IBM Cognos Analytics
Version 11.1.x

Configuring Cognos Analytics Guide

©

Product Information

This document applies to IBM Cognos Analytics version 11.1.0 and may also apply to subsequent releases.

Copyright

Contents

Chapter 1. Distribution options

Before implementing IBM® Cognos® Analytics, decide how to install it in your environment. You can install all server components on one computer, or distribute them across a network. The best distribution option depends on your reporting requirements, resources, and preferences. Configuration requirements are different when you install all components on one computer, and when you distribute the components across multiple computers.

Cognos Analytics is compatible with other Cognos products. If your environment includes other Cognos products, you must consider how Cognos Analytics will fit into that environment.

Cognos Analytics cannot be installed to the same location as other Cognos products, such as Cognos Framework Manager, Cognos Transformer, Cognos PowerPlay, and so on.

Cognos Analytics components

IBM Cognos Analytics is a web-based business intelligence solution with integrated reporting, dashboarding, analysis, event management, and more features. Cognos Analytics includes server and modeling components.

Cognos Analytics integrates easily into your existing infrastructure by using resources that are in your environment. Some of these existing resources are required, such as a database for the content store. Other resources are optional, such as a security provider for authentication.

Tip: When Cognos Analytics is installed using the **Easy install** option, you do not need to configure a content store database or a security provider. The product is preconfigured and ready to use.

IBM Cognos Analytics runs WebSphere® Application Server Liberty Profile as the application server.

Server components

The server components for IBM Cognos Analytics are separated into three tiers: data, application, and an optional gateway.

The server components provide the user interfaces for reporting, dashboarding, analysis, event management, and so on, as well as the functionality for routing and processing user requests.

In the installation program, you can select to install the following server components:

- “Content Tier” on page 1
- “Application tier: components” on page 2
- “Gateway tier: web communication” on page 4

  Tip: The optional gateway is needed for Kerberos only.

As an optional server component, you can also install Cognos Analytics samples. Using data from a fictitious company, the Sample Outdoors Company, the samples illustrate product features and technical and business best practices. You can use the samples for experimenting with and sharing report design techniques, and for troubleshooting. For more information, see the *Samples for IBM Cognos Analytics Guide*.

Content Tier

Content Manager is the IBM Cognos Analytics service that manages the storage of application data, including security, configuration data, models, report specifications, report outputs, and so on.

Content Manager is needed to publish packages, retrieve and store report specifications, manage scheduling information, and manage the Cognos namespace.

Content Manager stores information in a content store database.

Application tier: components

The IBM Cognos Analytics applications tier contains one or more Cognos Analytics servers. The servers run requests, such as reports, analyses, and queries that are forwarded by the gateway, and renders the interfaces.

Configuring and managing the product - IBM Cognos Configuration

IBM Cognos Configuration is used to configure Cognos Analytics, and to start and stop its services.

Publishing, managing, and viewing content - Cognos Analytics portal

Cognos Analytics portal provides 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 Cognos Analytics applications through the portal. Other applications, and web addresses to other applications, can be integrated with the portal.

Professional reporting

Using the Reporting tool, report authors create, edit, and distribute a wide range of professional reports.

Dashboarding

Cognos Analytics provides dashboards to communicate your insights and analysis. You can assemble a view that contains visualizations such as a graph, chart, plot, table, map, or any other visual representation of data.

A dashboard is a type of view that helps you to monitor events or activities at a glance. It provides key insights and analysis about your data on one or more pages or screens.

Central administration - Manage and Administration Console

Cognos Analytics has a **Manage** function that you can use to perform common administration tasks day to day. An option from the **Manage** menu opens the **Administration Console**, a central management interface that contains the administrative tasks for IBM Cognos Analytics. It provides easy access to the overall management of the IBM Cognos environment. Access to the administration functions depends on user's permissions.

IBM Cognos Mobile

IBM Cognos Mobile extends Cognos Analytics and performance management to mobile devices. With its rich client, Cognos Mobile enables users to view on their devices Cognos Analytics reports, workspaces, and analyses produced by tools such as Reporting, Query Studio, Analysis Studio, and Cognos Workspace. Cognos Mobile delivers timely, informative, and interactive information to support mobile users in their decision-making processes, regardless of where the users are located.

Cognos Mobile processes each Cognos Analytics report that it receives and renders it in a mobile-friendly version.

Cognos Mobile uses the Cognos Analytics prompts functionality and scheduling mechanisms to deliver customized reports in a timely fashion. For more information about prompts, see the *IBM Cognos*

Analytics - Reporting User Guide. For more information about schedules, see the *IBM Cognos Analytics Administration and Security Guide*.

Cognos Mobile uses Cognos Analytics security, implements additional security measures specific to a mobile application, leverages various vendor-specific security architectures, and takes advantage of device-based and server-based security measures.

Many of the device-specific management servers and administration tools used by Cognos Mobile offer the ability to remotely remove content from a device or to disable the device completely. So, for example, if a device is lost or stolen, the Cognos Analytics administrator can use this functionality to protect sensitive content on the device. Or, a Cognos Analytics administrator could set an expiry date for a report after which the report becomes inaccessible until the user re-authenticates. For more information about Cognos Analytics security, see the *IBM Cognos Analytics Administration and Security Guide*. For more information about device management and security, see the documentation for the device.

Cognos Mobile also supports requests between the mobile device and the server environment for the search, browse, and run product functions:

You must install and run the same version of Cognos Mobile and Cognos Analytics server.

Ad hoc querying and self-service reporting - Query Studio

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

Monitoring data for exceptional conditions - Event Studio

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

Facilitating decision-making - IBM Cognos Workspace

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

You can also use social software such as IBM Connections for collaborative decision making.

Microsoft Office compatibility - IBM Cognos for Microsoft Office

Using IBM Cognos for Microsoft Office, Microsoft Office users can access data and visualizations from IBM Cognos reports within Microsoft Office applications, such as Excel, PowerPoint, and Word.

Cognos for Microsoft Office components are included with Cognos Analytics and must be installed separately.

Gateway tier: web communication
Gateways are often CGI programs, but they can follow other standards, such as Internet Server Application Program Interface (ISAPI) or Apache Modules (apache_mod). IBM Cognos Analytics uses only CGI, ISAPI or Apache module for Kerberos. Otherwise, you do not need to configure a gateway.

In IBM Cognos Analytics the application tier provides the functions of a gateway.

Modeling components

Modeling components model data within data sources to structure and present data in a way that is meaningful to users. Modeling components include the following tools:

IBM Cognos Analytics web modeling

IBM® Cognos® Analytics has a simple-to-use, zero-footprint modeling tool that you can use to quickly create data modules from various data sources. You can use data sources, such as data servers, uploaded files, and previously saved data modules to create data modules. Cognos Analytics data modeling uses intent-driven modeling to generate a module by using terms that you define. For details on all the available features, see the *IBM Cognos Analytics Data Modeling Guide*.

Cognos Analytics data modeling does not replace the more complex modeling capabilities of IBM Cognos Framework Manager or IBM Cognos Cube Designer. These tools are still available in Cognos Analytics.

Creating a business view of your data - Framework Manager

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

Framework Manager must be installed to a different location than Cognos Analytics.

ROLAP modeling - Cube Designer

IBM® Cognos® Cube Designer is the modeling tool provided with IBM Cognos Dynamic Cubes. You use it to build dynamic cubes and publish them for use in IBM Cognos Analytics.

To get started, you import metadata from a relational database. Using the metadata, you model dynamic cubes and save the cube definitions in a project. After you publish the cubes, they are listed as data sources in Content Manager and their related packages are available to report authors.

Cube Designer must be installed to a different location than Cognos Analytics.

Multidimensional modeling - IBM Cognos Transformer

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

Transformer must be installed to a different location than Cognos Analytics.

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

Import and manage maps (legacy Map Manager maps only)

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

Map Manager must be installed to a different location than Cognos Analytics.

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

Required database components

In addition to the tools that are provided, IBM Cognos Analytics requires the following components that are created using other resources.

Content store

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

When setting up your Cognos Analytics environment, set up the content store to use a supported database that can be secured and tuned for performance and stability. For more information, see the topic about deploying the entire content store in the *IBM Cognos Analytics Administration and Security Guide*.

Design models and log files are not stored in the content store.

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

Data sources

Data sources, also known as query databases, are relational databases, dimensional or OLAP cubes, files, or other physical data stores that can be accessed through Cognos Analytics. Application tier components use data source connections to access data sources.

Cognos Mobile components

IBM Cognos Mobile includes Cognos Mobile service and Cognos Mobile app. These components are installed with IBM Cognos Analytics.

After you configure the Cognos Mobile service, users can install the Cognos Mobile app on their mobile devices to access Cognos Analytics content, such as reports or dashboards. To use the app, users download the iOS version from the Apple App Store or the Android version from the Google Play Store.

The Cognos Mobile service handles the following operations:

- Pushes report and analysis content to the mobile devices.
- Facilitates incoming and outgoing report-related and analysis-related requests between the mobile device and the environment to search, browse, or run reports.
- Synchronizes the mobile content store on the server with the mobile database on the mobile device.
- Communicates with the mobile device.

The mobile device contains the Cognos Mobile app and the compressed and encrypted mobile content store. These components provide the functionality that the mobile device user needs to work with Cognos Analytics reports, dashboards, and analyses.

The following diagram shows how the components interact within the Cognos Analytics environment. The mobile devices connect to the IBM Cognos server through the internet and wireless carriers using HTTP.

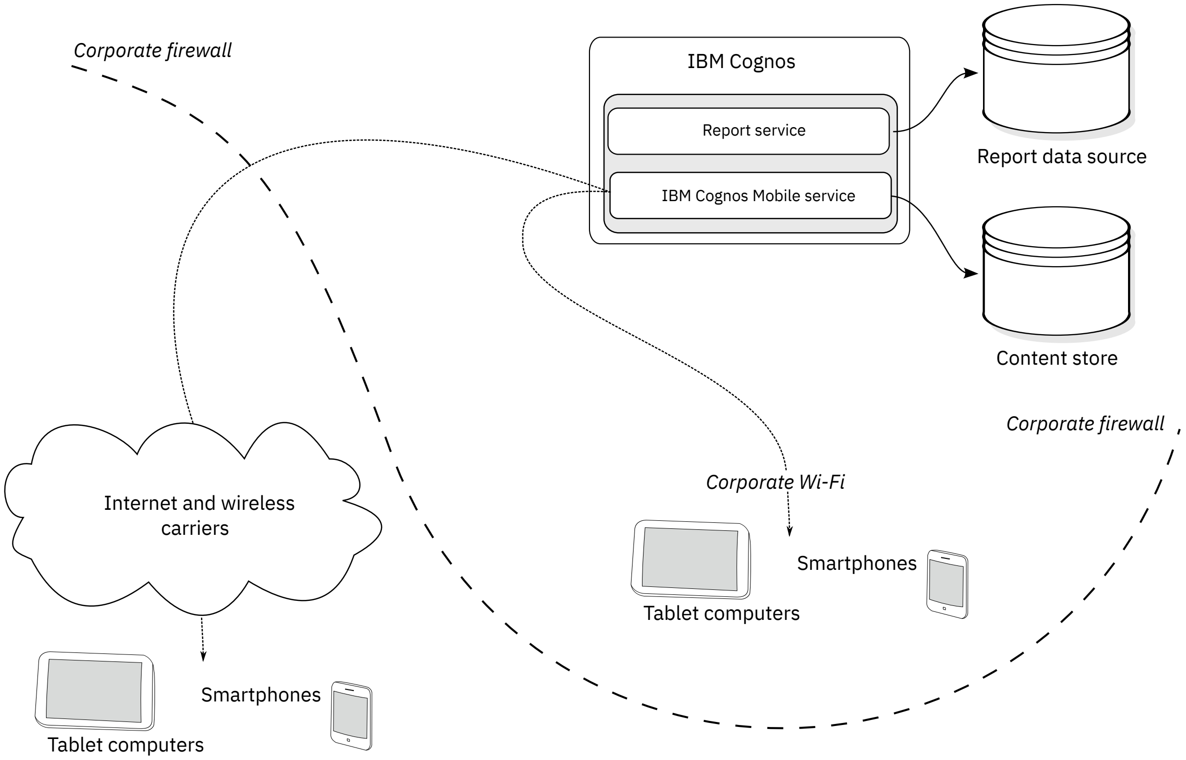


Figure 1: Cognos Mobile components within the Cognos Analytics environment

Distributing components

When you install IBM Cognos Analytics server components, you specify where to place the application tier, the data tier (Content Manager), and the optional gateway tier components.

You can use the following installation scenarios:

- Install all components on one computer.

  This option is typically used for departmental deployments, as a demonstration system, or in a proof of concept environment.

- Install application tier components and Content Manager on separate computers.

  Choose this option to maximize performance, availability, capacity, or security based on the processing characteristics of your organization.

- Install the optional gateway on a separate computer.

  In this option, the gateway and web server are on one computer, and the remaining Cognos components are on other computers. You can choose this option if you have existing web servers that are available to handle Cognos Analytics components requests.

- Consolidate multiple servers by installing on System z®

IBM Cognos Analytics is supported for Linux on System z operating system. This type of installation is suitable when you are setting up or customizing an installation in your environment to suit IT and infrastructure requirements.

After installing the server components, you must configure them so they can communicate with each other.

In addition to installing the data tier (Content Manager), application tier, and optional gateway tier components, you can also install Cognos Framework Manager, the metadata modeling tool, and Cognos Transformer, the modeling tool for creating PowerCubes. No matter which IBM Cognos installation scenario you follow, install the modeling components in separate locations.

Application Tier Components and Content Managers on separate computers

Application Tier Components balance loads, access data, perform queries, schedule jobs, and render reports. Content Manager stores all report specifications, results, packages, folders, and jobs in the content store.

You can install the Application Tier Components and Content Manager on the same computer, or on different computers. Installing on different computers can improve performance, availability, and capacity.

More than one Content Manager
You can install any number of installations of Content Manager, although only one is active at any time. The other installations each act as a standby Content Manager. One becomes active only if a failure occurs that affects the active Content Manager computer. For failover support, it is advisable to install Content Manager on two or more computers.

Install multiple Content Managers

Content Manager stores data that IBM Cognos Analytics needs to operate, such as report specifications, published models, and the packages that use them; connection information for data sources; information about the external namespace and the Cognos namespace itself; and information about scheduling and bursting reports. The content store is a relational database management system (RDBMS). There is only one content store for each IBM Cognos installation.

You may choose to install Content Manager separately from the Application Tier Components. For example, you may want Content Manager in your data tier instead of in the applications tier.

When an active Content Manager fails, unsaved session data is lost. When the new active Content Manager takes over, users may be prompted to logon.

In the following diagram, the gateway passes the request to the dispatcher (not shown), which passes it to the default active Content Manager computer. Because the computer has failed, the request is redirected to the standby Content Manager computer, which became active when the default active Content Manager computer failed.

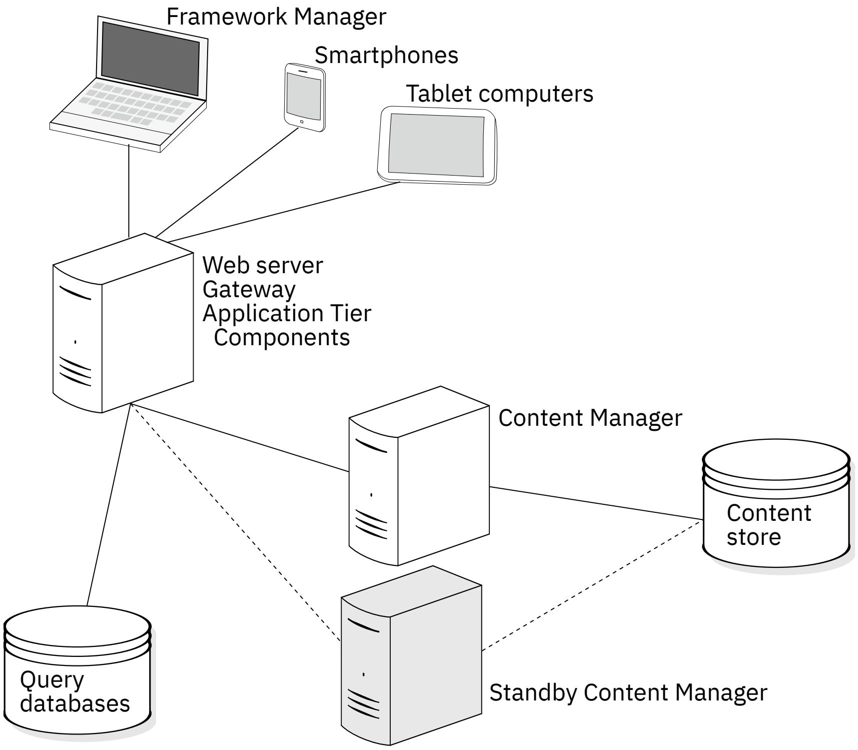


Figure 2: Installation with an active and a standby Content Manager

Configuration requirements

On each computer where you install Content Manager, you must

- specify connection information to the content store
- specify the Dispatcher URIs
- specify all Content Manager URIs
- specify the Dispatcher URI for external applications
- set up a connection to an email server (if you want to email reports or send notifications)

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

Configuration requirements

If you install one or more Application Tier Components on a separate computer, to ensure that they can communicate with other IBM Cognos Analytics components, do the following:

- specify all Content Manager URIs
- specify the Dispatcher URIs
- specify the Dispatcher URI for external applications

Consolidate servers for Linux on System z

Linux on System z operating system is a native implementation of the Linux operating system. Hosting options include running Linux in one or more logical partitions (LPAR).

Integrated facility for Linux (IFL)

IFLs are System z processors dedicated to running Linux operating system workloads either natively, or under virtualization software, depending on your needs. IFLs enable you to consolidate and centrally manage Linux resources on System z.

Logical partition (LPAR) mode

Linux operating system can run in LPARs and communicate with other Linux partitions using TCP/IP connections.

The horizontal scalability in a large Linux environment is limited by the number of LPARs that can be created. Running Linux in LPARs may be best if you are running a small number of Linux images, and those images will each be using a large amount of processing power, or will require a very large amount of dedicated memory. This ensures that the images will not have underutilized resources allocated to them.

Installation for optional modeling components

You install the modeling tools, such as Framework Manager and Transformer on Microsoft Windows operating system computers.

