, see *Installing and Configuring Controller*. For information about using IBM Cognos Configuration, see *Using Controller*. For information about using Controller Configuration, see *Configuring Controller*.

**Importing the IBM Cognos Controller standard reports package**

A Framework Manager model serves as an insulating layer between IBM Cognos Controller reporting users and the database.

Packages are model subsets that provide users with data that is appropriate for the reporting they need to do, and ensure that the data is structured in ways that make sense from a business perspective.

IBM Cognos Controller provides a standard reports package, which must be installed on the same computer as Content Manager. After installation, the package is imported using IBM Cognos Connection.

**Configuring Microsoft .NET Framework security policies**

To access IBM Cognos Controller, users click the Controller links in IBM Cognos Connection.

The client computer downloads the content required to run IBM Cognos Controller, including the IBM Cognos Controller Link for Microsoft Excel module, from the Controller Client Distribution Server. After the content is downloaded to a cache on the client computer, IBM Cognos Controller runs on the computer. Because IBM Cognos Controller is based on the Microsoft .NET Framework technology, the client computer must be configured to trust the computer from which this content is downloaded. This trust must be configured using the Microsoft .NET Framework Configuration tool on every computer that runs IBM Cognos Controller. For information about installing Microsoft .NET Framework and configuring this trust, see *Installing and Configuring Controller*.

**Monitoring configuration changes**

Each time that you save a configuration after making changes in IBM Cognos Configuration, date-stamped versions of the following configuration files are automatically saved in the c10_location/configuration directory.

These are the configuration files:

- cogstartup.xml
  This file records configuration settings. An example is cogstartup_200211231540.xml
• coglocale.xml

This file records locale settings used for multilingual reporting by the reporting components. An example is coglocale_200211261401.xml

If you are unable to save a configuration, or 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 IBM Software Support for help, print a history of the configuration changes made in IBM Cognos.

For more information about the cogstartup.xml file, the coglocale.xml file, and troubleshooting, see Installing and Configuring Controller.

Configuring Security

IBM Cognos Controller can provide security by using native security, by integrating with an existing security infrastructure to provide user authentication, or by using Microsoft Windows authentication.

IBM Cognos Controller can secure content by using the user and group definitions from your security system, without any changes required. A 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.

Cognos Controller includes IBM Cognos Application Firewall, which validates and filters incoming and outgoing reporting traffic for the Report Server dispatcher. By default, IBM Cognos Application Firewall is enabled.

IBM Cognos Controller 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 from Cognos, an IBM company.

If you intend to set up security for IBM Cognos Controller, it should be the first thing you do after installation [Chapter 4, “Security,” on page 19]. For information about setting up and maintaining security, see the IBM Cognos Administration and Security Guide.

Configuring multilingual reporting

The IBM Cognos Controller reporting components are Unicode products capable of querying data in many languages and encodings.

To facilitate multilingual reporting in Cognos Viewer, you may have to configure the Web browsers for your users.

Cognos Viewer uses the default browser configurations of supported browsers. To ensure that Cognos Viewer operates effectively, check your browser configuration settings and modify them if necessary. For information, see Installing and Configuring Controller.

You must also configure the language in Controller Configuration for interfaces and reporting templates.

Administering IBM Cognos Controller

You can administer IBM Cognos Controller.
After IBM Cognos Controller is installed and configured, you can use IBM Cognos Connection [“IBM Cognos Connection” on page 5] or your other software portal to
• monitor and administer servers
• back up data
• maintain security
• deploy IBM Cognos Controller from one environment to another

For information about using IBM Cognos Connection, see the *IBM Cognos Connection User Guide*. For information about administration, see the *IBM Cognos Administration and Security Guide*.

If users plan to use forms from earlier versions of IBM Cognos Controller, they must upgrade the forms. The tool used to upgrade forms is provided with IBM Cognos Controller and must be installed by the Administrator. For information about choosing consolidation models and upgrading forms, see *Installing and Configuring Controller*. 
Chapter 6. Deployment checklist

To get the most from IBM Cognos Controller, you must deploy it effectively.