To publish packages so that they are available to users, you must configure the optional modeling tools to use a dispatcher, either directly or through a gateway. If the portal is secured, you must have privileges to create data sources and publish packages in the portal

Firewall considerations

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

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

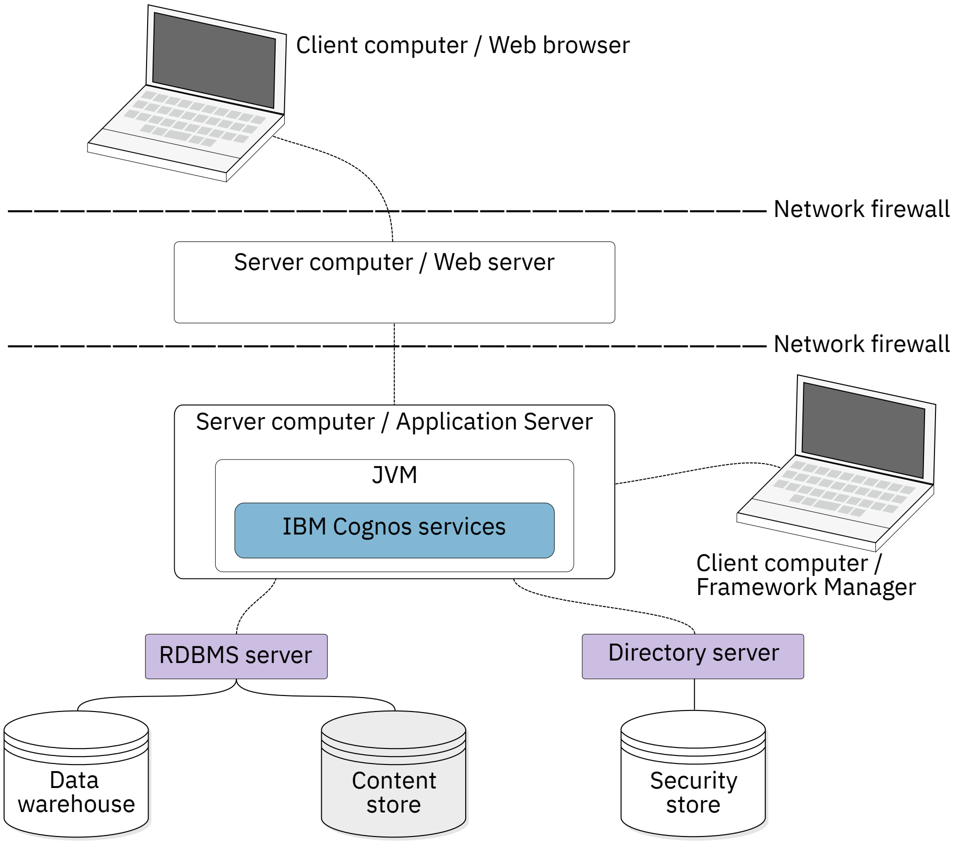

Client computer / Web browser
Network firewall
Server computer / Web server
Network firewall
Server computer / Application Server
JVM
IBM Cognos services
Client computer / Framework Manager
RDBMS server
Directory server
Data warehouse
Content store
Security store

Figure 3: Client computer outside of firewall

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

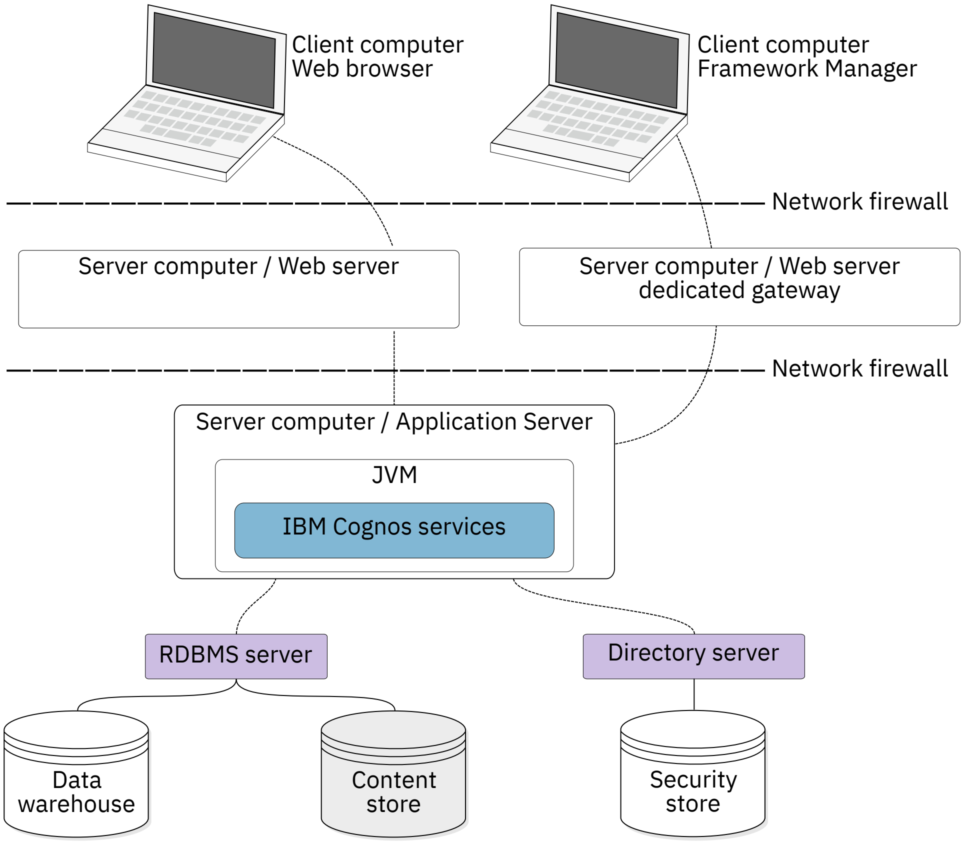


Figure 4: Client computer outside of firewall

Distributing Framework Manager components

Framework Manager communicates with the Application Tier Components, which can be installed on one or more application servers. To publish packages, you must configure Framework Manager to communicate with the dispatcher, either directly or through a dedicated gateway.

Configuration requirements

On the computer where Framework Manager is installed, configure the following environment properties:

- **Gateway URI**
- **Dispatcher URI for external applications**

If the modeling tool is using a dedicated gateway instead of communicating directly with the dispatcher, you must also configure the **Dispatcher URIs for gateway** property on the dedicated gateway computer.

Distributing Transformer components

Transformer can be installed on a computer that contains other IBM Cognos Analytics components or on a computer that is separate from other IBM Cognos Analytics components. When installed separately, Transformer can be used as a standalone product or it can be configured to communicate with other IBM Cognos Analytics components.

Transformer consists of the following components. You may have one or both, depending on your environment.

- Transformer on Windows

  This is the modeling tool for Microsoft Windows operating system for designing PowerCubes that are used in IBM Cognos Analytics. It can also be used to build and publish PowerCubes.
- Transformer on UNIX or Linux

This is a command line utility for building PowerCubes on UNIX and Linux operating systems. You first design the models using Transformer Windows or MDL scripting, and then use the models to build the PowerCubes.

You install Transformer PowerCube building components for Linux on System z.

Supported features

When you use Transformer as a standalone product, you can use data sources that are external to IBM Cognos Analytics and you cannot create secured views with dimensional filtering. When you use Transformer with other IBM Cognos Analytics components, you can use the following features provided by IBM Cognos Analytics:

- IBM Cognos Analytics authentication providers
- IBM Cognos Analytics data sources, such as published packages, Query Studio reports, and Reporting reports

  You cannot use flat files as data sources.
- the portal for publishing the PowerCube data source and package
- building PowerCubes

Role-based server considerations

You may want to set up dedicated Transformer servers for optimal cube build performance and accessibility to the IBM Cognos Analytics users. In this scenario, consider the following requirements:

- Database client software is installed on any computer where Transformer will be used to build PowerCubes or test data sources.
- For data source connectivity, set appropriate environment variables for UNIX and Linux servers.
- IBM Cognos Analytics servers have access to the location where PowerCubes are stored so that the report server can access the PowerCubes.

Building and updating production PowerCubes can be scripted and run remotely when sufficient access and user privileges are set up. For more information about building and updating production PowerCubes, see the Transformer *User Guide*.

Business analysts or specialists

You may have specialized business or power users who want to build PowerCubes that are modeled on a combination of corporate and personal data sources. These users may want to do their own analysis of the data for their line of business or a small group of users. You can enable such users to be self-sufficient within the IT and security infrastructure of the organization by meeting the following requirements:

- Database client software is installed, or available for modelers to install, on the Transformer computers that are used to access IBM Cognos Analytics data sources or IBM Cognos Series 7 IQD data sources.
- Modelers must have privileges to create a data source in IBM Cognos Administration.

  Modelers do not need direct access to IBM Cognos Administration. They can create and update data sources by using Transformer or command line tools. You can provide modelers with a secured folder in the portal in which to publish PowerCube packages.
- Modelers must have access to a location in which to store the PowerCube after building it.

  This location must also be accessible to the IBM Cognos service and can be a secured share on a LAN.

- To build PowerCubes on a specific Transformer server, modelers should have FTP privileges to transfer models and execute privileges to build cubes on that server.

  Modelers can transfer models and execute cube builds using scripts. Modelers can also use automated methods to build PowerCubes. For more information, see the *Administration and Security Guide*.

Configuration requirements

To publish PowerCube packages, you must configure Transformer to communicate with the dispatcher, either directly or through a dedicated gateway. If IBM Cognos Connection is secured, you must have privileges to create data sources and publish packages in the portal.

On the computer where Transformer is installed, configure the following environment properties:

- **Gateway URI**
- **Dispatcher URI for external applications**

If the modeling tool is using a dedicated gateway instead of communicating directly with the dispatcher, you must also configure the **Dispatcher URIs for gateway** property on the dedicated gateway computer.

Distribution options for Cognos Mobile

IBM Cognos Mobile is an integrated component of the IBM Cognos Analytics architecture. You can install all IBM Cognos Mobile components on one computer, or distribute them across a network.

Cognos Mobile consists of the following components:

- Application tier components
- The Cognos Mobile app.

You must install the Cognos Mobile application tier components with the Cognos Analytics application tier components.

All required components are installed and enabled by default.

Cognos Mobile components installed on one computer

You can install and configure IBM Cognos Mobile on a single computer.

The following diagram shows an example where all server components are installed on one computer.

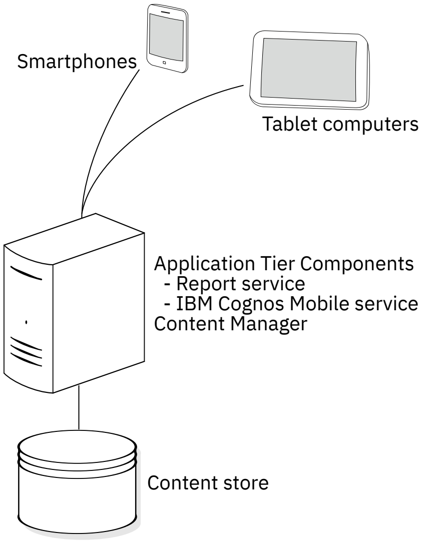


Figure 5: Cognos Mobile server components installed on one computer

Cognos Mobile components installed on separate computers

You distribute IBM Cognos Mobile components using the same installation and configuration method that you use to distribute IBM Cognos Analytics components.

Run the installation on each computer and then complete the configuration by specifying the location of distributed IBM Cognos Analytics components.

In a distributed installation, you install the Cognos Mobile application tier components on the systems where you want to run the Cognos Mobile service.

All instances of the IBM Cognos Mobile service must be able to access the database where the IBM Cognos Mobile tables are stored. If an IBM Cognos Analytics server instance is not configured with the database details for the IBM Cognos content store, or if you want IBM Cognos Mobile to use a database instance other than the IBM Cognos content store, use IBM Cognos Configuration to add a database.

IBM Cognos Analytics with other IBM Cognos products

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

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

Duplicated Services if Using Multiple Products

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

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

IBM Cognos products that interoperate with IBM Cognos Analytics

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

Cognos Planning - Analyst

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

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

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

Cognos Planning - Contributor

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

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

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

Cognos Controller

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

Cognos Transformer

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

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

Before you load the model, the IBM Cognos Series 7 namespace must be configured in IBM Cognos Analytics and the name ID that is used to configure it in IBM Cognos Analytics must match the name used in IBM Cognos Series 7.

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

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

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

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

Cognos Lifecycle Manager

Lifecycle Manager is a Windows-based application for auditing upgrades from Cognos 8 and above to newer versions of IBM Cognos Analytics. It provides a verification feature that validates, executes, and compares report results from two different IBM Cognos Analytics releases. This helps to identify upgrade and compatibility issues between releases. User interface design and status reporting functionality provide both a proven practice process and support for upgrade project planning and status reporting.

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

Planning Analytics

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

For more information, see the *IBM Planning Analytics* documentation.

Chapter 2. Upgrading Cognos Analytics

When upgrading IBM Cognos Analytics, you need to back up the content store, upgrade your data, understand the implications of the upgrade on other components in a distributed environment, ensure that files that must be preserved are not overwritten, and possibly perform other upgrade tasks.

The upgrade information in this document is applicable to all supported versions of Cognos Analytics. For version-specific information, the version number is included in the topic title.

Upgrading your current version of Cognos Analytics 11

You can upgrade your version of IBM Cognos Analytics by performing an "over the top" installation.

This is the default upgrade method, and the simplest and easiest way to upgrade. All components are upgraded to a newer version using the same configuration details, ports, themes and extensions as your previous installation.

The new and improved upgrade procedure takes advantage of the Cognos Analytics continuous delivery model, and deploys new features quickly and easily.

Detailed steps and a video can be found here: http://www-01.ibm.com/support/docview.wss?uid=swg21994915

Data upgrade tasks for Cognos Analytics version 11.1

To support the optimized user experience in dashboards, explorations, and other components, and to improve query performance on uploaded files and data sets, the IBM Cognos Analytics version 11.0.x data must be upgraded.

The upgrade process includes the following two tasks: retrieving some deeper data characteristics from data servers, packages, uploaded files, and data sets, and upgrading the Parquet file format in uploaded files and data sets.

Retrieve deeper data characteristics from data servers, packages, uploaded files, and data sets

The deeper data characteristics support the product functions that are behind the optimized user experience in dashboards, explorations, and other components. These characteristics are captured from samplings of data from the underlying sources.

Cognos Analytics 11.1 captures the deeper data characteristics for the following reasons:

- To intelligently set the default column properties, such as **Usage** and **Aggregate**.
- To provide recommendations for visualizations in dashboards, stories, and explorations.
- To determine the subset of fields that are the best candidates to show in the relationship diagram in **Explore**.
- To enable **Assistant** to be more successful in understanding the user's intent.
- To provide other forms of automated assistance.

To retrieve the deeper data characteristics, you need to re-upload the Cognos Analytics 11.0.x sources using the following methods:

- For data server connections, reload the schemas metadata.

  Use the **Load options** option. Ensure that the following check boxes are selected: **Retrieve the primary and foreign keys**, **Retrieve sample data**, **Retrieve statistics**.

For more information, see the topic about preloading metadata from a data server connection in the *IBM Cognos Analytics Managing Guide*.

- For packages, use the **Enrich package** action.

  Use the automatic enrichment option, and ensure that the check boxes **Retrieve sample data** and **Retrieve statistics** are selected on the **Load options** tab.

  For more information, see the topic about enriching packages in the *IBM Cognos Analytics Managing Guide*.
- For uploaded files and data sets, either run the `ParquetUpgrade` utility with option **m** or refresh the individual files and data sets manually.

  The `ParquetUpgrade` utility with option **m** retrieves the deeper data characteristics from all uploaded files and data sets in the content store. When running this utility, you will upgrade the Parquet format in the affected files and data sets at the same time. For more information, see "Running the ParquetMigrate utility " on page 18.

  For individual uploaded files, use the **Append file** and **Replace file** options. For individual data sets, use the **Refresh** option.

Upgrade the Parquet format in uploaded files and data sets

The Parquet file format that is used to store uploaded files and data sets has changed in Cognos Analytics version 11.1. The new Parquet format enables faster query processing on uploaded files and data sets.

You can implement this upgrade in the following ways:

- Use the `ParquetUpgrade` utility to upgrade the Parquet format in all uploaded files and data sets in the content store.

  Run this utility before users start running the reports, dashboards, or explorations. This ensures that all workloads immediately benefit from the performance gains associated with the new format. For more information, see "Running the ParquetMigrate utility " on page 18.
- Manually refresh data in the individual uploaded files and data sets.

  Use the **Append file** and **Replace file** options on uploaded files. Use the **Refresh** option on data sets.
- Do not upgrade at all.

  When a query uses data that wasn't upgraded, the query service internally initiates the upgrade, and the users experience a one-time performance degradation when they run the dashboards, stories, reports, or explorations in Cognos Analytics 11.1. Subsequent queries use the upgraded data.

The new Parquet format is used automatically when new files are uploaded, new data sets are created, and when deployment archives that contain uploaded files and data sets are imported.

Running the ParquetMigrate utility

Use the `ParquetMigrate` utility to apply the new Parquet format to uploaded files and data sets from IBM Cognos Analytics 11.0.x. When used with its option **m**, this utility also retrieves the deeper data characteristics from uploaded files and data sets.

The Parquet format that is used to store data in uploaded files and data sets has changed between Cognos Analytics versions 11.0.x and 11.1. Run the `ParquetUpgrade` command before users start running dashboards and reports. This ensures that all workloads immediately benefit from performance gains of the new format. If a query uses data that wasn't upgraded, the query service internally initiates the upgrade and the users experience a one-time performance degradation when they run the dashboards, stories, reports, or explorations in Cognos Analytics 11.1. Subsequent queries use the upgraded data.

The `ParquetMigrate` command supports the following parameters:

-h ***URL***

The URL to an active Cognos Analytics server. When you don't specify the URL, the URL that is configured in Cognos Configuration on the computer from which the command is run is used.

-n ***Namespace***

The namespace to authenticate into when connecting to the Cognos Analytics server.

-u ***User name***

The user name to authenticate with when connecting to the Cognos Analytics server.

-p ***Password***

The password to use for authentication to the Cognos Analytics server.

-d

Displays information about the uploaded files and data sets in the content store. No objects are upgraded.

-m

Retrieves the deeper data characteristics in Cognos Analytics. For more information, see "Data upgrade tasks for Cognos Analytics version 11.1" on page 17

Procedure

1. Open the command line utility, and navigate to the *cognos_analytics_location*\bin64 directory.
2. Specify the ParquetMigrate command using the following syntax.

   To display information about uploaded files or data sets, use the following syntax:

   ```
   ParquetMigrate -d -n namespace -u user_name -p password
   ```

   Or

   ```
   ParquetMigrate -d -h http://cognos_analytics_host:9300 -n namespace -u user_name -p password
   ```

   To upgrade files or data sets, use the following syntax:

   ```
   ParquetMigrate -d -n namespace -u user_name -p password
   ```

   To upgrade files and data sets, and at the same time retrieve the deeper data characteristics, use the following syntax:

   ```
   ParquetMigrate -m -d -n namespace -u user_name -p password
   ```

3. Run the command.

Results

When the command completes, the number of upgraded objects is displayed. A value of 0 indicates that no objects requiring upgrade were found.

Preserved files and folders when upgrading Cognos Analytics

You can install a new version of IBM Cognos Analytics over your current, running version of the product without overwriting configuration settings from the previous version.

Files to be preserved during an upgrade are listed in the *install_location*\configuration\preserve\.ca_base_preserve.txt file. Do not edit this file. Instead, edit the *install_location*\configuration\preserve\preserve.txt file if you want to remove or preserve certain files or directories when upgrading. Instructions about using preserve.txt are included in the file itself.

Tip: Hard or soft links created by customers within the Cognos Analytics file structure are not supported.