This means installing and configuring IBM Cognos Controller so that it integrates with your information technology infrastructure and meets your financial consolidation and reporting requirements.

To deploy IBM Cognos Controller effectively, do the following:

- **Familiarize yourself with the IBM Cognos Controller architecture.** Read the chapters 1 to 5 of this book. It will help you understand the components that make up IBM Cognos Controller, 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 Controller** Chapter 7, “Installation options,” on page 33.

  Know what your options are for installing and configuring IBM Cognos Controller, and decide which option best meet your needs.

- **Decide how to maximize IBM Cognos Controller performance in your environment** Chapter 8, “Performance planning and tuning,” on page 37.

  Understand the factors that can affect IBM Cognos Controller performance, and plan to ensure and maintain adequate capacity for IBM Cognos Controller in your environment.

- **Decide how to configure IBM Cognos Controller multilingual capabilities** Chapter 9, “Globalization considerations,” on page 47.

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

When you complete your planning and are ready to install and use IBM Cognos Controller, refer to the other IBM Cognos Controller documents for step-by-step instructions “Introduction” on page v.
Chapter 7. Installation options

Before implementing IBM Cognos Controller, 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 install IBM Cognos Controller, you specify where to install the following components:

- gateway components, which include the gateway, Controller Client Distribution Server, and Gateway Integration Enabler
- application tier components, which include Controller Web Services Server, Report Server, and IBM Cognos Connection Integration Enabler.
- Content Manager components, which include Content Manager and Controller Framework Manager Model

You can install all IBM Cognos Controller components on one computer, or distribute them across a network.

Installing all components on one computer

Install all components on one computer when IBM Cognos Controller is accessed only inside your network firewall or for proof of concept in demonstration environments.

In the following diagram, all IBM Cognos Controller components are installed on one computer, along with a Web server. The content store and Controller database may be located on the same or different computers.
Installing gateway components on a separate computer

You can install gateway components on one computer, and install the remaining IBM Cognos Controller components on another computer.

Both the gateway components computer and the computer with the remaining IBM Cognos Controller components must include a Web server.

Installing gateway components on a separate computer provides an additional level of security if you have users who access IBM Cognos Controller remotely. The gateway components computer routes requests from remote users to the appropriate server and downloads IBM Cognos Controller to remote clients without exposing other IBM Cognos Controller components outside the firewall.

In the following diagram, remote users access the gateway components computer and internal clients access the servers directly. Incoming requests from remote clients are passed to the gateway and forwarded to the appropriate component on either the gateway or server computer. To enable internal clients to access IBM Cognos Controller from within the firewall, one gateway component (the Controller Client Distribution Server) is installed on the server computer. Internal clients access IBM Cognos Controller by typing the URL of the Controller Client Distribution Server directly in their Web browsers.
Distributing components on multiple computers

You can distribute components on multiple computers to improve performance, availability, capacity, and security.

When you distribute components on several computers, you must ensure that the components are configured so that they can access the required components on the other computers. On each computer, you must configure properties and set up virtual directories.

In the following diagram, the Controller Client Distribution Server and Gateway Server components are on one computer, the Controller Web Services Server component is on another computer, and the remaining IBM Cognos components are on a third computer.
Figure 8. Distributing components on multiple computers
Chapter 8. Performance planning and tuning

To ensure that IBM Cognos Controller performs optimally, plan your implementation with performance in mind.

After your initial planning and installation is complete, regularly monitor and tune performance as an IBM Cognos Controller environment changes over time. As user populations grow, processing requests tend to increase in number and complexity, and network capacity and other aspects of infrastructure may be modified. Maintaining IBM Cognos Controller performance is an ongoing task.

Performance planning

Performance is a measure of how effectively a system completes the tasks it was designed to accomplish.

An important aspect of performance is the capacity of your system to process requests quickly.