By default, the following folders and files are preserved when upgrading Cognos Analytics:

Folders

install_location\data

install_location\data\cmstorage

install_location\data\search

install_location\deployment

install_location\drivers

install_location\ldapschema

install_location\informix

install_location\configuration\certs

install_location\configuration\csk

install_location\configuration\data

install_location\configuration\caSerial

install_location\webcontent\bi\alp\images

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

install_location\iso-swid

install_location\apacheds\instances\cognos

install_location\war\AuditExt

Configuration files

install_location\configuration\cogconfig.prefs

install_location\configuration\cogconfig_reg.txt

install_location\configuration\coglocale.xml

install_location\configuration\cogstartup.xml

install_location\configuration\dispatcher.properties

install_location\configuration\install_gatewayurl.xml

install_location\configuration\installData.properties

install_location\configuration\ipfclientconfig.xml

install_location\configuration\configuration\caSerial

install_location\configuration\xqe.diagnosticlogging.xml

install_location\configuration\c11AuditExtension.keystore

install_location\configuration\local-server.xml

Miscellaneous files

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

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

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

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

install_location\wlp\usr\servers\dataset-service\bootstrap.properties

install_location\wlp\usr\servers\dataset-service\jvm.options

install_location\wlp\usr\servers\dataset-service\server.xml

install_location\cgi-bin\web.config

install_location\wlpdropins\AuditExt.war

Webcontent files

install_location\webcontent\web.config *install_location*\webcontent\default.htm

install_location\webcontent\index.html

install_location\webcontent\bi\web.config

TM1 files

install_location\templates\ps\portal\variables_TM1.xml

install_location\templates\ps\portal\variables_plan.xml

install_location\templates\ps\portal\icon_active_application.gif

install_location\webcontent\planning.html

install_location\webcontent\tm1\web\tm1web.html

install_location\webcontent\PMHub.html

install_location\templates\ps\system.xml

install_location\templates\ps\portal\system.xml

PowerPlay files

install_location\webcontent\skins\series7\ppwb

install_location\webcontent\skins\presentation\ppwb

install_location\webcontent\skins\modern\ppwb

install_location\webcontent\skins\corporate\ppwb

install_location\webcontent\skins\contemporary\ppwb

install_location\webcontent\skins\classic\ppwb

install_location\webcontent\skins\business\ppwb

install_location\webcontent\bi\skins\series7\ppwb

install_location\webcontent\bi\skins\presentation\ppwb

install_location\webcontent\bi\skins\modern\ppwb

install_location\webcontent\bi\skins\corporate\ppwb

install_location\webcontent\bi\skins\contemporary\ppwb

install_location\webcontent\bi\skins\classic\ppwb

install_location\webcontent\bi\skins\business\ppwb

install_location\webcontent\bi\ppwb

install_location\webcontent\ps\powerplaystudio

install_location\webcontent\fragments\ppesAdmin

install_location\webcontent\ppwb

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

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

install_location\msgsdk\ppesAdminStrings_en.xml

install_location\msgsdk\ppesAdminStrings_ldkspec.xml

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

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

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

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

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

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

LCM files

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

```
install_location\project
```

```
install_location\benchmarks
```

```
install_location\configuration
```

You need to manually migrate these files and folders only under the following circumstances:

- You are installing the new version in a new directory.
- You are uninstalling the current version, and then installing the new version.

  Uninstalling the current version completely deletes the *install_location* directory.

Standard upgrade process

The enhancements in new versions of IBM Cognos Analytics can affect many parts of your business intelligence environment. Therefore it is best to perform the upgrade in stages. To ensure success, treat upgrading as an IT project that requires careful planning, adequate time, and adequate resources.

You must plan your upgrade so that you know what to expect at each stage of the process. In the planning stage, you can review the upgrade documentation for information about expected behavior, new features, deprecated features, compatibility between versions, and requirements for preparing your production environment. When you finish the review, you can then conduct a site survey to identify the BI infrastructure, applications, reports, and custom configuration settings. Finally, you can test the upgrade on a subset of your data so that you can fine-tune your reports and data before committing to the full upgrade.

When planning your upgrade, perform the following tasks:

- Gather the necessary information, such as the required inputs and expected outputs for each phase.
- Assess the applications in your reporting environment and group similar reports together.
- Install the new software in a test environment and deploy the content to the test environment.
- Test the upgraded applications to ensure that your reports run as expected.

  You can use Lifecycle Manager to compare reports from a different version of IBM Cognos Analytics. For more information, see the Lifecycle Manager documentation.

Deployment and testing is usually an iterative process. Assess any differences between the source and target environments. Move to your production environment when you are satisfied that the deployed applications meet your business requirements.

The following diagram shows a general upgrade workflow and the stages in the upgrade process. The process includes the following stages:

- Creating an upgrade plan, which includes the following activities:
  - Reviewing resources, such as the documentation, the Upgrade Central Website (www.ibm.com/support/docview.wss?uid=swg22011664), and the following upgrade steps: http://www.ibm.com/support/docview.wss?uid=swg21994915
  - Verifying the supported environments to ensure compatibility with your other software by going to the IBM Software Product Compatibility Reports page (www.ibm.com/support/docview.wss?uid=swg27047186). You may also want to check this page if you are thinking of upgrading your operating system.

- Evaluating your existing system to determine what you want to move to your new version of the product.
- Creating a detailed plan to implement your upgrade strategy.

- Creating a development or test system with the new version of the product.
- Using the information learned from the development or test system and applying it as you create your QA or production systems.

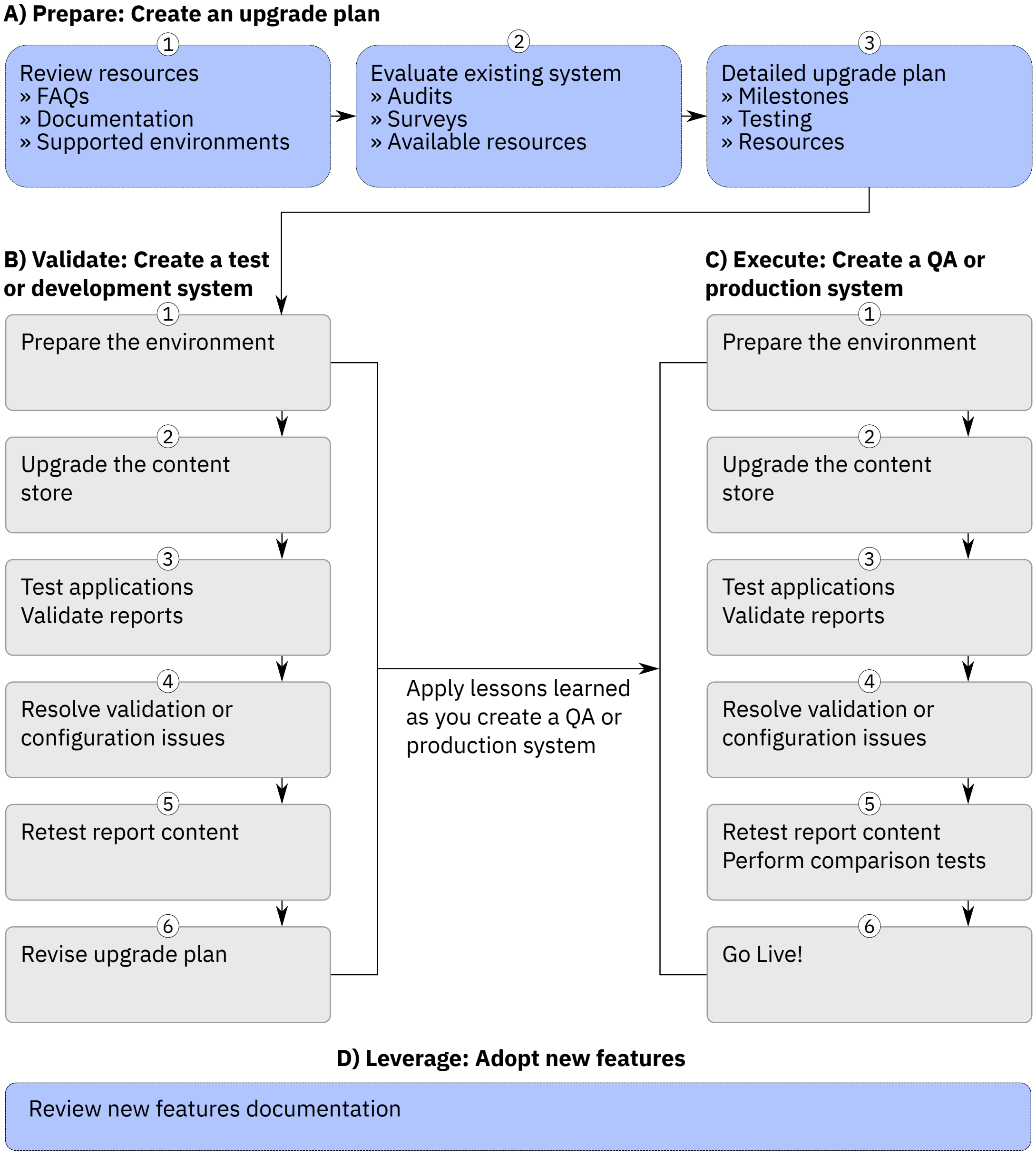


Figure 6: Upgrade process

Reviewing the documentation

Documentation is provided to help you achieve a successful upgrade.

All the documentation is available online at IBM Cognos Knowledge Center (http://www.ibm.com/support/knowledgecenter/SSEP7J_11.1.0/com.ibm.swg.ba.cognos.cbi.doc/welcome.html).

Assess applications in your environment before you upgrade

Preparing to upgrade provides an opportunity to review your existing applications and clean up your source environment.

For example, you might have many applications in your environment. However, it is not uncommon to find that a number of applications are not used or no longer meet your requirements.

Assessing your applications is a useful exercise because it can reduce the number of applications to consider during an upgrade.

An audit of your existing applications can include the following tasks:

- Do a site survey to assess the current production environment and identify areas that require attention during the upgrade. The site survey includes information about the infrastructure, applications, users, and configuration settings.
- Assess the software that you use in your environment and create a list of the software, such as operating systems, web servers, security providers, and databases.

  To review an up-to-date list of environments that are supported by IBM Cognos Analytics products, including information on operating systems, patches, browsers, web servers, directory servers, database servers, and application servers, see the IBM Software Product Compatibility Reports page (www.ibm.com/support/docview.wss?uid=swg27047186).
- Complete a detailed assessment of your applications. The usage, age, size, and complexity of your applications are important factors to consider when planning the upgrade. The total size of the applications can have an impact on the time required to complete the upgrade.
- List the following information about your configuration:
  - Configuration settings that you enabled in IBM Cognos Configuration

    Installing the new version of the product in a different location than the existing version lets you compare the settings between the two version. To run the two versions you must ensure that you use unique port numbers, web server aliases, and unique content store databases.
  - Changes to other configuration files

    You must manually change other configuration files during the upgrade. If you changed other configuration files, you must assess the changes that you want to preserve in the upgraded environment. This might include `.xml`, `.txt`, and `.css` files in the `configuration`, `templates`, `webapps`, and `webcontent` directories.

    Note: If you have modified `.ini` files, please contact Customer Support to determine whether the changes are supported in the new version of the software.
- Back up your content store database.

After your audit is complete, you can create an upgrade plan.

Guidelines when upgrading your operating system

You might want to consider the following guidelines before you upgrade to a later version of the operating system on the computers where IBM Cognos Analytics is installed:

- Check the IBM Software Product Compatibility Reports page (www.ibm.com/support/docview.wss?uid=swg27047186) to ensure that the IBM Cognos Analytics version supports the version of the operating system you are thinking of moving to.
- Ensure that the third-party software that is used by IBM Cognos Analytics is supported on the proposed operating system version. Third-party software would include components, such as database and database drivers, application servers, web servers, and browsers.
- Determine whether you must recompile IBM Cognos Analytics SDK applications.
- Determine whether you must re-create web deployments, which include web archive (.war) files and enterprise archive (.ear) files.

Install and configure a new version of the product

Install the new version of the product to a new location. The location can be on the same computer as your existing version of the product or on another computer.

Installing to a new location allows you to maintain your existing version of the product and run it in addition to the new version of the product. This can help you test your new version without affecting your existing version. You can compare the configuration settings between version and compare the appearance and functionality of the reports in both environments to ensure equivalency.

Running multiple versions or instances of IBM Cognos Analytics on the same computer
To have multiple versions or instances of IBM Cognos Analytics on the same computer, you must change the configuration to ensure that the versions do not share port numbers or other resources.

Required configuration changes for running multiple versions on the same computer

To run multiple versions of IBM Cognos Analytics on the same computer, ensure that each installation is distinct. The versions or instances must be installed in different directories. The configuration settings for each version must use different settings for the following configuration properties.

Ports and URI settings

If you are using the default application server, you must use different port numbers than 9300 to avoid port conflicts. IBM Cognos Analytics reserves a range of port number, so you must ensure that you use an offset of at least 100 for the port number. For example, if you are using the default port number, 9300, for one instance of IBM Cognos Analytics. For a second installation on the same computer, you must change the port number to at least 9400. Do not use the same port numbers for both installations.

Change the following ports.

- Dispatcher URIs for gateway
- External dispatcher URI
- Internal dispatcher URI
- Dispatcher URI for external applications
- Content Manager URIs
- Local log server port number

If you are installing the product on an application server other than the one provided with IBM Cognos Analytics, ensure that you install the new version to a new application server profile or a separate instance than your existing version.

Content store
Use a different content store or schema for each installation. You cannot revert the content after it is upgraded. You can use a restored copy of your existing content store as the content store for the newer version of IBM Cognos Analytics. The newer version of the product upgrades the content store when you start the services.

Optional web server virtual directories

To view static content for IBM Cognos Analytics, the virtual directories for the web server must be different for each version. Ensure that you update the Gateway URI in Cognos Configuration to reflect the names of the virtual directories.

For example, the default virtual directory is `http://`*`servername`*`/ibmcognos`. If you have two gateways that are installed on the same computer, you must change the `ibmcognos` virtual directory for one of the gateways.

Application pools (Microsoft IIS web server)
If you use `cognosisap.dll`, each gateway must use a separate application pool.

User account that starts the service (optional)

Changing the user account might be helpful when you are troubleshooting. For example, you can troubleshoot Java™ processes by owner.

Configuration settings that are the same for multiple versions on the same server

Multiple instances or versions of IBM Cognos Analytics running on the same computer use the same resources, such as memory, network, and disk space.

Multiple versions of IBM Cognos can use the same authentication source for both versions. You can configure identical properties for the namespace.

Customized configuration files

If you manually edited any configuration files, you must reapply the changes. Keep a record of any customizations to ensure that they can be reapplied after you upgrade. Also, back up these files so that the original version can be restored if necessary.

The IBM Cognos Analytics presentation service supports automatic upgrade of some `system.xml` files. If you made many customization changes to `system.xml` files, you can use this automatic upgrade feature instead of reapplying the changes manually after you upgrade. By replacing the `system.xml` files with files from your earlier version of the product, the files can be upgraded by the new version of the product. The automatic upgrade is applied when you start the IBM Cognos service.

The `system.xml` files for which automatic upgrade is supported are in the following directories:

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

Configuring a second instance of IBM Cognos Analytics on one computer

To have more than one instance of IBM Cognos Analytics on one computer, you must configure each instance with unique values for ports, the web server virtual directory, and content store database.

Before you begin

For the new version of the product, you require a new content store. If you are upgrading your entire content store, create a content store from a backup of your existing content store. If you are moving your content with deployment archives you can create a blank content store database.

Ensure that you have your new content store database in place before you configure the new version of the product.

Important: If you are connecting to a backup of your content store, the first time you start your IBM Cognos services, you are prompted to upgrade your reports. Upgrading your reports can take a long time, and it is better to upgrade them after you have the new version running. You can upgrade your reports afterwards using IBM Cognos Administration.

Procedure

1. For the new instance of IBM Cognos Analytics, start IBM Cognos Configuration.
2. In the **Explorer** window, click **Environment**.
3. Ensure that the port numbers for the following settings do not conflict with your other instance or version of IBM Cognos Analytics:

   - **Dispatcher URIs for gateway**
   - **External dispatcher URI**
   - **Internal dispatcher URI**
   - **Dispatcher URI for external applications**

- **Content Manager URIs**

4. Ensure that the **Gateway URI** uses a different virtual directory or alias than your other instance or version of IBM Cognos Analytics.
5. Click **Logging**, and ensure that the **Local log server port number** is unique.
6. If you are using Portal Services, update the `applications.xml` file location:
   - In the **Explorer** window, click **Environment** > **Portal Services**.
   - In the **Properties** window, ensure that the port number for the **Location of applications.xml** property matches the port number for the other URI properties.
7. In the **Explorer** window, under **Data Access** > **Content Manager**, ensure that you do not use the same content store that is used for your other instance or version of IBM Cognos Analytics.
8. Save the configuration, and start IBM Cognos Analytics.

Move your content to the new version of the product

There are two methods for moving your content. You can move the entire content store, or you can move content by creating deployment archives.

Move your entire content store

This method requires you to make a backup of your existing content store, and then restore the backup to a new content store. You then connect your new version of the product to the restored content store, and the product upgrades the content store to the new version.

This method maintains all of your security and user preferences, but it does require a new content store database.

When configuring security, ensure that you set the unique identifier to the same value as it was in the release that you are upgrading from, otherwise the security settings will be lost.

Run a consistency check on your content store before you upgrade to ensure that there are no inconsistencies. For more information, see the "Create a Content Store Maintenance Task" topic in the *IBM Cognos Business Intelligence Administration and Security Guide*.

Important: When you use this method, the first time you start your IBM Cognos services, you are prompted to upgrade your reports. Upgrading your reports can take a long time, and it is better to upgrade them after you have the new version running. Additionally, if you have Software Development Kit applications that create, modify, or save report specifications, do not select the option to upgrade your report specifications. You can upgrade your reports afterwards using IBM Cognos Administration.

Also, you must ensure you unregister any dispatchers from your previous version of the product. You can do so using IBM Cognos Administration after you have started the services.

Move content by creating deployment archives

You can move content by creating deployment archives.

This method lets you move specific content, but it can be time consuming for a large content store.

If you are changing content store database vendors, you must create deployments to move your content. For example, if you are changing your contents store from Microsoft SQL Server to IBM Db2, you must do so with deployment archives.

Considerations for both methods

There is no requirement to bring over the existing NC tables during an upgrade, as the system will resynchronize them. Given that there is a requirement for the queue tables to be empty, consider not using the existing NC tables when performing the upgrade.

NC tables must be completely empty before performing the upgrade. Run the appropriate `NC_DROP_`*`Database_Type`*`.sql` before you upgrade.

As part of the upgrade process, ensure that your applications work as expected in the new version. Sometimes, changes can introduce unexpected results. It is important to test your applications with the new version of the product before you move them to your production environment.

Upgrade your content store

IBM Cognos Analytics upgrades the content store database to the new version of the product when you start the services for the first time.

The process for upgrading your content store to the new version of the product includes the following steps:

1. Make a backup of your existing content store database.
2. Create a database from the backup.
3. Connect the new version of the product to the content store that you created from the backup in IBM Cognos Configuration.
4. Start your services.

   The content store is upgraded during the startup process.

   Tip: When restarting services manually, (if applicable) the `ApacheDS - cognos` service must be started before the `IBM Cognos` service.

This process lets you use the old and new versions of the product at the same time, where each version has its own content store.

When you use this method, the first time you start your IBM Cognos services, you are prompted to upgrade your reports. Upgrading your reports can take a long time, and it is better to upgrade them after you have the new version running. You can upgrade your reports with IBM Cognos Administration. Additionally, if you have Software Development Kit applications that create, modify, or save report specifications, do not select the option to upgrade your report specifications.

When you connect the new version of the product to the content store you created from the backup, the content store database is upgraded, and can no longer be used with your older version of the product.

Unregister previous version dispatchers from your content store

If you use a backup of your existing content store with a new version of the product, you must unregister the dispatchers from your previous version.

Procedure

1. From **Manage** > **Administration console**, open IBM Cognos Administration.
2. Click **Configuration**, and then click **Dispatchers and Services**.
3. Click **More** for the dispatchers belonging to your previous version.
4. Click **Unregister**, and then click **OK**.

   The dispatcher information is removed from the content store.

Moving your content with a deployment archive

To move specific content from your content store you can use deployment archives. Deployment archives are compressed files that you can then import into your new version of the product.

Important: If you have moved your content by restoring your existing content store, you do not need to move your content using deployment archives.

Moving your content with deployment archives involves the following steps:

1. Creating the archive.
2. Copying the archive to the new version of the product.
3. Importing the content.

Creating a deployment archive

Use the following task to create a deployment archive.

Procedure

1. In **IBM Cognos Administration**, on the **Configuration** tab, click **Content Administration**.
2. On the toolbar, click the **New Export** icon .
3. Enter **Name** for the archive.
4. Select the content you want to include in the archive:
   - To export specific folders and directory content, click **Select public folders and directory content**.
   - To export the entire content store, click **Select the entire content store**. If you select the entire content store, you can also select **Include user account information**.
5. Click **Next**.
6. If you clicked **Select the entire content store**, enter a password to be used when you import the content, and then click **OK**.
7. If you clicked **Select public folders and directory content**:
   a) On the **Select the Public folders content** panel, click **Add**.

   b) On the **Select entries** panel, in the **Available Entries** box, select the packages or folders that you want to export.

   You can browse the Public Folders hierarchy and choose the packages and folders that you want.

   Click the **Add** icon ➡ to move the selected items to the **Selected entries** box, and click **OK**.

   c) For each package and folder that you export, do the following, and then click **Next**:

   - If you want to make any changes to the package or folder in the target environment, click the **Edit** icon ✎, make your changes, and click **OK**.
   - To restrict access to the package or folder and its entries, select the check box in the **Disable after import** column. This is useful when you want to test the reports before you make them available in the target environment.
   - Under **Options**, select whether you want to include the report output versions, run history, and schedules and what to do with entries when there is a conflict.

   d) On the **Select the directory content** panel, select the options that you want, and click **Next**.

   e) On the **Specify the general options** panel, select the options that you want, and click **Next**.

   f) On the **Specify a deployment archive** panel, select an existing deployment archive from the list, or create one.

   If you are typing a new name for the deployment archive, do not use spaces in the name. If the name of the new deployment specification matches the name of an existing deployment archive, the existing deployment archive is overwritten.
8. Review the summary information and click **Next**.
9. Under **Actions**, select **Save and run once**.
10. On the **Run with options** panel, select **Now** and click **Run**.

Results

A deployment archive is created in the `deployment` directory where you installed IBM Cognos Analytics.

Copying the deployment archive to your new version

You must manually copy the deployment archives from the instance where they were created to your new instance.

Procedure

Copy the deployment archives you created from the *old_version_install_location*`/deployment` directory to the *new_version_install_location*`/deployment` directory.

Note: The `deployment` directory is configurable in IBM Cognos Configuration. By default, the location is *install_location*`/deployment`. If you are using a different location, ensure that you copy the deployment archives to the appropriate directory.

Including configuration objects when you import a deployment archive of the entire content store

You can include configuration objects when importing an entire content store. For example, you might want to import the configuration because you have a series of advanced settings for your services that you want from the source environment.

By default, configuration objects are excluded when you import an entire content store, even though they are included in the export. Configuration objects include dispatchers and configuration folders used to group dispatchers.

Procedure

1. In **IBM Cognos Administration**, on the **Configuration** tab, click **Dispatchers and Services**.
2. Click the dispatcher you want.
3. Next to **ContentManagerService**, click the set properties icon.
4. Click the **Settings** tab.
5. In the **Value** column, click **Edit**.
6. Select the **Override the settings acquired from the parent entry** check box.
7. In the **Parameter** column, type the following uppercase text:

   ```
   CM.DEPLOYMENTINCLUDECONFIGURATION
   ```
8. In the **Value** column, type `true`.
9. Click **OK** to finish.

Importing a deployment archive

To import the entries, you create an import deployment specification.

When you import, you select from entries that were exported. You can either accept the default options set during the export, or change them. You can select options that were included in the deployment archive during the export.

If you do a partial deployment of specific public folders and directory content, the import wizard shows whether packages and folders exist in the target environment and the date and time that they were last modified. You can use this information to help you decide how to resolve conflicts. When you redeploy, the wizard also shows whether the packages and folders were in the original deployment.

Before you begin

Ensure that you have copied the deployment archive to the *install_location*`/deployment` directory for your new version of the product.

Procedure

1. For your new version of the product, in **IBM Cognos Administration**, on the **Configuration** tab, click **Content Administration**.
2. On the toolbar, click the new import icon.

3. In the **Deployment archive** box, select the deployment archive that you want to import, and click **Next**.
4. If your deployment archive is of your entire content store, type the password entered during the export, and click **OK**.
5. Type a name for the import and select the folder where you want to save it, and then click **Next**.
6. Select the content that you want to include in the import, select the options, and click **Next**.

   Tip: Click the edit icon next to the package if you want to change the target location for the imported content.
7. On the **Specify the general options** panel, select the options that you want, and click **Next**.
8. Review the summary information, and click **Next**.
9. Under **Actions**, select **Save and run once**, and click **Finish**.
10. On the **Run with options** panel, do the following:

    a) Select **Upgrade all report specifications to the latest version** if you want to upgrade the report specifications during the import. You can also perform this task after you import the content.

    b) Click **Run**.

Use Lifecycle Manager to compare reports between your versions of the product

Lifecycle Manager lets you verify your upgraded content by comparing reports in your old environment with the reports in your new version of the product.

For more information, see the IBM Cognos Lifecycle Manager documentation.

Upgrade your report specifications

Report specifications will have changed from one version of IBM Cognos Analytics to another. You must upgrade any report specifications created in previous versions of the product.

If you are upgrading from a backup of your existing content store, you should upgrade the report specifications after you have started the services.

If you are moving content to a new version using deployment archives, you can choose to upgrade the import specifications during the import.

If you moved your content using deployment archive you may have selected the option to upgrade your report specifications. If you upgraded the report specifications during the import, you do not have to do it again.

Before you begin

Important: Do not upgrade your report specifications if you have Software Development Kit applications that create, modify, or save report specifications. You must first update your Software Development Kit applications to comply with the IBM Cognos report specifications schema. Otherwise, your Software Development Kit applications may not be able to access the upgraded report specifications. For information about upgrading report specifications, see the *IBM Cognos Software Development Kit Developer Guide*.

Procedure

1. Open **IBM Cognos Administration**.
2. On the **Configuration** tab, click **Content Administration**.
3. Click the arrow on the new content maintenance button on the toolbar, and then click **New Report Upgrade**
4. Type a name for the upgrade task and, if you want, a description and screen tip. Click **Next**.
5. Select the packages and locations for the report specification you want to upgrade. Click **Next**.

If you upgrade report specifications by package, all reports in the content store that are based on the model in the package will be upgraded. If you upgrade report specifications by folder, all reports in the folder will be upgraded.

6. Choose one of the following:
    - **Save and run once** opens the run with options page.
    - **Save and schedule** opens the scheduling tool.
    - **Save only** allows you to save the upgrade so that you can run it at a later time.

Chapter 3. Configuring server components

You can install all IBM Cognos Analytics components on one computer, on multiple servers for a distributed installation, or you can expand an existing single computer installation to another server to improve performance.

The following options are available when installing IBM Cognos Analytics from the installation wizard.

- Use the **Easy install** option to help you get up and running with IBM Cognos Analytics in no time, without any additional configuration and without the need to install any supporting software.

  Important: Easy install is available for Windows OS only. If you are upgrading an **Easy install** (that is, installing over the top of an existing installation), shut down all services manually first, including Informix and ApacheDS services.

  With this install option, you get the following with all the configuration already in place:

  - A full version of IBM Cognos Analytics software with all the new capabilities.
  - Informix 12.10 installed and configured for use as content store database.
  - Apache Directory Server to create and manage users.
- Use the **Custom** option for full flexibility to pick and choose the IBM Cognos Analytics components that you want to install. Maybe you want to customize or integrate IBM Cognos Analytics with third-party software? This is the option you would want to select.

If you plan to install two or more components on the same computer, install them in the same installation location to avoid conflicts among ports and other default settings.

When performing a custom install, the server components are collected into the following tiers:

- Content repository (Content Manager)
- Application services
- Gateway tier

You can install each component on a separate computer, or on the same computer. You must install the gateway on a computer that is also running a web server.

Stopping services sequence

If you need to stop services in a distributed environment, the sequence is important. Stop the IBM Cognos service for Application Tier Components first, followed by the standby Content Manager, and then the active Content Manager.

It is important to also stop the following:

- Applications that are related to the IBM Cognos service, such as Framework Manager, Cognos Transformer, or IBM Cognos Administration.
- Any Software Development Kit applications that are running.

Upgrading your installation

If you are upgrading from a previous release of IBM Cognos products, see Chapter 2, “Upgrading Cognos Analytics,” on page 17.

If you are upgrading from an earlier version of IBM Cognos Analytics, all the distributed components must be the same version of IBM Cognos Analytics. If you install IBM Cognos Analytics on additional or alternate hosts, you must update location-specific properties in IBM Cognos Configuration.

64-bit installations

The IBM Cognos Analytics gateway provides 32-bit libraries, whether you install on a 64-bit server or a 32-bit server. Some Web servers, such as Apache Web Server, cannot load a 32-bit compiled library in a 64-bit compiled server. In that situation, install the 32-bit version of the IBM Cognos gateway on a 32-bit Web server.

The report server component, included with the Application Tier Components, is provided in both 32- and 64-bit versions. Selecting which version you use is done using IBM Cognos Configuration after installation. By default, the report server component is set to use the 32-bit mode, even on a 64-bit computer. The 32-bit mode allows you to run all reports, whereas the 64-bit mode allows you to run only reports created for dynamic query mode.

If you are upgrading IBM Cognos Analytics in an environment that includes earlier versions of other IBM Cognos Analytics products, such as IBM Cognos Business Intelligence Controller Version 8.x, IBM Cognos Analytics Planning Version 8.x, or IBM Cognos Business Intelligence Analysis *for Microsoft Excel* Version 8.x, install the new version of IBM Cognos Analytics in a separate location from the other IBM Cognos Analytics product and configure the new version of IBM Cognos Analytics to operate independently of that product. After you upgrade the other product to a compatible version with IBM Cognos Analytics, you can then configure the two products to operate together.

Windows installations

For Microsoft Windows operating system installations, ensure that you have administrator privileges for the Windows computer you are installing on. Also ensure that your computer has a TEMP system variable that points to the directory where you want to store temporary files. During installation, files from the disk are temporarily copied to this directory.

UNIX installations

For UNIX operating system installations, you can install server components using a graphical user interface or by running a silent installation. To run graphical-mode installation, the console attached to your UNIX computer must support a Java-based graphical user interface.

Also, IBM Cognos Analytics uses 755 permissions. This affects only the installation directories. It does not affect the file permissions within the directories.

Printer requirements

To ensure that reports print properly on Windows, Adobe Reader requires that you configure at least one printer on the operating system where Application Tier Components are installed. All reports, regardless of the print format that you choose, are sent as temporary PDF files to Adobe Reader for printing.

Uninstallation

For uninstallation instructions, see Chapter 10, “Uninstalling IBM Cognos Analytics,” on page 211.

Installation sequence for server components

In a distributed installation, the sequence in which you configure components is important. Configure and start the services in at least one location where you installed Content Manager before you configure other server components.

You must configure the gateway component last so that cryptographic keys are shared and secure communication can take place among the three components. The server specified for the external dispatcher URI property on the gateway computer must be the last server component that you start.

The following diagram shows the sequence of the installation process for distributed components. After planning and preparing your environment, install and configure Content Manager components, then Application Tier Components and then gateways. After server components are installed, you install and configure Framework Manager.

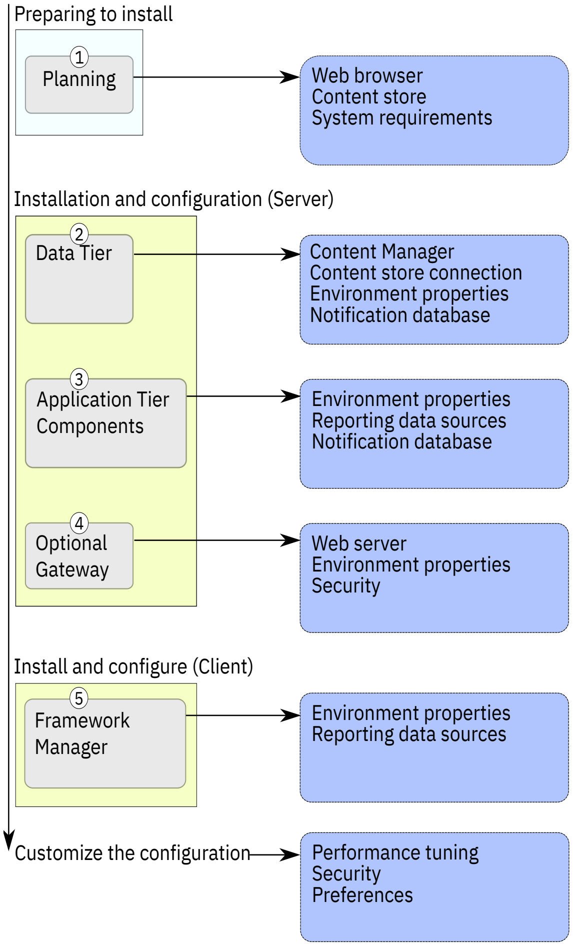


Figure 7: Distributed installation process workflow

Recommendation - Install and Configure the Basic Installation for Distributed Installations

When you do a distributed installation, there are many different installation and configuration options that you can do to customize IBM Cognos Analytics so that it fits into your corporate infrastructure.

Do a basic installation first, which involves installing one or more instances of each of the required server components: data tier (Content Manager), application tier components, and gateway tier. Perform only the required configuration tasks, such as configuring distributed components to communicate with each other, to get your distributed environment running before you customize your settings.

Later, you can add optional components and customize your configuration settings to better suit your business intelligence needs.

The sequence in which you configure computers is important. You must configure and then start the services on at least one computer where you installed Content Manager before you configure other server components or Framework Manager. For more information, see "Installation sequence for server components" on page 34.

The simplest and quickest way to get IBM Cognos Analytics running in your environment is ensuring that a basic installation works in your environment.

Installation modes

For a complete installation, you must install components on your server and then configure them to work in your environment.

Interactive mode

Typically, you run the IBM Cognos installation and configuration programs in interactive mode. This means that the install wizard prompts you to provide information, and the configuration tool enables you to change default settings. The install wizard is `ca_srv_<platform>_<build>.exe` (Windows), or `ca_srv_<platform>_<build>.bin` (UNIX, Linux).

Silent mode

You can automate the installation of components using response files and running the installation program in silent mode.

You can automate the configuration of components by exporting the configuration settings from one computer to another as long as the installed components are the same. Run IBM Cognos Configuration in interactive mode the first time.

The other option is to edit the cogstartup.xml file, using settings that apply to your environment, and then running the configuration tool in silent mode.

Interactive mode on UNIX systems

Unless you intend to complete a silent-mode installation, install the software from an X Window System workstation, an X terminal, or a PC or other system with X server software installed.

To run an interactive-mode installation, the console attached to your computer must support a Java-based graphical user interface.

Installing server components on UNIX or Linux operating systems

Use the installation wizard to select the server components that you want to install, and the location on your computer where you want to install them.

Before you begin

Go to the IBM Software Product Compatibility Reports page (www.ibm.com/support/docview.wss?uid=swg27047186) to verify that the required patches are installed on your computer.

Procedure

1. Set the JAVA_HOME environment variable to point to the installation location of your Java Runtime Environment (JRE), such as `/`*`directory`*`/java/`*`java_version`*`/jre`.

   IBM Cognos Analytics requires a JVM, such as the one that is provided by IBM, to run on Linux operating system.
2. Go to the location where the installation files were downloaded and extracted.

   Tip: Use new versions of file compression software to extract the files. Older versions of such software might not extract the files.
3. To start the installation wizard, go to the operating system directory, and type the following command:

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

   Where *<build>* is the build number, and *<platform>* is win (Windows), i386 (Linux i386), ppcle (Linux pl E), ppc (Linux Power PC), s390x (Linux z), aix (AIX), and zos (z/OS).

Tip: When you use the `./ca_srv_<platform>_<build>.bin` command with XWindows, Japanese characters in messages and log files might be corrupted. When installing in Japanese on UNIX or Linux, first set environment variables LANG=C and LC_ALL=C (where C is the language code), and then start the installation wizard.

If you do not use XWindows, run an unattended installation. For more information, see the Installation Guide.

4. Follow the directions in the installation wizard to copy the files to your computer.

   Install to a directory that contains only ASCII characters in the path name. Some UNIX and Linux web servers do not support non-ASCII characters in directory names.

5. In the **Finish** page of the installation wizard, you can click **View** to access the log files. Do not configure IBM Cognos Analytics immediately because you must do other tasks first to ensure that your environment is properly set up.
6. Append the `install_location/bin` directory to the appropriate library path environment variable.

   - For Linux, LD_LIBRARY_PATH
   - For AIX®, LIBPATH

What to do next

You can configure IBM Cognos Analytics by using IBM Cognos Configuration. Type `cogconfig.sh` in the `install_location/bin` directory to start Cognos Configuration.

Installing server components on Windows operating systems

Use the installation wizard to select the server components that you want to install, and the location on your computer where you want to install them.

For Windows computers, the default installation location uses the **Program Files** directory. If you install to this location, ensure that you run IBM Cognos Configuration as an administrator. Alternatively, you can install the product to a directory outside of **Program Files**, such as `C:\IBM\cognos\analytics`.

The installation requires at least 5 GB in the temporary directory. The temporary directory is set with the environment variable TMP.

Procedure

1. Go to the location where the installation files were downloaded and extracted, and double-click `ca_srv_<platform>_<build>.exe`.

   Tip: Use new versions of file compression software to extract the files. Older versions of such software might not extract the files.

2. Select the language to use for the installation.

   The language that you select determines the language of the user interface. All supported languages are installed. You can change the user interface to any of the installed languages after installation.

3. Follow the directions in the installation wizard to copy the files to your computer.

   You can use one of the following installation options:

   - Use the **Easy install** option to install components to a single computer, install an instance of Informix database for the content store, and configure the system.

     Important: If you are upgrading (that is, installing over the top of an existing installation) an **Easy install**, manually shut down all services first, including Informix and ApacheDS services.

   - Use the **Custom** option for a distributed installationto install components on multiple servers.

   Install IBM Cognos Analytics components in a directory that contains only ASCII characters in the path name. Some Windows web servers do not support non-ASCII characters in directory names.

4. If this is the first installation, select the **First install** option. To expand the capacity of a running installation, select the **Connect and install** option. You are prompted for the components to install, and the URL and credentials for the running system. The namespace and credentials must be for a system administrator.

   - You can find the URL value for the running installation in IBM Cognos Configuration, in the **Environment** > **Dispatcher Settings** category. The URL value that you need is **External Dispatcher URI**.
   - You can find the namespace for the running installation in IBM Cognos Configuration, in the **Security** > **Authentication** category.

Installing and configuring Content Manager for the content repository

You can install more than one Content Manager to ensure failover, and you can install Content Manager in a separate location than other components to enhance performance.

The Content Manager computers must know the location of the content store, the location of other Content Manager components, and the database that is used for notification.

In a distributed installation, at least one of the computers where you install Content Manager must be configured, running and accessible before you configure other computers in your IBM Cognos environment. This ensures that the certificate authority service, which is installed with Content Manager, is available to issue certificates to other computers.

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

Permissions

You can install using either root or non-root authority.

Also, IBM Cognos Analytics respects the file mode creation mask (umask) of the account running the installation program. This affects only the installation directories. It does not affect the file permissions within the directories. However, run-time generated files, such as logs, respect the mask. We recommend umask 022 on the installation directory.

Rules for configuring

In an installation where you have more than one Content Manager components, or where Content Manager is located in a separate location, at least one of the one Content Manager must be configured, running and accessible before you configure other components in your environment. This ensures that the certificate authority service, which is installed with Content Manager, is available to issue certificates to other IBM Cognos computers.

For information about the sequence of the installation process for distributed components, see "Installation sequence for server components" on page 34.

Rules for active Content Manager

If you are installing multiple Content Manager components, the first Content Manager computer that you start becomes the default active Content Manager. You can designate another Content Manager computer as default active, using IBM Cognos Administration.

The standby Content Manager computers are for failover protection. If the active Content Manager computer is not available because of a software or hardware failure, a standby Content Manager computer becomes active and requests are directed to it.

When the active Content Manager fails, unsaved session data is lost. When another Content Manager becomes active, users may be prompted to log on.

For information about activating a Content Manager service, see the *Administration and Security Guide*. For information about active and standby Content Manager components, see "Active and Standby Content Manager Components" on page 39.

In installations with multiple Content Managers, configure IBM Cognos Analytics to use compiled gateways instead of the default CGI gateway. For example, use Apache Module for Apache Server or for IBM HTTP Server, or use ISAPI for IIS. Otherwise, performance may be affected after failover.