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 Controller capacity requirements, gather information about the following:

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

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

Estimating IBM Cognos Controller 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 Controller, estimate the number of people who will use IBM Cognos Controller and determine when they will use it. 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.
Concurrent users

The only users placing load on IBM Cognos Controller 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 Controller; that is, your total user population.

- **active users**
  A subset of named users, active users are logged on to IBM Cognos Controller 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. During the process of closing books at year-end, the number of concurrent users is significantly higher than at other times of the year.

Load distribution

In IBM Cognos Controller, load is generated by user navigation and processing requests, such as requests to add accounts or to view reports.

By determining when users are most likely to be using IBM Cognos Controller 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 Controller 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.

**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 a IBM Cognos Controller application depends on such things as the amount of work required to process requests, and the size and layout of the report output.

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.

**Planning infrastructure components**

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

Ideally, IBM Cognos Controller 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 Controller, 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.

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.
Citrix platforms

Citrix can be used to provide Windows client access to IBM Cognos Controller applications in distributed environments that have limited network bandwidth.

This type of access is typically required only for remote application administrators. IBM Cognos Controller also provides a Web client for normal user access.

The following table shows the minimum and recommended configuration for terminal emulation services.

Table 1. Minimum and recommended configuration for terminal emulation services

<table>
<thead>
<tr>
<th>Component</th>
<th>Minimum</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hard drive</td>
<td>SCSI</td>
<td>RAID</td>
</tr>
<tr>
<td>CPU</td>
<td>1 CPU, 2 GHz</td>
<td>2 CPU, 3 GHz</td>
</tr>
<tr>
<td>Free disk space</td>
<td>500 MB</td>
<td>10 GB (up to 30 GB for cubes)</td>
</tr>
<tr>
<td>Memory</td>
<td>2 GB</td>
<td>2 GB</td>
</tr>
</tbody>
</table>

Scalability

IBM Cognos products are easily expanded to adapt to the changing requirements of an application.

IBM Cognos Controller scales vertically using more powerful computers, and horizontally using a greater number of computers.

Consolidation load balancing

You can load balance the consolidation functions of IBM Cognos Controller by installing Controller Web Services Server on two computers and then moving the COM+ components that are used for consolidation to the second computer. The first computer accepts user requests but does not perform consolidation tasks. The second computer acts as the consolidation server.

In the following diagram, the components are fully distributed on several computers and two Controller Web Services Server computers are set up for consolidation load balancing.
Performance tuning

Because changes to your IBM Cognos Controller environment can affect performance, it is important to monitor and tune performance regularly.

Monitoring performance means regularly gathering data about your application usage and response times. Tuning can involve adjusting such things as your databases “Database tuning” and PDF rendering settings “Tuning PDF rendering” on page 43, and performing regular disk maintenance “Disk maintenance” on page 44.

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 “Performance planning” on page 37.

Database tuning

IBM Cognos Controller uses a relational database management system, such as Microsoft SQL Server, or Oracle.

To ensure that IBM Cognos Controller continues to perform well, it is important to maintain optimal performance for your databases. As IBM Cognos Controller and other applications place increasing demands on a database, you may experience increased response times and degradation in IBM Cognos Controller performance and scalability.

For information about tuning your database, see the documentation provided by your database vendor.
Tuning an IBM DB2 content store
If you use a IBM DB2® database for the content store, you can take steps to improve the speed with which requests are processed.

By default, DB2 assigns tables that contain large objects (LOBS) to a database-managed tablespace. As a result, the LOBS are not managed by the DB2 buffer pools. This results in direct I/O requests on the LOBS, which affects performance. By reassigning the tables that contain LOBS to a system-managed tablespace, you reduce the number of direct I/O requests.

Before tuning a DB2 content store, allocate sufficient log space to restructure the database.

To tune the DB2 content store, do the following:
• Export the data from the tables that contain at least one large object (LOB).
• Create the tables in a system-managed table space.
• Import the data into the tables.

Application server tuning
The Java application server for reporting components contains the Content Manager servlet and dispatcher servlet.

IBM Cognos Controller installs and uses Tomcat as the application server for reporting components. To enhance and maintain reporting performance, you should monitor memory settings and connection limits and tune them based on IBM Cognos Controller usage characteristics.

Changing memory settings
The memory settings of your application server dictate the memory that is available to Report Server 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 can 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, we recommend that you 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 kilobytes, but you should only consider this for single users, or for proof of concept or demonstration applications.

To configure Apache Tomcat memory settings, use IBM Cognos Configuration. For information about using IBM Cognos Configuration, see Installing and Configuring Controller.

Setting connection limits
For the Report Server 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 determines the number of available connections, or threads, that can be handled simultaneously by the application server process.
To configure Apache Tomcat connection settings, use the `\conf\server.xml` file located in the Tomcat directory in your IBM Cognos Controller installation location. IBM Cognos Controller uses the settings for the coyote connector.

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

**Tuning 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.

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

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, we recommend that you turn off font embedding.
- 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.

**Batch processing**

Batch processing provides a way to run large jobs during off-peak times.

For example, running consolidations takes a significant amount of time. You can schedule this job to run as an overnight batch process.

You can define up to four independent batch processes in Controller Configuration. Each batch job may be scheduled to run at a specific time. For information about defining batch processes, see *Installing and Configuring Controller*.

**Optimizing Microsoft Excel reporting**

In addition to the IBM Cognos reporting features, some reporting is available from Microsoft Excel.

For Microsoft Excel reports that contain a large amount of data, performance may be improved with enhanced reporting optimization. When this feature is enabled, bulk insert technology is used to insert data into the database, which allows for faster data transfer. This option only affects the IBM Cognos Controller Link for Microsoft Excel reports and Controller Report Generator reports.
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.

Monitoring Report Servers
You should conduct regular and targeted monitoring of the Report Servers.

This is important to assess the occurrence and impact of paging, memory use, and other measures of an efficient system.

Temporary space for Report Servers
Report Servers use a variety of directory access depending on the type and amount of activity.

For running reports, Report Servers frequently use temporary space. We recommend that the Report Server temporary space be hosted on a physical disk that is separate from other IBM Cognos Controller directory locations. This maximizes parallel disk access and avoids the unnecessary sequential access that is common when only a single disk device is used.

Reducing disk use
Depending on the size of reports and the amount of available memory, Report Servers may access a physical disk when processing reports. To improve performance, you can ensure that report processing uses available memory rather than disk space.

Using memory instead of disk space is particularly beneficial in cases where temporary files are created on Report Servers, causing information transfer from memory to disk. You can monitor the occurrence of temporary files using the c10_location\temp directory. Monitor this folder during report processing periods to determine whether temporary files are created as cclvpage*.tmp.

To ensure that Report Servers use memory instead of disk space, in the rsvpproperties.xml file, edit the VirtualMemoryDiagnostics property to use unlimited memory (value = 2) rather than limited memory (value = 0):
<property>VirtualMemoryDiagnostics</property>
<value type="long">2</value>

Note: Remove the comment to enable the VirtualMemoryDiagnostics property.

For information about using the rsvpproperties.xml file, see "Changing report processing behavior."

Changing report processing behavior
By default, IBM Cognos Controller is configured to process reports using a standard model applicable to all applications.

You can change the default processing behavior for the Report Server by modifying entries in the rsvpproperties file.
The rsvpproperties.xml.sample file is located in the \c10_location\configuration directory. Depending on your specific IBM Cognos Controller application and on the demands placed on it, changing settings in the rsvpproperties.xml file may benefit performance. Examples of settings that can be modified to enhance performance include prompt application and virtual memory.

To enable the rsvpproperties.xml.sample file, you must rename the file rsvpproperties.xml and restart the IBM Cognos service. This activity must be conducted on all Report Servers.

Settings in the rsvpproperties.xml file are very sensitive to change. Changing these properties may greatly impact the behavior of IBM Cognos Controller. As a result, you should use discretion when changing these values. For more information, contact Cognos Software Services for support.
Chapter 9. Globalization considerations

Many businesses perform transactions in the global market.