Upgrading

If you are upgrading from ReportNet or an earlier version of IBM Cognos Business Intelligence, you can use the existing configuration data. However, some features in IBM Cognos Analytics are new and may require configuration.

PowerCubes

If you plan to install IBM Cognos Transformer and you will be using PowerCubes that are secured against an IBM Cognos Series 7 namespace, you must install Content Manager on a computer that supports IBM Cognos Series 7.

Active and Standby Content Manager Components

You can install any number of installations of Content Manager, although only one is active at any time. The other installations each act as a standby Content Manager.

The standby Content Manager components are for failover protection. If the active Content Manager is not available because of a software or hardware failure, a standby Content Manager becomes active and requests are directed to it.

When the active Content Manager fails, unsaved session data is lost. When another Content Manager becomes active, users may be prompted to log on.

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

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

If you are installing multiple Content Managers, you **must** ensure that the system clocks on the Content Manager computers are synchronized for successful failover between Content Managers.

Installing Content Manager on UNIX or Linux operating systems

Use the following procedure to install Content Manager on a UNIX or Linux operating system.

Before you begin

Go to the IBM Software Product Compatibility Reports page (www.ibm.com/support/docview.wss?uid=swg27047186) to verify that the required patches are installed on your computer.

Procedure

1. Set the JAVA_HOME environment variable to point to the installation location of your Java Runtime Environment (JRE), such as `/`*`directory`*`/java/`*`java_version`*`/jre`.

IBM Cognos Analytics requires a JVM, such as the one that is provided by IBM, to run on Linux operating system.

2. Go to the location where the installation files were downloaded and extracted.

   Tip: Use new versions of file compression software to extract the files. Older versions of such software might not extract the files.

3. To start the installation wizard, go to the operating system directory, and type `./ca_srv_<platform>_<build>.bin`

   Tip: When you use the `ca_srv_<platform>_<build>.bin` command with XWindows, Japanese characters in messages and log files may be corrupted. When installing in Japanese on UNIX or Linux, first set environment variables LANG=C and LC_ALL=C (where C is the language code), and then start the installation wizard.

   If you do not use XWindows, run an unattended installation. For more information, see Unattended installation, uninstallation, and configuration.

4. Follow the directions in the installation wizard to copy the files to your computer and implement a basic configuration.

   - When selecting the directory, consider the following:

     Install Content Manager in a directory that contains only ASCII characters in the path name. Some UNIX and Linux Web servers do not support non-ASCII characters in directory names.

     If you are installing IBM Cognos Analytics on a computer that has an earlier version of IBM Cognos Analytics and you want to keep the earlier version, you must install the new version in a different directory.

   - When selecting components, clear all components except for **Content repository**.

5. Click **Finish**.

6. Append the *`install_location`*`/bin` directory to the appropriate library path environment variable.

   - For Linux, LD_LIBRARY_PATH
   - For AIX, LIBPATH

What to do next

Do not configure IBM Cognos Analytics immediately because you must do other tasks first to ensure that your environment is properly set up.

You can later configure IBM Cognos Analytics using IBM Cognos Configuration by typing `cogconfig.sh` in the *`install_location`*`/bin` directory.

Installing Content Manager on Windows operating systems

Use the following procedure to install Content Manager on a Microsoft Windows operating system.

For Windows computers, the default installation location uses the **Program Files** directory. If you install to this location, ensure that you run IBM Cognos Configuration as an administrator. Alternatively, you can install the product to a directory outside of **Program Files**, such as `C:\IBM\cognos\analytics`.

The installation requires at least 5 GB in the temporary directory. The temporary directory is set with the environment variable TMP.

Before you begin

Go to the IBM Software Product Compatibility Reports page (www.ibm.com/support/docview.wss?uid=swg27047186) to verify that the required patches are installed on your computer.

Procedure

1. Go to the location where the installation files were downloaded and extracted, and double-click `ca_srv_<platform>_<build>.exe`.

Tip: Use new versions of file compression software to extract the files. Older versions of such software might not extract the files.

2. Select the language to use for the installation.

   The language that you select determines the language of the user interface. All supported languages are installed. You can change the user interface to any of the installed languages after installation.
3. Select the **Custom** installation option, and follow the directions in the installation wizard to copy the files to your computer.
   - When selecting the directory, consider the following:

     Install Content Manager in a directory that contains only ASCII characters in the path name. Some Microsoft Windows operating system Web servers do not support non-ASCII characters in directory names.

     If you are installing IBM Cognos Analytics on a computer that has an earlier version of IBM Cognos Analytics and you want to keep the earlier version, you must install IBM Cognos Analytics in a different directory.
   - When selecting components, clear all components except **Content repository** from the **Custom** install option.
4. Click **Finish**.

What to do next

If you start IBM Cognos Configuration from the installation wizard, ensure that you follow the additional tasks in this section to ensure that your environment is properly set up before you start the services.

You can start IBM Cognos Configuration using the **IBM Cognos Configuration** shortcut from the **Start** menu.

Set up database connectivity for the content store database

You may have to install database client software, or Java Database Connectivity (JDBC) drivers, or both, on each computer where you install Content Manager. Doing this allows Content Manager to access the content store database.

Set up database connectivity for a Microsoft SQL Server content store

11.0.5

The Microsoft JDBC driver replaces the JSQLConnect driver for SQL Server. From version 11.0.5 forward you must download, from Microsoft, and put the new type 4 driver in the `*install_location*/drivers` folder.

The driver JAR file `sqljdbc42.jar` is the file you need to support the Java version that is shipped with IBM Cognos Analytics.

Important: For single sign-on (SSO) and Windows authentication, you need to put `sqljdbc_auth.dll` in the `bin64` directory. Windows authentication is a single sign-on setup. The selection in Configuration Manager for the Content Manager is called **Microsoft SQL Server database (Windows Authentication)**.

Set up database connectivity for an IBM Db2 content store

This procedure describes how to set up database connectivity for a Db2content store. You must perform this procedure on each computer where you install Content Manager.

You must use a type 4 Java Database Connectivity (JDBC) driver to connect to your content store.

The type 4 driver is considered an independent product. It does not require the Db2 client to be installed.

Procedure

Copy the following files from *DB2_installation*`\sqllib\java` directory to the *install_location* `\drivers` directory:

- The universal driver file, `db2jcc4.jar`
- The license file:

  For Db2 on Linux, UNIX, or Windows operating systems, use `db2jcc_license_cu.jar`.

  For Db2 on z/OS®, use `db2jcc_license_cisuz.jar`.

  If you are connecting to Db2 on z/OS, use the driver version from Linux, UNIX, or Windows version 9.1 fix pack 5 or version 9.5 fix pack 2.

  Tip: To check the driver version, run the following command:

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

Generating a script file to create a database for an IBM Db2 content store

You can generate a script file to automatically create the content store in Db2 on all platforms. The script file is a DDL file.

Procedure

1. Start **IBM Cognos Configuration**.
2. In the **Explorer** window, under **Data Access** > **Content Manager**, click **Content Store**.

   The default configuration is for an Db2 database. Ensure that the **Type** is **DB2 database**.
3. In the **Database server and port number** field, enter the name of your computer and port number on which Db2 is running.
   For example, `localhost:50000`. Where, 50000 is the default port number that is used by Db2. If you are using a different port number, ensure you use that value.
4. Click the **Value** field next to the **User ID and password** property and then click the edit icon. Type the appropriate values and click **OK**.
5. In the **Properties** window, for the **Database name** property, type the name for your content store database.

   Important: Do not use a name longer than eight characters and use only letters, numbers, underscores, and hyphens in the name.
6. Right-click **Content Store**, and click **Generate DDL**.
7. Click **Details** to record the location of the generated DDL file.

   The DDL file named `createDB.sql` is created. The script is created in the `*install_location*\configuration\schemas\content\db2` directory.

What to do next

Use this script to create a database in Db2. For more information about using a DDL file, see your Db2 documentation.

If you use the Db2 command-line interface, you can run the script by entering the following command:

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

Creating tablespaces for a content store on IBM Db2 for z/OS

A database administrator must run scripts to create a set of tablespaces required for the content store database. Modify the scripts to replace the placeholder parameters with ones that are appropriate for your environment.

By default, the content store is used for notifications, human tasks, and annotations. You can create separate databases for each.

About this task

Ensure that you use the naming conventions for Db2 on z/OS. For example, all names of parameters must start with a letter and the length must not exceed eight characters. There are two exceptions to the character length limit:

- CMSCRIPT_CS_ID is no more than 2 characters.
- CMSCRIPT_TABLESPACE is no more than 6 characters.

The reason for the exception is that when the two parameters are concatenated the character length can be no more than 8.

For more information, see the IBM Db2® for z/OS Knowledge Center (http://www.ibm.com/support/knowledgecenter/SSEPEK/db2z_prodhome.html).

Procedure

1. Connect to the database as a user that has privileges to create and drop tablespaces and to allow execution of SQL statements.
2. Go to the directory that contains the scripts:

   install_location/configuration/schemas/content/db2zOS
3. Make a backup copy of the `tablespace_db2zOS.sql` script file and save the file to another location.
4. Open the original `tablespace_db2zOS.sql` script file.
   a) Add a connection statement to the beginning of the script.

      For example,

      ```
      connect to databasename;
      ```
   b) Use the following table to help you to replace the generic parameters with ones appropriate for your environment.

      Not all of the parameters listed are in the script, but some might be added in the future.

Table 1: Parameter names and description for the content store tablespace script

Parameter name	**Description**
CMSCRIPT_STOGROUP	Specifies the name of the storage group.
CMSCRIPT_DATABASE	Specifies the name of the content store database.
CMSCRIPT_CS_ID	Specifies the subsystem identification for the content store database. The ID must not be longer than 2 characters.
CMSCRIPT_TABLESPACE	Specifies the name of the tablespace that contains all of the base tables in the content store. Auxiliary tables are not included. The name cannot be longer than 6 characters.

Table 1: Parameter names and description for the content store tablespace script (continued)

Parameter name	Description
CMSCRIPT_LARGE_BP	Specifies the name of the large buffer pool allocated for especially large objects. This bufferpool is the 32 KB buffer pool that was created when the database administrator created the content store database on the z/OS system.
CMSCRIPT_REGULAR_BP	Specifies the name of the regular size buffer pool allocated for regular and large objects. This bufferpool is the 16 KB buffer pool that was created when the database administrator created the content store database on the z/OS system.
CMSCRIPT_USERNAME	Specifies the user account that accesses the content store database.

5. Save and run the script.

   For example, if you set up your `clp.properties` file and your Db2 alias in your profile or `tcshrc` script file, type the following command to run the script:

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

6. Grant the IBM Cognos user rights to the tablespaces that were created when you ran the `tablespace_db2zOS.sql` file script:

   a) Make a copy of the `rightsGrant_db2zOS.sql` script file and store it in another location.

   b) In the remote access tool, open the original `rightsGrant_db2zOS.sql` script file and replace the placeholder parameters with values that are appropriate for your environment.

      Ensure that you use the same values that you used when you allocated resources to the buffer pools and user account

      .

   c) Add a connection statement to the beginning of the script.

      For example,

      ```
      connect to databasename user username using password;
      ```

   d) Save and then run the script.

      For example,

      ```
      db2 -tvf rightsGrant_db2zOS.sql
      ```

7. To create the notification tablespaces, go to the *`install_location`*`/configuration/schemas/delivery/zosdb2` directory.

   a) Make a backup copy of the `NC_TABLESPACES.sql` script file and save the file to another location.

   b) Open the original `NC_TABLESPACES.sql` script file and use the following table to help you to replace the placeholder parameters with ones appropriate for your environment.

Table 2: Tablespace parameter names and descriptions for the Db2 notification database on z/OS

Parameter Name	Description
NCCOG	Specifies the name of the notification database.
DSN8G810	Specifies the name of the storage group.
BP32K	Specifies the name of the buffer pool.

Not all of the parameters listed are in the script, but might be added in the future.

c) Save and run the script.

For example,

```
db2 -tvf NC_TABLESPACES.sql
```

d) Open the `NC_CREATE_DB2.sql` script file and replace the NCCOG placeholder parameter with the name of the notification database.

e) Save the script.

The Job and Scheduling Monitor services will automatically run the script. However, you may choose to run it yourself.

8. To create the human tasks tablespaces, go to the *`install_location`*`/configuration/schemas/hts/zosdb2` directory.

a) Make a backup copy of the `HTS_tablespaces.sql` script file and save the file to another location.

b) Open the original `HTS_TABLESPACES.sql` script file and use the following table to help you to replace the generic parameters with ones appropriate for your environment.

Table 3: Tablespace parameter names and descriptions for human tasks on Db2 for z/OS

Parameter Name	Description
NCCOG	Specifies the name of the database.
DSN8G810	Specifies the name of the storage group.
BP32K	Specifies name of the 32 k buffer pool.

See the script for a complete list of the parameters required.

c) Save and run the script.

d) Open the `HTS2_CREATE_Db2zos.sql` script file and use the following table to help you to replace the generic parameters with ones appropriate for your environment.

Table 4: Tablespace parameter names and descriptions for human tasks on Db2 for z/OS

Parameter Name	Description
NCCOG	The name of the database.

See the script for a complete list of the parameters required.

e) Save and run the script.

9. To create the annotations tablespaces, go to the *`install_location`*`/configuration/schemas/ans/zosdb2` directory.

a) Make a backup copy of the ANN_TABLESPACES.sql script file and save the file to another location.

b) Open the original ANN_TABLESPACES.sql script file and use the following table to help you to replace the generic parameters with ones appropriate for your environment.

Table 5: Tablespace parameter names and descriptions for annotations on Db2 for z/OS

Parameter Name	**Description**
NCCOG	The name of the database.
DSN8G810	The name of the storage group.
BP32K	The name of the 32 k buffer pool.

See the script for a complete list of the parameters required.

c) Save and run the script.

d) Open the ANS2_CREATE_Db2zos.sql script file and use the following table to help you to replace the generic parameters with ones appropriate for your environment.

Table 6: Tablespace parameter names and descriptions for annotations on Db2 for z/OS

Parameter Name	**Description**
NCCOG	The name of the database.

See the script for a complete list of the parameters required.

e) Save and run the script.

Set up database connectivity for an Oracle content store

This procedure describes how to set up database connectivity for an Oracle content store. You must perform this procedure on each computer where you install Content Manager.

Procedure

1. On the computer where the Oracle client is installed, go to the *ORACLE_HOME*/jdbc/lib directory.
2. Copy the correct library file for your version of the Oracle client to the *install_location*\drivers directory on the computer where Content Manager is installed and where notification is sent to an Oracle database.

   If you are using Oracle 12c, you must have ojdbc7.jar.

   If you are using Oracle 11g, you must have ojdbc5.jar.

   The files are available from an Oracle client or server install, and can also be downloaded from the Oracle technology Web site.

Set up database connectivity for an Informix content store

This procedure describes how to set up database connectivity for an Informix content store. You must perform this procedure on each computer where you install Content Manager.

Procedure

1. On the computer where Informix® is installed, go to the *Informix_location*/sqllib/java directory.
2. Copy the following files to the *install_location*\drivers directory on every computer where Content Manager is installed.

   - the universal driver file, db2jcc4.jar

- the license file, `db2jcc4_license_cisuz.jar`

Critical configuration actions to take first!

These configuration actions are critical to the success of your installation. Take these actions after you install the components.

Ensure that JDBC drivers are in the correct location

For the IBM Cognos Analytics 11.1.x release, the JDBC drivers must be copied to the *install_location*\drivers directory.

The use of *install_location*\webapps\p2pd\WEB-INF\lib for JDBC drivers is not supported.

Replace the JSQL driver for Microsoft SQL Server with the Microsoft JDBC driver

Starting with IBM Cognos Analytics version 11.0.5, the JSQL driver for Microsoft SQL Server has been replaced with the Microsoft JDBC driver. You must download and place the required JAR file in the *install_location*\drivers directory. For more information, see Set up for a Microsoft SQL Server content store.

Specify the Configuration Group property

If you used the **Custom** installation to install IBM Cognos Analytics, open IBM Cognos Configuration and set the **Configuration Group** property. For more information, see Managing the Configuration Group.

Enable or disable web-based modeling

By default, JDBC data source connections that were created in IBM Cognos Administration are not exposed in the **Manage** > **Data servers** administration interface for use in data modules. If you want to use your existing (upgraded) data source connections to create data modules, you must enable web-based modeling on those connections.

Some data sources are inappropriate to use as sources for creating data modules. In this case, you can prohibit the use of web-based modeling on the data source connections.

To enable or disable web-based modeling for your data source connections, perform the following steps:

1. In IBM Cognos Analytics, go to **Manage** > **Administration console**.
2. In IBM Cognos Administration, on the **Configuration** tab, select **Data source connections**.
3. Locate the data source, and click its **Set properties** action.
4. On the **Connection** tab, select or clear the **Allow web-based modeling** check box.

Start IBM Cognos Configuration

Use IBM Cognos Configuration to configure IBM Cognos Analytics components and to start and stop IBM Cognos services.

Before you begin

Before starting IBM Cognos Configuration, ensure that the operating environment is properly set up. For example, ensure that all environment variables have been set.

On a Microsoft Windows operating system, you can start IBM Cognos Configuration in the last page of the installation wizard only if additional setup is not required. For example, if you use a database server other than Microsoft SQL for the content store, copy the Java Database Connectivity (JDBC) drivers to the *install_location*/drivers folder before you start the configuration tool.

On UNIX or Linux operating systems, do not start IBM Cognos Configuration in the last page of the installation wizard. Additional setup is required before you can configure IBM Cognos Analytics. For example, you must update your Java environment.

Ensure that user or service account used to run IBM Cognos has been set up.

Read "Critical configuration actions to take first!" on page 47.

Procedure

1. On Microsoft Windows, click **Start** > **IBM Cognos Configuration**.

   If you are using a Windows computer, and have installed the product to the `Program Files (x86)` directory, start IBM Cognos Configuration as an Administrator.
2. On UNIX or Linux operating systems, go to the *install_location*/`bin64` directory and then type the following command:

   ```
   ./cogconfig.sh
   ```

   If IBM Cognos Configuration does not open, ensure that you set the DISPLAY environment variable.

   If you see a `JAVA.Lang.unsatisfied link` message, verify that you are using a supported version of Java.

   If you see a `Java.lang.unsupportedClassVersionError` message, ensure that you are using a 64-bit version of Java.

Set Database Connection Properties for the Content Store

You must specify the database server information to ensure that Content Manager can connect to the database you use for the content store. Content Manager uses the database logon to access the content store. After you set the database connection properties, you can test the connection between Content Manager and the content store.

In a production environment, you must use an enterprise-level database for your content store. For more information, see the topic about deploying the entire content store in the Administration and Security Guide.

If you are upgrading from IBM Cognos Business Intelligence or an earlier release of IBM Cognos Analytics, configure IBM Cognos Analytics to point to a copy of the existing content store database. After you save the configuration and start the IBM Cognos service, the data in the content store is automatically upgraded and cannot be used by the earlier version. By using a copy of the original database with the new version, you can keep IBM Cognos Analytics or the earlier version running with the original data.

Ensure that you used one of the supported database servers to create the content store.

Setting database connection properties for a IBM Db2 content store

You must specify the database server information to ensure that Content Manager can connect to the database you use for the content store.

Procedure

1. In the location where you installed Content Manager, start IBM Cognos Configuration.
2. In the **Explorer** window, under **Data Access**, **Content Manager**, click **Content Store**.
3. In the **Properties** window, for the **Database name** property, type the name of the database or the database alias.
4. Change the logon credentials to specify a valid user ID and password:
   - Click the **Value** box next to the **User ID and password** property and then click the edit button when it appears.
   - Type the appropriate values and click **OK**.

5. In the **Database server and port number** field, enter the name of your computer and port number on which Db2 is running. For example, `localhost:50000`. 50000 is the default port number used by Db2. If you are using a different port number, ensure you use that value.
6. From the **File** menu, click **Save**.
7. To test the connection between Content Manager and the content store database, from the **Actions** menu, click **Test**.