In this environment, users speak different languages, work in different currencies, and use different date and time formats.

You can configure the IBM Cognos Controller user interfaces for your preferred supported language and regional settings, or any combination of supported languages.

To configure IBM Cognos Controller for a global environment, you must use Controller Configuration to customize the language support for the IBM Cognos Controller and Cognos Viewer user interfaces and for the report templates.

You can control the language setting for the IBM Cognos Controller and Cognos Viewer user interfaces and for report templates. This setting is available in Controller Configuration.

Reporting components support various types of locale. By default, reporting components ensure that all locales, which may come from different sources and in various formats, use a consistent format. This means that all expanded locales conform to a language and regional code setting.

A locale specification consists of the following parts, separated by a dash (-):

- The first part is a two-character-set code, such as en (English), that specifies a language.
- The second part is a two-character-set code, such as us (United States), 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 IBM Cognos Connection user interface and all messages, including error messages.

Server locale

The server locale ensures that all log messages generated by reporting components are in one language. It is configured during installation. In a distributed environment, reporting components obtain the server locale from Content Manager.
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.
This Software Offering does not use cookies or other technologies to collect personally identifiable information.

**Trademarks**

IBM, the IBM logo and 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.
- 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  27

A
Access Manager  9
active users  37
administration  29
  IBM Cognos Connection  29
Apache Tomcat  42
application complexity  39
application servers  42
  multiple server access to reporting database  40
  tuning  42
application tier components  7
architecture  13
security  19
workflow  25
authentication providers  20
authentication services  19
authorization services  21

B
batch processing  43
BI Bus API  13
browsers  28
  configuring  28

C
capacity planning  37
  infrastructure components  39
certificate authority  22
third-party  23
CGI  5
  See common gateway interface
Citrix  39
coglocale.xml  27
Cognos Application Firewall  23
Cognos Configuration  5
Cognos Controller
  security  19
Cognos Controller solution  1
Cognos namespace  21, 28
Cognos security  20
Cognos Viewer  47
  language of user interface  47
  user interfaces  4
cogstartup.xml  27
COM+ identity  14
communications  14
COM+ Server  14
  communications  14
  (continued)
  component  7
COM+ users  14
  common gateway interface  5
  communications  13
components
  Content Manager  8
  distributing for consolidation load balancing  40
  installing on multiple computers  34
  installing on one computer  33
  startup configuration  26
components,  See gateway components
concurrent users  37
configuration  27
  Cognos Configuration  5
  for multilingual reporting  28
  Microsoft .NET Framework security policies  19, 27
  monitoring changes  27
  of Web browsers  28
  planning  31
  report processing  44
  security  28
  startup  26
configuration files  27
configuration requirements
  Citrix  39
  connecting to database  14
  connection limits
    setting  42
Content Manager
  Access Manager  9
  component  8
  importing IBM Cognos Controller standard reports package  27
Content Manager service  7
content providers  10
content store component  10
database connection management  14
Controller
  server components  4
Controller Client Distribution Server
    component  6
    configuring trust  19
Controller Configuration
  user interfaces  4
Controller Data Mart database  13
Controller database
  component  11
database connection management  14
  native security  19
Controller standard reports package
  component  10
Controller Web Services Server
  COM+ Server  7
  component  7
cryptographic keys  23
cryptographic providers  enhanced  22
### Cryptographic Providers
- **Standard**: 22
- **Services**: 22

### D
- **Data Mart**: 
  - Database for Framework Manager model: 13
- **Data Sources**: 10
- **Database**: 
  - Tuning: 41
  - Database connection management: 14
  - Content store database: 14
  - Controller database: 14
- **Databases**: 
  - Controller data mart: 13
  - Multiple application servers accessing one reporting database: 40
- **DB2 Content Store**: 42
- **Disk Maintenance**: 44
- **Dispatcher Component**: 7
- **Distributed Installation**: 35

### E
- **Enhanced Reporting Optimization**: 43
- **Estimating Load Distribution**: 37

### F
- **Firewall**: 23
- **Framework Manager Model Data Mart**: 13

### G
- **Gateway Component**: 5
- **Gateway Components**: 5
  - Installing on separate computer: 34
- **Gateway Integration Enabler Component**: 6
- **Geographic Distribution and Capacity Planning**: 37
- **Globalization Considerations**: 47
  - **Groups**: 22

### H
- **HTML Reports**: 
  - Running: 16
- **Hypertext Transfer Protocol**: 13

### I
- **IBM Cognos Application Firewall**: 28
- **IBM Cognos Configuration**: 26
  - Server Components: 5
  - User Interfaces: 4
- **IBM Cognos Connection**: 
  - Language of User Interface: 47
  - Server Components: 5

### L
- **Language**: 
  - IBM Cognos Controller and Report Templates: 47
  - Reporting Components: 47
  - Load Balancing: 
    - For Application Servers: 40
    - For Consolidation: 40
  - Load Distribution: 
    - Estimating: 37
  - Locale: 
    - Description: 47
    - Product: 47
    - Server: 47
  - Log Messages: 
    - Language: 47
    - Processing: 15
  - Log Service: 7
  - Logging: 
    - Secure: 23

### M
- **Maintaining Disks**: 44
- **Memory Settings**: 
  - Apache Tomcat: 42
  - Microsoft .NET Framework Communications: 13
  - Configuring Security Policies: 19, 27
  - Other Component: 10
- **Multilingual Reporting**: 
  - Configuring for: 28
  - Multiple Computer Installation: 34, 35
| N | named users 37 |
|   | native security 19 |
| O | other components 10 |
|   | Microsoft .NET Framework 10 |
| P | parameter signing 23 |
|   | PDF rendering 43 |
|   | PDF reports running 16 |
|   | performance planning 37 |
|   | performance tuning 41 |
|   | permissions 21 |
|   | planning checklist 31 |
|   | configuration 31 |
|   | implementation 26, 31 |
|   | installation 31 |
|   | performance 37 |
|   | port usage 15 |
|   | presentation service 7 |
|   | processing jobs batch mode 43 |
|   | processing log messages 15 |
|   | product locale 47 |

| R | rendering PDF reports 43 |
|   | Report Server component 7 |
|   | dispatcher 7 |
|   | monitoring 44 |
|   | services 7 |
|   | temporary disk space 44 |
|   | report service 7 |
|   | report templates language 47 |
|   | report types and capacity planning 37 |
|   | reporting database access from multiple application servers 40 |
|   | reports enhanced optimization 43 |
|   | running 16 |
|   | request flow processing 16 |
|   | roles 22 |
|   | rsyp.properties.xml 44 |
|   | running reports 16 |

| S | scalability 40 |
|   | secure logging 23 |
|   | secure sockets layer 22 |
|   | SecureError 23 |
|   | security See also cryptographic keys authentication providers 20 |
|   | Cognos Controller 19 |
|   | security (continued) configuration 28 |
|   | Content Manager 21 keys, 23 types of 19 |
|   | security policies configuring for Microsoft .NET Framework 27 |
|   | Microsoft .NET Framework 19 server locale 47 |
|   | server components Controller 4 |
|   | IBM Cognos Configuration 5 |
|   | IBM Cognos Connection 5 |
|   | IBM Controller Configuration 5 services authentication 19 |
|   | authorization 21 |
|   | Content Manager 7 |
|   | cryptographic 22 log 7 presentation 7 Report Server 7 report service 7 single computer installation 33 single signon 21 SSL See secure sockets layer standard reports package importing 27 startup configuration 26 files 27 |

| T | third-party certificate authority 23 tuning application servers 42 databases 41 DB2 content store 42 performance 41 |

| U | unattended installation 26 user community size 37 user interfaces 4 user load estimating 37 users 22 active 37 concurrent 37 named 37 |

| W | Web browsers configuring 28 Windows authentication 21 workflow 25 |

| X | XML configuration files 27 |