   Content Manager connects to the database, checks the database permissions, and creates and populates a table. The table is not deleted and is used each time that the test is repeated.

Setting database connection properties for a content store on IBM Db2 for z/OS
You must specify the database server information to ensure that Content Manager can connect to the database you use for the content store.

Procedure

1. In the location where you installed Content Manager, start IBM Cognos Configuration.
2. In the **Explorer** window, under **Data Access** > **Content Manager**, click **Content Store**.
3. In the **Properties** window, for the **Database name** property, type the name of the database or the database alias.
4. Change the logon credentials to specify a valid user ID and password:
   - Click the **Value** box next to the **User ID and password** property and then click the edit icon when it appears. Ensure that you specify the same user ID as the value you specified for CMSCRIPT_USERNAME when you created the tablespaces.
   - Type the appropriate values, and click **OK**.
5. For the **Database server and port number** property, type the database information as *`hostname`*`:`*`port`*.
6. In the **Explorer** window, click **Local Configuration**.
7. Click inside the **Value** box for **Advanced properties**, and then click the edit icon.

   The **Value - Advanced properties** dialog box appears.
8. Click **Add** to add the parameters for the database connection.

   The values in the table are examples, ensure that you enter the correct values for your environment.

Table 7: Content store connection parameters for Db2 for z/OS

Parameter name	Example value
CMSCRIPT_CREATE_IN	COGUCS.T1TSCS
CMSCRIPT_STOGROUP	DBOIUSR
CMSCRIPT_DATABASE	COGUCS
CMSCRIPT_CS_ID	T1
CMSCRIPT_TABLESPACE	TSCS
CMSCRIPT_LARGE_BP	BP32K
CMSCRIPT_REGULAR_BP	BP16K0

9. Click **File** > **Save**.
10. To test the connection between Content Manager and the content store database, from the **Actions** menu, click **Test**.

Setting database connection properties for a Microsoft SQL Server, Oracle, Informix content store

You must specify the database server information to ensure that Content Manager can connect to the database you use for the content store.

Procedure

1. On the computer where you installed Content Manager, start IBM Cognos Configuration.
2. In the **Explorer** window, under **Data Access**, **Content Manager**, right-click **Content Store** and click **Delete**.

   This step deletes the connection to the default resource. Content Manager can access only one content store.
3. Right-click **Content Manager**, and then click **New resource**, **Database**.
4. In the **Name** box, type a name for the resource.
5. In the **Type** box, select the type of database and click **OK**.

   Tip: If you want to use an Oracle PDB or Oracle RAC functionality, select **Oracle database (Advanced)**.
6. In the **Properties** window, provide the values for your database type:

   - If you use a Microsoft SQL Server database, type the appropriate values for the **Database server with port number or instance name** and **Database name** properties.

     For a Microsoft SQL Server database, you can choose to use a port number, such as 1433, or a named instance as the value for the **Database server with port number or instance name** property.

     For the **Database server with port number or instance name** property, include the instance name if there are multiple instances of Microsoft SQL Server.

     To connect to a named instance, you must specify the instance name as a Java Database Connectivity (JDBC) URL property or a data source property. For example, you can type `localhost\instance1`. If no instance name property is specified, a connection to the default instance is created.

     The properties specified for the named instance, along with the user ID and password, and database name, are used to create a JDBC URL. Here is an example:

     ```
     jdbc:JSQLConnect://localhost\\instance1/user=sa/
     more properties as required
     ```

   - If you use an Oracle database, type the appropriate values for the **Database server and port number** and **SID** properties.
   - If you use an Oracle PDB, for the **Database specifier** property, type `//`*`<server>`*`/`*`<servicename>`*. For example, `//corpserv1:1522/PDB1`
   - If you use an advanced Oracle Net 8 database, for the **Database specifier** property, type the Oracle Net8 keyword-value pair for the connection.

     Here is an Oracle Net8 keyword-value pair example:

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

     When you select the advanced Oracle database, IBM Cognos Analytics uses enterprise-oriented Oracle features to select a listener, switch to another listener if the first listener fails, automatically reconnect to the database if the connection fails, balance connection requests among listeners, and balance connection requests among dispatchers.
   - If you use an Informix database, type the appropriate values for the **Database server and port number** and **Database name** properties.
7. To configure logon credentials, specify a user ID and password:

- Click the **Value** box next to the **User ID and password** property and then click the edit icon when it appears.
- Type the appropriate values and click **OK**.

8. If you host more than one content store database on an Informix instance, create the advanced property CMSCRIPT_CS_ID and specify the account under which the instance runs:
   - In the **Explorer** window, click **Local Configuration**.
   - In the **Properties** window, click the **Value** column for **Advanced properties** and then click the edit icon.
   - In the **Value - Advanced properties** dialog box, click **Add**.
   - In the **Name** column, type `CMSCRIPT_CS_ID`
   - In the **Value** column, type the user ID of the account under which the instance of the content store runs.

     Use a different user account for each instance of Informix content store database.
9. From the **File** menu, click **Save**.

   The logon credentials are immediately encrypted.
10. To test the connection between Content Manager and the content store database, from the **Actions** menu, click **Test**.

    Content Manager connects to the database, checks the database permissions, and creates and populates a table. The table is not deleted and is used each time that the test is repeated.

Results

Content Manager can now create the required tables in the content store when you start the IBM Cognos service for the first time. If the connection properties are not specified correctly, you cannot start the IBM Cognos services.

Configure Environment Properties for Content Manager Computers

The Content Manager computers must know the location of the content store, the other Content Manager computers, and the database that is used for notification.

After installing Content Manager on the computers you are using for failover protection, you must configure Content Manager on those computers. If you installed more than one Content Manager, you must list all Content Manager URIs on each Content Manager computer.

After you complete the required configuration tasks and start the IBM Cognos Analytics service, the certificate authority service is available to issue certificates to other computers. You can then perform the required configuration tasks on other computers, such as the Application Tier Components computer and gateway computers. Otherwise, you can continue to configure the Content Manager computers by changing the default property settings (see “Changing Default Configuration Settings” on page 94) so that they better suit your environment. For example, you can configure IBM Cognos Analytics components to use an authentication provider (see Chapter 7, “Configuring authentication providers ,” on page 163), enable and disable services (see “Enable and Disable Services” on page 104) on the Content Manager computers, or change global settings (see “Changing Global Settings” on page 145).

Note that if you change global settings on one Content Manager computer, you must make the same changes on the other Content Manager computers.

Configuring the active Content Manager

The Content Manager computers must know the location of the content store, the other Content Manager computers, and the database that is used for notification.

Procedure

1. On the Content Manager computer that you want to designate as the default active Content Manager, start IBM Cognos Configuration.
2. In the **Explorer** window, click **Environment**.
3. In the **Properties** window, click the value for **Content Manager URIs** and then click the edit button.
4. Specify the URIs for the other Content Manager computers:
   - In the **Value - Content Manager URIs** dialog box, click **Add**.
   - In the blank row of the table, click and then type the full URI of the Content Manager computer.

     Do not delete the first value in the table. This value identifies the local Content Manager computer and is required.

     Replace the localhost portion of the URI with a host name or IP address. All URI properties must use the the same format: all host names or all IP addresses.
   - Repeat the previous two bulleted steps for each URI to be added.

     You must include all Content Manager URIs in the list.
   - Click **OK**.
5. From the **File** menu, click **Save**.

Configuring standby Content Managers

The Content Manager computers must know the location of the content store, the other Content Manager computers, and the database that is used for notification.

Procedure

1. Ensure that you already configured the Environment properties on at least one Content Manager computer and that IBM Cognos Analytics components are running on that computer.
2. On the standby Content Manager computer, start IBM Cognos Configuration.
3. In the **Explorer** window, click **Environment**.
4. In the **Properties** window, click the value for **Content Manager URIs**, and then click the edit button.
5. Specify the URIs for the other Content Manager computers:
   - In the **Value - Content Manager URIs** dialog box, click **Add**.
   - In the blank row of the table, click and then type the full URI of the Content Manager computer.

     Do not delete the first value in the table. This value identifies the local Content Manager computer and is required.

     Replace the localhost portion of the URI with a host name or IP address. All URI properties must use the the same format: all host names or all IP addresses.
   - Repeat the previous two bulleted steps for each URI to be added.

     You must include all Content Manager URIs in the list.
   - Click **OK**.
6. In the **Explorer** window, under **Security** > **Cryptography**, click **Cognos**, the default cryptographic provider.
7. Ensure that all cryptographic settings match what you configured on the default active Content Manager computer.
8. In the **Explorer** window, under **Data Access** > **Content Manager**, click **Content Store**.
9. Ensure that the values for all of the properties match what you configured on the default active Content Manager computer.
10. From the **File** menu, click **Save**.

Specify a connection to an email server

If you want to send reports by email, you must configure a connection to your email server.

Procedure

1. In the **Explorer** window, under **Data Access**, click **Notification**.
2. In the **Properties** window, for the **SMTP mail server** property, type the host name and port of your SMTP (outgoing) email server.

   To be able to open reports that are sent by email, you must change the host name portion of the **Gateway URI** from localhost to either the IP address of the computer or the computer name. Otherwise the URL in the email will contain localhost, and remote users will not be able to open the report.

   To be able to open reports that are sent as links, ensure that the **Gateway URI** on report servers and notification servers specifies an accessible web server hosting IBM Cognos content. If you have mobile users accessing links remotely, consider using an external URI.
3. Click the **Value** box next to the **Account and password** property, and click the edit button when it appears.
4. Type the values in the **Value - Account and password** dialog box, and click **OK**.

   If logon credentials are not required for the SMTP server, remove the default information for the **Account and password** property. When you are prompted for confirmation to leave this property blank, click **OK**. Ensure that the default user name is removed. Otherwise, the default account is used and notifications do not work properly.
5. In the **Properties** window, type the appropriate value for the default sender account.
6. In the **Explorer** window, right-click **Notification**, and click **Test**.

   IBM Cognos Analytics tests the email server connection.

Enabling a secure TLS connection to your email server

Enable a secure TLS connection to your email server to allow encrypted TLS communication.

Note: If SSL Encryption is configured but a secure TLS connection is not enabled, the connection fails and the following message appears:

502 Unknown command

Before you begin

You must have a certificate, typically in .crt format, that is common to the email server.

Procedure

1. Import the certificate to enable a trust between Cognos Analytics and the email server.

   a) If you are using HTTP on the dispatcher URI, you must import the certificate into the JRE keystore:

   - On Windows, type `*install_location*\bin\DLS_SSL_CertImportTool.bat *certificate_location*\*email_certificate*.crt -p *keystore_password*`
   - On Unix or Linux, type `*install_location*/bin/DLS_SSL_CertImportTool.sh *certificate_location*/*email_certificate*.crt -p *keystore_password*`

   b) If you are using HTTPS on the dispatcher URI, you must import the certificate into the Cognos keystore:

   - On Windows, type `*install_location*\bin\ThirdPartyCertificateTool.bat -T -i -r *certificate_location*\*email_certificate*.crt -p *keystore_password*`
   - On Unix or Linux, type `*install_location*/bin/ThirdPartyCertificateTool.sh -T -i -r *certificate_location*/*email_certificate*.crt -p *keystore_password*`
2. In Cognos Configuration, select **Data Access** > **Notification** and edit the properties as follows:

Name	value
SMTP mail server	*email_server_name*:*port_number*, where *port_number* represents a port that is enabled for TLS/SSL or STARTTLS
Account and password	A userid and password when authentication to the email server is required.
Default Sender	The email account that sends emails from the email server.
SSL Encryption Enabled	True

3. In Cognos Configuration, select **Local Configuration**.
   a) Click the **Value** field for **Advanced properties**.
   b) Click the pencil icon ✏.
   c) Click **Add**.
   d) In the **Name** field, type `emf.mail.tls.enabled`
   e) In the **Value** field, type `true`
   f) Click **OK**.
4. In Cognos Administration, configure the advanced setting `emf.mail.tls.enabled` with a value of `true`. For more information, see *Configuring advanced settings for specific services*.

   Note: You must restart the delivery service after you make this change.

Enable Security

By default, IBM Cognos Analytics allows anonymous access. If you want to use security in your IBM Cognos Analytics environment, you must disable anonymous access and configure IBM Cognos Analytics to use an authentication provider.

Procedure

1. In the IBM Cognos Configuration **Explorer** window, click **Security** >**Authentication** > **Cognos**.
2. Click the **Value** box for **Allow Anonymous Access**, and select **False**.
3. Right-click **Authentication**, and click **New Resource** > **Namespace**.
4. In the **Name** box, type a name for your authentication namespace.
5. In the **Type** list, click the appropriate namespace type and then click **OK**.

   The new authentication provider resource appears in the **Explorer** window, under the **Authentication** component.
6. In the **Properties** window, for the **Namespace ID** property, specify a unique identifier for the namespace.
7. From the **File** menu, click **Save**.

Start Content Manager

After you have set the database connection properties for the content store and configured the security namespace, you can start the Content Manager computer.

Before you begin

Ensure that user or service account is set up. For information, see Configure a User Account or Network Service Account for IBM Cognos Analytics.

Procedure

1. Start IBM Cognos Configuration.

If you are upgrading, a message appears indicating that configuration files were detected and upgraded to the new version.

2. Ensure that you save your configuration, otherwise you cannot start the IBM Cognos service.
3. From the **Actions** menu, click **Test**.

   IBM Cognos Configuration checks the common symmetric keys (CSK) availability, tests the namespace configuration, and tests the connections to the content store and other resources.

   Tip: If **Test** is not available for selection, in the **Explorer** window, click **Local Configuration**.
4. If the test fails, reconfigure the affected properties and then test again.

   You can test some components individually by right-clicking the component in the **Explorer** panel and selecting **Test**.

   Do not start the service until all tests are error-free.
5. From the **Actions** menu, click **Start**.

   It may take a few minutes for the IBM Cognos service to start.

   This action starts all installed services that are not running and registers the IBM Cognos service on Windows.

Test the Content Manager installation

You can test the installation using a web browser.

Procedure

1. Open a web browser.
2. Test that Content Manager is running by typing the URI for the active Content Manager. For example, `http://`*`host_name:port`*`/p2pd/servlet`

   The default value for *`host_name:port`* is localhost:9300.

   Content Manager is available when the **State** value is **Running** or **Standby**.

Installing and configuring the Application services

You can install the Application services components on different computers or on the same computer.

Install the Application services components

Ensure that the computer where you installed the active Content Manager is configured and available before you configure Application services components computers.

If you are upgrading, IBM Cognos Analytics uses the existing configuration data for the Application services components computers. However, if you installed the Application services components in a new location, you must configure the environment properties.

64-bit Installations

The report server component, included with the Application services components, is provided in both 32- and 64-bit versions. Selecting which version you use is done using IBM Cognos Configuration after installation. By default, the report server component is set to use the 32-bit mode, even on a 64-bit computer. The 32-bit mode allows you to run all reports, whereas the 64-bit mode allows you to run only reports created for dynamic query mode.

Printer Requirements

To ensure that reports print properly on a Microsoft Windows operating system, Adobe Reader requires that you configure at least one printer on the operating system where Application services components are installed. All reports, regardless of the print format that you choose, are sent as temporary PDF files to Adobe Reader for printing.

Installing the application services components on UNIX or Linux operating systems

You can install Application services components on one or more computers, depending on your environment.

Before you begin

Go to the IBM Software Product Compatibility Reports page (www.ibm.com/support/docview.wss?uid=swg27047186) to verify that the required patches are installed on your computer.

Procedure

1. Go to the location where the installation files were downloaded and extracted.

   Tip: Use new versions of file compression software to extract the files. Older versions of such software might not extract the files.
2. To start the installation wizard, go to the operating system directory and then type `./ca_srv_<platform>_<build>.bin`

   Tip: When you use the `ca_srv_<platform>_<build>.bin` command with XWindows, Japanese characters in messages and log files may be corrupted. When installing in Japanese on UNIX or Linux, first set environment variables LANG=C and LC_ALL=C (where C is the language code, for example ja_JP.PCK on Solaris), and then start the installation wizard.

   If you do not use XWindows, run an unattended installation. For more information, see Installation Guide.
3. Follow the directions in the installation wizard to copy the files to your computer.
   - When selecting the directory, consider the following:

     Install Application services components in a directory that contains only ASCII characters in the path name. Some UNIX and Linux Web servers do not support non-ASCII characters in directory names.
   - When selecting components, clear all components except **Application services**.
4. Click **Finish**.

   Do not configure IBM Cognos Analytics immediately because you must do other tasks first to ensure that your environment is properly set up.
5. Append the *`install_location`*`/bin` directory to the appropriate library path environment variable.
   - For Linux, LD_LIBRARY_PATH
   - For AIX, LIBPATH

What to do next

Configure IBM Cognos Analytics using IBM Cognos Configuration. Open this tool by typing `cogconfig.sh` in the *`install_location`*`/bin64` directory.

Installing the application services components on Windows operating system

You can install application services components on one or more computers, depending on your environment.

For Windows computers, the default installation location uses the **Program Files** directory. If you install to this location, ensure that you run IBM Cognos Configuration as an administrator. Alternatively, you can install the product to a directory outside of **Program Files**, such as `C:\IBM\cognos\analytics`.

Procedure

1. Go to the location where the installation files were downloaded and extracted, and double-click `ca_srv_<platform>_<build>.exe`.

   Tip: Use new versions of file compression software to extract the files. Older versions of such software might not extract the files.
2. Select the language to use for the installation.

   The language that you select determines the language of the user interface. All supported languages are installed. You can change the user interface to any of the installed languages after installation.
3. Select the **Custom** installation option, and follow the directions in the installation wizard to copy the files to your computer.
   - When selecting the directory, consider the following:

     Install application services components in a directory that contains only ASCII characters in the path name. Some web servers do not support non-ASCII characters in directory names.
   - When selecting components, clear all components except **Application services**.
4. Click **Finish**.

What to do next

You can start IBM Cognos Configuration using the **IBM Cognos Configuration** shortcut from the **Start** menu.

Set up database connectivity for reporting databases

To support communication between IBM Cognos Analytics and the data sources, you must install additional software for your data sources on the same computer that hosts the report server. Depending on the data source and query mode, the required software might include database clients, or Java Database Connectivity (JDBC) driver files, or both.

For IBM Cognos Analytics, the query database (also known as the reporting database) is only accessed by the reporting engine that runs reports. The reporting engine is installed with Application Tier Components and is also used by Framework Manager, and IBM Cognos Transformer.

Compatible query mode

To run reports that use the compatible query mode, you must use 32-bit data source client libraries and configure the report server to be 32-bit. The compatible query mode uses native client and ODBC connections to communicate with data sources.

Dynamic query mode

Dynamic query mode provides communication to data sources using Java/XMLA connections.

For supported relational databases, a type 4 JDBC connection is required. A type 4 JDBC driver converts JDBC calls directly into the vendor-specific database protocol. It is written in pure Java and is platform-independent.

For supported OLAP data sources, Java/XMLA connectivity optimizes access by providing customized and enhanced MDX for the specific source and version of your OLAP technology and it harnesses the smarts of the OLAP data source.

To review an up-to-date list of environments that are supported by IBM Cognos Analytics products, including information on operating systems, patches, browsers, web servers, directory servers, database servers, and application servers, see the IBM Software Product Compatibility Reports page (www.ibm.com/support/docview.wss?uid=swg27047186).

Access OLAP data sources on Windows operating systems

To access the relational databases and OLAP data sources for reporting, you must install the client API software that is provided by your data source vendor. The software must be installed on the same computer where the Application Tier Components are installed.

Procedure

1. Install the database API software for your relational databases and OLAP data sources on the computer that hosts the report server (where Application Tier Components are installed).

   On Microsoft Windows operating systems, the reporting engine supports either native database connectivity or ODBC.
2. If Framework Manager is installed in a separate location from the Application Tier Components, you must also install the client API software on the computer where Framework Manager is installed.

   For more information, see "Setting variables for data source connections for Framework Manager" on page 90.

Access ODBC data sources on UNIX or Linux operating systems

To use an ODBC data source on UNIX or Linux to connect to a supported data source, you must configure the environment to locate the `.odbc.ini` file which contains the references to data source, the connectivity libraries, and their accompanying Driver Manager libraries.

To review supported ODBC data sources, see the IBM Software Product Compatibility Reports page (www.ibm.com/support/docview.wss?uid=swg27047186).

After configuring for the ODBC connections, you must create connections to the data sources in IBM Cognos Administration. For information, see the *IBM Cognos Administration and Security Guide*.

If your database vendor does not supply a driver manager, you can use unixODBC or iODBC, depending on your operating system.

On Linux operating systems, the unixODBC package provided with the operating system provides the ODBC Driver Manager. You must install unixODBC version 2.2.11 or later before you can set up data source connections. To verify the version you have installed, use the following command: `odbcinst --version`. Check which version of unixODBC is required for the database you are using, and ensure you use that version.

On UNIX operating systems, the open source iODBC driver manager is provided as part of the IBM Cognos installation.

Procedure

1. Create an environment variable to specify the location of the `.odbc.ini` file.

   For example,

   ```
   export ODBCINI=/usr/local/etc/.odbc.ini
   ```
2. Set the appropriate library path environment variable to specify the location of the 32-bit connectivity libraries and Driver Manager for your database.

   The following table lists the environment variables for each operating system that must specify the location of the driver manager libraries.

   Table 8: Environment variables for your operating system

Operating system	Environment variable
AIX	LIBPATH
Linux	LD_LIBRARY_PATH

3. If your database vendor does not provide a driver manager, set the library path to include the path the local driver manager.

   - On UNIX, iODBC is provided as part of the IBM Cognos installation. The library files are located in the *install_location*/bin directory. Your library path should already contain the *install_location*/bin directory.

     For example,

     ```
     LIBPATH=/usr/IBM/cognos/bin:$LIBPATH
     ```

   - On Linux, the unixODBC package provides the required driver manager libraries.

     For example,

     ```
     LD_LIBRARY_PATH=/usr/lib:$LD_LIBRARY_PATH
     ```

What to do next

If you are using multiple ODBC sources on UNIX or Linux operating systems, you may encounter dependencies of library files with common names but different implementations for both the connectivity and the driver manager. In a scenario where one ODBC source validates while another fails based on a dependency, please contact Customer Support. Using a common `.odbc.ini` may result in having incompatible entries for different driver managers. To resolve the problem, review the structure requirements between the driver managers you are using and try to use syntax that is common between the conflicting driver managers.

Configuring IBM Cognos Analytics to use Oracle Essbase

If you use IBM Cognos Analytics with an Oracle Essbase data source version 11.1.1, you must edit a configuration file to inform the IBM Cognos Analytics server of your version.

By default, IBM Cognos Analytics is configured to use Oracle Essbase version 11.1.2. Therefore, no configuration is required if you use this version. If you use another supported version of Oracle Essbase, you must edit the qfs.config.xml file for your version.

In addition, if you use Oracle Essbase version 11.1.2, you must install Oracle Foundation Services as well as the Oracle Essbase client.

Procedure

1. Go to the *install_location*/configuration directory.
2. Open the qfs_config.xml file in an xml or text editor.
3. Locate the following lines:

   ```
   <!--provider name="DB2OlapODP" libraryName="essodp111" connectionCode="DO"-->
   <provider name="DB2OlapODP" libraryName="essodp1112" connectionCode="DO">
   ```

4. For Oracle Essbase 11.1.1, change them as follows:

   ```
   <provider name="DB2OlapODP" libraryName="essodp111" connectionCode="DO">
   <!--provider name="DB2OlapODP" libraryName="essodp1112" connectionCode="DO"-->
   ```

5. For Oracle Essbase 11.1.2, ensure that the lines appear as follows:

   ```
   <!--provider name="DB2OlapODP" libraryName="essodp111" connectionCode="DO"-->
   <provider name="DB2OlapODP" libraryName="essodp1112" connectionCode="DO">
   ```

6. Save the file and restart the IBM Cognos service

Configuring Oracle Essbase on a UNIX or 64-bit Microsoft Windows operating system

If you use an Oracle Essbase version 11.1.2 data source with IBM Cognos Analytics on a UNIX or 64-bit Microsoft Windows operating system, you must manually configure the ARBORPATH and ESSBASEPATH environment variables.

The ARBORPATH and ESSBASEPATH environment variables are created during the installation of the Oracle Essbase client. IBM Cognos Analytics uses these variables to find the Oracle Essbase client location.

To use Oracle Essbase with IBM Cognos Analytics on a UNIX or 64-bit Microsoft Windows operating system, you must install the 64-bit Oracle Essbase client. This 64-bit client includes a 32-bit client that IBM Cognos Analytics uses. To point to this 32-bit client, you must manually change the ARBORPATH and ESSBASEPATH environment variables to replace `EssbaseClient` with `EssbaseClient-32`. The following example assumes that the client is installed on the C drive. Your installation location might be different.

```
ARBORPATH=C:\Hyperion\EPMSystem11R1\products\Essbase\EssbaseClient-32
```

```
ESSBASEPATH=C:\Hyperion\EPMSystem11R1\products\Essbase\EssbaseClient-32
```

If you use a 32-bit Microsoft Windows operating system with a 32-bit Oracle Essbase client, you are not required to change these environment variables.

Start IBM Cognos Configuration

Use IBM Cognos Configuration to configure IBM Cognos Analytics components and to start and stop IBM Cognos services.

Before you begin

Before starting IBM Cognos Configuration, ensure that the operating environment is properly set up. For example, ensure that all environment variables have been set.

On a Microsoft Windows operating system, you can start IBM Cognos Configuration in the last page of the installation wizard only if additional setup is not required. For example, if you use a database server other than Microsoft SQL for the content store, copy the Java Database Connectivity (JDBC) drivers to the *install_location*/`drivers` folder before you start the configuration tool.

On UNIX or Linux operating systems, do not start IBM Cognos Configuration in the last page of the installation wizard. Additional setup is required before you can configure IBM Cognos Analytics. For example, you must update your Java environment.

Ensure that user or service account used to run IBM Cognos has been set up.

Read “Critical configuration actions to take first!” on page 47.

Procedure

1. On Microsoft Windows, click **Start** > **IBM Cognos Configuration**.

   If you are using a Windows computer, and have installed the product to the `Program Files (x86)` directory, start IBM Cognos Configuration as an Administrator.
2. On UNIX or Linux operating systems, go to the *install_location*/`bin64` directory and then type the following command:

   ```
   ./cogconfig.sh
   ```

   If IBM Cognos Configuration does not open, ensure that you set the DISPLAY environment variable.

   If you see a `JAVA.Lang.unsatisfied link` message, verify that you are using a supported version of Java.

   If you see a `Java.lang.unsupportedClassVersionError` message, ensure that you are using a 64-bit version of Java.

Configure Environment Properties for Application services components computers

If you install the Application services components on a different computer than Content Manager, you must configure the Application services components computer so that it knows the location of Content Manager. The distributed components can then communicate with each other.

The Application services components computer must know the location of the Content Manager computers and the notification database to use for job and schedule information. The Application services components computer must use the same notification database that the Content Manager computers use. For more information, see "Change the notification database" on page 114.

If you installed more than one Content Manager, you must list all Content Manager URIs on each Application services components computer.

Procedure

1. Start IBM Cognos Configuration.
2. In the **Explorer** window, click **Environment**.
3. In the **Properties** window, change the **localhost** portion of the **Content Manager URIs** property to the name of any Content Manager computer.
4. Specify the URIs for the remaining Content Manager computers:
   - In the **Value - Content Manager URIs** dialog box, click **Add**.
   - In the blank row of the table, click and then type the full URI of the Content Manager computer.

     Replace the localhost portion of the URI with a host name or IP address. All URI properties must use the the same format: all host names or all IP addresses.
   - Repeat the previous two bulleted steps for each URI to be added.

     You must include all Content Manager URIs in the list.
   - Click **OK**.
5. Change the **localhost** portion of the **Gateway URI** property to the name of the computer on which you plan to install the gateway component.

   This will ensure that users in different locations can connect to reports and workspaces that are sent by email.
6. Change the **localhost** portion of the remaining URI properties to the name or IP address of your IBM Cognos Analytics server.
7. In the **Explorer** window, under **Security** > **Cryptography**, click **Cognos**, the default cryptographic provider.
8. Under the **Certificate Authority settings** property group, set the **Password** property to match what you configured on the default active Content Manager computer.
9. Ensure that all other cryptographic settings match what you set on the default active Content Manager computer.
10. From the **File** menu, click **Save**.

Enabling the 64-bit version of report server

You can choose to use a 32-bit or 64-bit version of the report server component. To use the 64-bit version, you must enable it using IBM Cognos Configuration. The default option is 32-bit.

A 32-bit report server can be used with both dynamic query mode and compatible query mode packages. A 64-bit report server can be used only with dynamic query mode packages.

The report server works with the query service. The query service is the engine that powers the dynamic query mode and dynamic cubes. In a 64-bit installation, the query service is 64-bit regardless of whether the report server component is configured to be 32-bit or 64-bit.

Using the 64-bit version of the report server allows more addressable memory for rendering report outputs. For example, out-of-memory conditions during the rendering stage of running a report can be avoided. It is only large report outputs, for example PDF reports with more than 1 thousand pages that require the 64-bit version of the report server component.

You must use the 32-bit version of report server for packages that do not use dynamic query mode. For example, if your package is based on IBM Cognos PowerCubes, you must use the 32-bit version of report server.

If you have multiple Application Tier Components instances in your environment, you can set one instance to use the 32-bit report server. You can then use routing rules so that report requests for non-dynamic query mode packages are routed to the instance that is running the 32-bit version of report server. For more information about routing rules, see the *Administration and Security Guide*.

To enable the 64-bit version, you must install the 64-bit version of the Application Tier Components on a 64-bit computer. If you install the 32-bit version of the Application Tier Components or are using a 32-bit computer, do not enable the 64-bit report server.

Procedure

1. In the IBM Cognos Configuration **Explorer** window, click **Environment**.
2. Click the **Value** box for **Report server execution mode**, and select **64-bit**.
3. From the **File** menu, click **Save**.
4. Restart your IBM Cognos services if they are running.

Start the Application services components

After you have configured the environment properties, you can start the services on the Application services components computer.

Before you begin

To use IBM Cognos Analytics for reporting, you must install and configure the server components, start the IBM Cognos service, and have a package that references an available data source. Note that if you are upgrading, you can continue to use the same data sources.

Ensure that user or service account is set up. For information, see Configure a User Account or Network Service Account for IBM Cognos Analytics.

Procedure

1. Start IBM Cognos Configuration.

   If you are upgrading, a message appears indicating that configuration files were detected and upgraded to the new version.
2. Ensure that you save your configuration, otherwise you cannot start the IBM Cognos service.
3. From the **Actions** menu, click **Test**.

   IBM Cognos Configuration checks the common symmetric keys (CSK) availability, tests the namespace configuration, and tests the connections to the content store and other resources.

   Tip: If **Test** is not available for selection, in the **Explorer** window, click **Local Configuration**.
4. If the test fails, reconfigure the affected properties and then test again.

   You can test some components individually by right-clicking the component in the **Explorer** panel and selecting **Test**.

   Do not start the service until all tests are error-free.
5. From the **Actions** menu, click **Start**.

   It may take a few minutes for the IBM Cognos service to start.

   This action starts all installed services that are not running and registers the IBM Cognos service on Windows.

Test the Application services components

You can test the installation using a Web browser.

Procedure

1. Open a Web browser.
2. Test the availability of the dispatcher by typing the **External dispatcher URI** value from IBM Cognos Configuration. For example,

   `http://`*`host_name:port`*`/bi`

   The default value for *`host_name:port`* is localhost:9300.

   The dispatcher is available when the portal appears.

Setting up a Cognos Mobile database

By default, the Cognos Mobile tables are created in the IBM Cognos Analytics content store database. If Cognos Analytics Content Manager and the application tier components are not installed in the same location, you can configure an alternative Cognos Mobile database.

To set up the Cognos Mobile database, you must first create the database, create a user account under which the database will operate, and then configure Cognos Analytics to use the database.

Procedure

1. Create a database using the same instructions as when creating a content store database. For more information, see Guidelines for creating the content store.
2. Create a user account that will be used to operate the database.
3. On the computer where the application tier components are installed, start IBM Cognos Configuration.
4. In the **Explorer** pane, under **Data Access**, right-click **Mobile**, and select **New resource** > **Database**.
5. In the **Type** field, select the database type.
6. Type a name for the database, and click **OK**.
7. In the **Database - Resource Properties** window, specify the database server name and port number, and the user ID and password as specified in step 2.
8. From the **File** menu, click **Save**.

   The logon credentials are immediately encrypted.
9. To test the connection to the new database, from the **Actions** menu, click **Test**.
10. From the **Actions** menu, **Start** or **Restart** the **IBM Cognos** service.

    The Cognos Mobile tables are automatically created after the Mobile service starts for the first time.

    Tip: If the tables are not created, perhaps because the Cognos Analytics security credentials do not allow it, you can create them manually. The creation scripts are available in the *`install_location`* `\configuration\schemas\mobile` directory.

What to do next

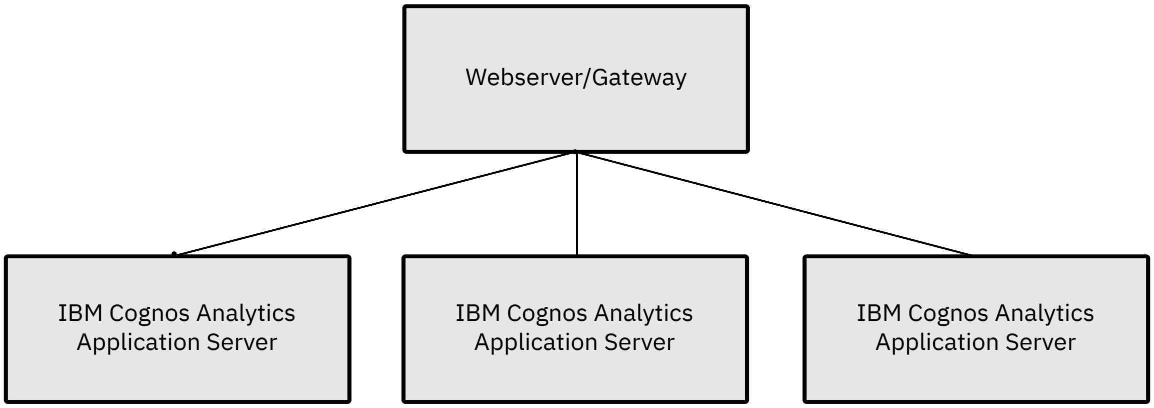
Users can install the IBM Cognos Mobile app on their mobile devices to access IBM Cognos Analytics reports or analyses. The iOS version of the app can be downloaded from the Apple App Store and the Android version from the Google Play Store.

Chapter 4. Configuring the gateway

You can install the optional gateway on one or more computers. Install the gateway if you plan on setting up advanced options such as single sign-on with Kerberos security with IIS, or an architecture where the web server is publicly available outside a firewall. IBM Cognos Analytics uses the web server for load balancing certain requests in addition to hosting and serving static content like icons and image files.

Ensure that the computer where you installed the active Application services is configured and available before you configure gateway computers.

The following diagram shows the gateway server and multiple Cognos Analytics servers. With load balancing enabled, the work load can be distributed across the servers.


Webserver/Gateway
IBM Cognos Analytics Application Server
IBM Cognos Analytics Application Server
IBM Cognos Analytics Application Server

This configuration is also recommended in a single application tier environment as the routing would just go to the one server and is ready to add additional tier servers when needed.

Perform the following steps to install and configure the gateway:

- Install the gateway components. See "Installing the Cognos Analytics gateway" on page 65.
- Configure IBM Cognos Analytics. See "Configure Cognos Analytics with your web server" on page 66.
- If your web server is Apache HTTP Server or IBM HTTP Server, perform the procedures in "Configure Apache HTTP Server or IBM HTTP Server " on page 69 .
- If your web server is Microsoft Internet Information Services, perform the procedures in "Configure Microsoft Internet Information Services " on page 76.
- Test the gateway installation .

Installing the Cognos Analytics gateway

You can install the IBM Cognos Analytics gateway on one or more computers. If you have a web farm, you can install an IBM Cognos Analytics gateway on each web server.

Before you begin

Go to the IBM Software Product Compatibility Reports page (www.ibm.com/support/docview.wss?uid=swg27047186) to verify that the required patches are installed on your computer.

Ensure that the temporary directory has at least 5 GB of memory.

Tip: The temporary directory is set with the environment variable *IATEMPDIR* for the UNIX or Linux operating system or with *TMP* for the Microsoft Windows operating system.

Procedure

1. Start the installation wizard.
    a) For UNIX or Linux, go to the operating system directory and type: `./ca_srv_platform_build.bin`

    Tip: When you use the `ca_srv_<platform>_<build>.bin` command with XWindows, Japanese characters in messages and log files may be corrupted. When installing in Japanese on UNIX or Linux, first set environment variables LANG=C and LC_ALL=C (where C is the language code, for example ja_JP.PCK on Solaris), and then start the installation wizard.

    If you do not use XWindows, run an unattended installation. For more information, see Unattended installation, uninstallation, and configuration.

    b) For Microsoft Windows, go to the operating system directory, or where the installation files were downloaded, and double-click `ca_srv_platform_build.exe`.
2. Select the language to use for the installation.

    The language that you select determines the language of the user interface. All supported languages are installed. You can change the user interface to any of the installed languages after installation.
3. Select the **Custom** installation option, and follow the directions in the installation wizard to copy the required files to your computer.
    - When selecting the directory, consider the following:

      Install gateway components in a directory that contains only ASCII characters in the path name. Some UNIX and Linux web servers do not support non-ASCII characters in directory names.
    - When selecting components, clear all components except **Gateway**.
4. Click **Finish**.

Configure Cognos Analytics with your web server

You must configure your web server before users can connect to the IBM Cognos Analytics portal.

For IBM Cognos Analytics for reporting, you must also set the content expiry for the images directory in your web server so that the web browser does not check image status after the first access.

File permissions

The account under which the web server runs must have read, write and execute privileges to the Cognos installation location. Read access is required to the `./configuration` directory for the `cogstartup.xml` file. Write access is required to `./logs` if debug tracing is required. Execute access is required to the `./cgi-bin` directory so that the SSO modules for Apache HTTP Server, IBM HTTP Server, or Microsoft Internet Information Services can be run by the web server.

Reference values for the configuration procedures

Refer to the following values where required:

- server name: host name of the web server
- port #: 80 (non-SSL) or 443 (SSL)
- virtual directory name: ibmcognos
- Cognos Analytics server name: host name of the IBM Cognos Analytics server(n)

  Important: If your environment contains more than one Cognos Analytics server, do not include the server running Content Manager service in the steps below. Include only Cognos Analytics servers that have the application server components installed and configured.

- Cognos Analytics port #: `9300`

Some or all of these URI settings are in Cognos Configuration, depending on the type of install used:

- **Gateway URI**: For non-SSL use `http://`*`web_server_host_name`*`:80/ibmcognos/bi/v1/disp`. For SSL use `https://`*`web_server_host_name`*`:443/ibmcognos/bi/v1/disp`

  This is the URL for disconnected content such as links in PDFs, Excel, and Active Reports. It is also used in links sent by email.

- **Dispatcher URIs for gateway**: `http(s)://`*`IBM_Cognos_Analytics_server_host_name`*`:9300/bi/v1/disp`

  This is the list of URIs that the Cognos Apache module or ISAPI code connects to when forwarding requests. Multiple entries are used for failover. Include all relevant IBM Cognos Analytics application servers.

- **Dispatcher URI for external applications**: `http(s)://`*`IBM_Cognos_Analytics_server_host_name`*`:9300/bi/v1/disp`

  External applications such as Framework Manager connect on this URL to perform SDK operations.

Microsoft Internet Information Services

If you want to configure single sign-on (SSO), make sure that IsapiModule and WindowsAuthenticationModule are installed and enabled.

Install the Application Request Routing extension for IIS. For information about how to do this, see https://www.iis.net/downloads/microsoft/application-request-routing. This will also install the URL Rewrite extension.

URL Rewrite enables web administrators to create powerful rules to implement URLs that are easier for users to remember and easier for search engines to find. Application Request Routing enables web server administrators to increase web application scalability and reliability through rule-based routing, client and host name affinity, load balancing of HTTP server requests, and distributed disk caching.

If you are upgrading from Cognos Analytics 11.0.3 to Cognos Analytics 11.0.4 (or later) and you had modified `server.xml` to configure an `sso/login` path pointing to `/ibmcognos/cgi-bin/cognosisapi.dll`, remove the following entry from *`install_location`*`/wlp/usr/servers/cognosserver/server.xml:`

```
<jndiEntry jndiName="glass/sso/login" value="/ibmcognos/cgi-bin/cognosisapi.dll"/>
```

For details on configuration for Active Directory Server, see "Enable single signon between Active Directory Server and IBM Cognos components" on page 173

Enabling the 32-bit web gateway

For a 32-bit web server, you must manually move the 32-bit gateway files in your installation directory.

Procedure

1. Go to the *`install_location`*`/cgi-bin`.
2. Type the following command:
   - On UNIX or Linux operating systems, type `./copyGateMod.sh 32bit`
   - On Windows operating systems, type `copyGateMod.bat 32bit`

Results

The 32-bit gateway files are copied from the `cgi-bin/lib` directory to the `cgi-bin` directory.

Note: If you need to restore the default 64-bit gateway files, follow the procedure and type `./copyGateMod.sh 64bit` or `copyGateMod.bat 64bit`. The 64-bit gateway files are copied from the `cgi-bin/lib64` directory to the `cgi-bin` directory.

Configuring dispatcher URIs

If you install the gateway component on a different computer than Content Manager or Application Tier Components, you must configure the gateway computer so that it knows the location of a dispatcher. A dispatcher is installed on every Content Manager and Application Tier Components computer. Configure the gateway to use the dispatcher on an Application Tier Components computer.

For failover protection, you can configure more than one dispatcher for a gateway computer. When multiple dispatchers are configured, requests are normally routed to the first dispatcher in the list. If this dispatcher becomes unavailable, the gateway determines the next functioning dispatcher on the list and routes requests there. The primary dispatcher status is monitored by the gateway, and requests are routed back to this component when it returns to service.

After you do the required configuration tasks, the gateway computer can work in your environment.

Before you begin

Ensure that the computers where you installed Content Manager are configured and the default active Content Manager computer is available before you configure gateway computers.

Procedure

1. Start IBM Cognos Configuration.
   a) On Microsoft Windows, click **Start** > **IBM Cognos Configuration**.

      If you are using a Windows 7, or Windows 2008 computer, and have installed the product to the `Program Files (x86)` directory, start IBM Cognos Configuration as an Administrator.

   b) On UNIX or Linux operating systems, go to the *`install_location`*`/bin64` directory and then type the following command:

      ```
      ./cogconfig.sh
      ```

      If IBM Cognos Configuration does not open, ensure that you set the *DISPLAY* environment variable.

      If you see a `JAVA.Lang.unsatisfied link` message, verify that you are using a supported version of Java.

      If you see a `Java.lang.unsupportedClassVersionError` message, ensure that you are using a 64-bit version of Java.
2. In the **Explorer** window, click **Environment**.
3. In the **Properties** window, under **Gateway Settings**, specify the values for **Dispatcher URIs for the gateway**:
   - Click in the **Value** column.
   - Click the **Edit** button.
   - Change the *localhost* portion of the URI to the name or IP address of an Application Tier Components computer.

     This will ensure that users in different locations can connect to reports and workspaces that are sent by email.

     Tip: If you want to send requests to the dispatcher from a Software Development Kit application or an IBM Cognos Analytics modeling tool that is outside of a network firewall, connect to a dedicated gateway that is configured to connect to the dispatcher using the internal dispatcher URI for your environment (for example, http://localhost:9300/p2pd/servlet/dispatch). For security reasons, the default setting for the Dispatcher URI for gateway property prevents the dispatcher from accepting requests for an Software Development Kit application or modeling tool that is outside the firewall. Ensure that you configure appropriate security for this dedicated gateway, such as SSL (see

"Configuring the SSL protocol for IBM Cognos components" on page 122). Do not change your main gateway to use the internal dispatcher URI. Doing so will reduce the security of the IBM Cognos Analytics portal and studios.

- If you want to add another URI, click **Add** and change the *localhost* portion of the new URI to the name or IP address of another Application Tier Components computer.

  Tip: If you want to use the dispatcher on a standby Content Manager computer, ensure that you add it after you add the Application Tier Components computers. If you add the dispatcher from the active Content Manager computer, ensure that it is last in the list.
- After you specify all the URIs, click **OK**.

4. In the **Explorer** window, under **Security** > **Cryptography**, click **Cognos**, the default cryptographic provider.
5. Under the **Certificate Authority settings** property group, set the **Password** property to match what you configured on the default active Content Manager computer.
6. Ensure that all other cryptographic settings match what you set on the default active Content Manager computer.
7. Test that the symmetric key can be retrieved. In the **Explorer** window, right-click **Cryptography** and click **Test**.

   IBM Cognos Analytics components check the common symmetric keys (CSK) availability.
8. From the **File** menu, click **Save**.

Configure Apache HTTP Server or IBM HTTP Server

This section describes how to configure Apache HTTP Server or IBM HTTP Server as your web server in IBM Cognos Analytics.

Configuring IBM HTTP Server V9

You can use IBM HTTP Server (IHS) V9 web server to support load balancing and failover across multiple IBM Cognos Analytics application servers.

To do that, you must install IHS V9 and the Web Server Plug-ins for IBM WebSphere Application Server V9, and then configure IHS V9 to use the `cognos.conf` file.

For more information about installing the Web Server Plug-ins for IBM WebSphere Application Server V9, see this article (www.ibm.com/support/knowledgecenter/en/SSAW57_9.0.0/com.ibm.websphere.installation.nd.doc/ae/rins_plugins_info.html).

Procedure

1. Install IBM Installation Manager (IIM), preferably version 1.8.5 or later, if you do not already have it installed.

   You can download IIM from this location (www.ibm.com/support/docview.wss?uid=swg24041188).
2. Using IIM, install IBM HTTP Server (IHS) V9 and the Web Server Plug-ins for IBM WebSphere Application Server V9 from Online product repositories for Liberty offerings (www.ibm.com/support/knowledgecenter/SSEQTP_liberty/com.ibm.websphere.wlp.nd.multiplatform.doc/ae/cwlp_ins_repositories.html).

   Ensure that you use the following installation paths:

   - `/opt/IHS90` as the IHS V9 install root
   - `/opt/IHS90Plugin` as the Web Server Plug-ins for IBM WebSphere Application Server install root

     You cannot install the Plug-ins within the IHS V9 install root.

3. Associate the WAS Web Server Plug-ins V9 and IHS V9 by running the following commands:

   ```
   . cd /opt/IHS90
   . bin/simplepct.sh /opt/IHS90Plugin
   ```

   Tip: On UNIX, check the httpd.conf file in your IHS V9 installation after running this command. If you see $PLG_ROOT, replace it with WAS Web Server Plug-ins V9 install root folder, such as /opt/IHS90Plugin.
4. Generate the plugin-cfg.xml file for WAS Web Server Plug-ins. For more information, see "Generating the plugin-cfg.xml for Cognos Analytics servers " on page 71.
5. Copy the plugin-cfg.xml file that was generated in step 4 to the *WAS_Web_Server_Plugins_install_root*/config/webserver1 directory, such as /opt/IHS90Plugin/config/webserver1.

   Tip: On UNIX, ensure that the plugin-cfg.xml file has read and execute permissions after copying the file.
6. Configure the IHS V9 using the following steps:
   a) Access the template file cognos_IHS9_SSO.conf or cognos_IHS9.conf in the *cognos_analytics_gateway_component_install_location*/cgi-bin/templates directory.
   b) Copy the template file to *IHS9_install_root*/conf directory, such as /opt/IHS90/conf, and rename it to cognos.conf. Modify the cognos.conf file to point to the proper installation location.
   c) Configure httpd.conf, as documented in the article Configuring Cognos Analytics with Apache HTTP Server or IBM HTTP Server.
   d) Restart the IHS V9 web server.

Configuring IBM HTTP Server V9 with SSL

If you use Secure Sockets Layer (SSL) on IBM Cognos Analytics with IBM HTTP Server V9 as your web server, you must set up SSL between WAS Web Server Plug-ins and the Cognos Analytics application server by extracting the IBM Cognos certificate and adding it to the WAS Web Server Plug-ins trust store.

If you use SSL on IBM HTTP Server V9, configure your environment as documented in the article "Configuring IBM HTTP Server with SSL" on page 73.

Procedure

1. Start the IBM Cognos Analytics application server that is configured to use SSL.
2. Copy the Server section from the *Cognos_Analytics_applicaton_server_install_root*/wlp/usr/servers/cognosserver/logs/state/plugin-cfg.xml file to the plug-in/config/webserver1/plugin-cfg.xml file. Ensure that the Cognos Analytics https entry point is specified, as shown in the following example:

   ```
   <Server CloneID="a4949c5e-cb36-40dd-9f43-58702daf7b1a" ConnectTimeout="5"
   ExtendedHandshake="false" LoadBalanceWeight="20" MaxConnections="-1"
   Name="default_node_cognosserver" ServerIOTimeout="900" WaitForContinue="false">
      <Transport Hostname="hostname" Port="xxx" Protocol="https">
      <Property Name="keyring" Value="D:\install\IBM\WebSphere\Plugins\config\
            webserver1\plugin-key.kdb"/>
      <Property Name="stashfile" Value="D:\install\IBM\WebSphere\Plugins\config\
            webserver1\plugin-key.sth"/>
      </Transport>
   </Server>
   ```
3. In the Plug-in/config/webserver1/plugin-cfg.xml file, add the following attribute to the Config section:

   ```
   AutoSecurity="false"
   ```
4. Obtain the IBM Cognos certificate by using the following steps:

a) Go to the Cognos Analytics *applicaton_server_install_root*/bin directory.

b) Extract the certificate by typing a command that is appropriate for your operating system.

On UNIX or Linux operating systems, type

```
ThirdPartyCertificateTool.sh -E -T -r destination file -p NoPassWordSet
```

On Windows operating systems, type

```
ThirdPartyCertificateTool.bat -E -T -r destination file -p NoPassWordSet
```

5. Copy the `.cert` file, for example `ca-host1.cert`, that was generated in step 4 to WAS Web Server Plug-ins host.
6. Add the Cognos Analytics `.cert` file to the WAS Web Server Plug-ins key store `plugin-key.kdb`. If the `plugin-key.kdb` file does not exist, create one as described in step 7.

   You can use different methods to add the `.cert` file to the key store. The following steps describe how to do that by using the `gskcapicmd` tool that is shipped with IHS V9.

   a) Go to the IHS9 ROOT folder.

   b) Type a command that is appropriate for your operating system.

   On UNIX or Linux operating systems, type

   ```
   bin/gskcapicmd -cert -add -db WAS_Plugin_root/config/webserver1/plugin-key.kdb
   -stashed -label ca-host1 -file ca-host1.cert
   ```

   On Windows operating systems, type

   ```
   bin\gskcapicmd.bat -cert -add -db WAS_Plugin_root\config\webserver1\plugin-key.kdb
   -stashed -label ca-host1 -file ca-host1.cert
   ```

   For information about other methods of adding certificate files to the key store, search IBM Knowledge Center (www.ibm.com/support/knowledgecenter/SSEP7J_11.0.0).
7. Create an empty key store for WAS Web Server Plug-ins:

   a) Go to the IHS9 ROOT folder.

   b) Type a command that is appropriate for your operating system.

   On UNIX or Linux operating systems, type

   ```
   bin/gskcapicmd -keydb -create -db WAS_Plugin_root/config/webserver1
     /plugin-key.kdb -pw xxx -stash
   ```

   On Windows operating systems, type

   ```
   bin\gskcapicmd.bat -keydb -create -db WAS_Plugin_root\config\webserver1
      \plugin-key.kdb -pw xxx -stash
   ```

Generating the plugin-cfg.xml for Cognos Analytics servers

In an environment with WebSphere Application Server, the `plugin-cfg.xml` file contains configuration information that determines how the web server plug-in forwards requests.

Tip: The following procedure is not applicable to the IBM Cognos Analytics servers that are used to run the Content Manager service.

Procedure

1. Go to the Cognos Analytics application server installation location.

2. Open the *ca_applicaton_server_install_root*/wlp/usr/servers/cognosserver/server.xml file, and add the following setting to the file:

   ```
   <pluginConfiguration pluginInstallRoot="WAS_Web_Server_Plugin_install_root”
   webserverPort="IHS9_port"/>
   ```

   For example:

   ```
   <pluginConfiguration pluginInstallRoot="/opt/IHS90Plugin" webserverPort="8080"/>
   ```

3. Configure and start the Cognos Analytics application server.

   After the server is started, a file named plugin-cfg.xml is generated in the Cognos Analytics *applicaton_server_install_root*/wlp/usr/servers/cognosserver/logs/state directory.

4. Open the plugin-cfg.xml file, and modify the UriGroup section by deleting everything except for the following two elements:

   ```
   <UriGroup Name="default_host_cognosserver_default_node_Cluster_URIs">
       <Uri AffinityCookie="JSESSIONID" AffinityURLIdentifier="jsessionid"
           Name="/bi/*"/>
       <Uri AffinityCookie="JSESSIONID" AffinityURLIdentifier="jsessionid"
           Name="/bi/v1/*"/>
   </UriGroup>
   ```

   Tip: The second URL entry does not exist in the file. You need to add it.

5. Save the plugin-cfg.xml file.

   You just configured one Cognos Analytics application server for the ServerCluster.

6. To add another Cognos Analytics application server to the ServerCluster, perform the following steps:

   a) From the Cognos Analytics *application_server_install_root*/wlp/usr/servers/cognosserver/logs/state directory, open the plugin-cfg.xml file. Copy the Server element under the ServerCluster section. For example, copy the following Server element:

   ```
   <Server CloneID="081cd7c5-bb6c-4a93-a074-33fa07e587f3" ConnectTimeout="5"
   ExtendedHandshake="false" LoadBalanceWeight="20" MaxConnections="-1"
   Name="default_node_cognosserver" ServerIOTimeout="900" WaitForContinue="false">
   <Transport Hostname="caserverhost" Port="9300" Protocol="http"/>
   </Server>
   ```

   b) Paste the Server element to the ServerCluster section in the plugin-cfg.xml file that was generated in step 4. Ensure that the endpoint specified in the Server element is accessible from your web server host.

   c) Change the name of the server by modifying the value of the Name attribute. Ensure that the name is different than other server names in the ServerCluster. For example, change the value from default_node_cognosserver to default_node_cognosserver_1.

   d) Add the new server to the PrimaryServers section, as shown below:

   ```
   <PrimaryServers>
       <Server Name="default_node_cognosserver"/>
       <Server Name="default_node_cognosserver_1"/>
   </PrimaryServers>
   ```

   e) Save the plugin-cfg.xml file. The new server is added to the ServerCluster.

7. To add more servers, repeat step 6.

What to do next

For more information about merging plugin-cfg.xml from multiple standalone WebSphere Liberty Profile servers, see this article (www.ibm.com/support/knowledgecenter/en/SSAW57_9.0.0/com.ibm.websphere.nd.multiplatform.doc/ae/twsv_merge_configfiles.html).

Configuring WebDAV on IBM HTTP Server or Apache HTTP Server

To view and browse images in the Reporting, configure Web Distributed Authoring and Versioning (WebDAV) on your web server. Report authors can browse for images to include in reports in a way that is similar to browsing a file system. On IBM HTTP Server or Apache HTTP Server, you must add directives to your server configuration file, and then configure the directory access.

Procedure

1. In the *webserver_location*/conf directory, open the httpd.conf file in a text editor.
2. Uncomment the directives that load modules/mod_dav.so and modules/mod_dav_fs.so.

```
LoadModule dav_module modules/mod_dav.so
LoadModule dav_fs_module modules/mod_dav_fs.so
```

3. Provide a location for the DAVLockDB directive.

   For example,

   DAVLockDB "*webserver_location*/var/DavLock"

   Ensure that the directory exists.
4. Create an alias for the directory where your images are stored.
5. Add Dav On to the <Directory> information for the alias.

   For example,

```
Alias /images "path/shared_images"

<Directory "path/shared_images">
   Dav On
   Options Indexes MultiViews
   AllowOverride None
   Order allow,deny
   Allow from all
</Directory>
```

6. Save the file.
7. Restart your web server.

Results

With WebDAV enabled, Reporting users can add images to their reports. When users click **Browse** in the image browser, the default location for browsing is http://*servername*/ibmcognos/bi/samples/images. If you created another location, users can enter that location.

Configuring IBM HTTP Server with SSL

If you are using Secure Sockets Layer (SSL) on IBM HTTP Server, you must change the **Gateway URI** values in IBM Cognos Configuration to be able to access the portal.

To enable SSL on your web server, you must obtain a web server certificate signed by a Certificate Authority (CA) and install it into your web server. For more information about using certificates with your web server, see your web server documentation. These certificates are not provided with IBM Cognos products.

To enable users to access the IBM Cognos portal using SSL, you must change the **Gateway URI** values in IBM Cognos Configuration for each computer where the Application Tier Components and Framework Manager are installed.

Before you begin

IBM HTTP Server must have IBM Global Security Kit (GSKit) installed. For more information about the supported versions of GSKit on IBM HTTP Server, see Global Security Kit (GSKit) supported versions for releases of IBM HTTP Server (www.ibm.com/support/docview.wss?rs=177&context=SSEQTJ&uid=swg21173214) on the IBM Support portal.

Procedure

1. On each computer where the Application Tier Components or Framework Manager are installed, start IBM Cognos Configuration.
2. Under **Local Configuration**, click **Environment**, and change the **Gateway URI** value from `http` to `https`.
3. In the **Gateway URI** value, change the port number to the SSL port number defined for your web server.
   For example, the default port number for SSL connections is usually 443.
4. On each computer where the Application Tier Components or Framework Manager are installed, go to the *install_location*`/bin` directory, and import all the certificates that make up the chain of trust, in order starting with the root CA certificate, into the IBM Cognos truststore.

   Import the certificates by typing the following command:

   On UNIX or LINUX, type

   ```
   ThirdPartyCertificateTool.sh -T -i -r path/certificate_fileName -p password
   ```

   On Windows, type

   ```
   ThirdPartyCertificateTool.bat -T -i -r path\certificate_fileName -D
   install_location\configuration\certs -p password
   ```

   Note: If password is not set, the default password is NoPassWordSet.
5. Type the following command from the web server *ihs_install_root*`/bin` directory:

   ```
   ihs_install_root/bin/script_name
   ```

   Where *ihs_install_root* is the directory where IBM HTTP Server is installed and *script_name* is `gskver.bat` for Microsoft Windows or `gskver.sh` for UNIX or Linux.

   The GSKit shared libraries and version information are displayed. Verify that the version displayed is the minimum supported version as shown in the support document mentioned in the *Before you begin* section of this procedure.
6. Start the iKeyman utility by typing the following command:

   ```
   ihs_install_root/bin/script_name
   ```

   Where *ihs_install_root* is the directory where IBM HTTP Server is installed and *script_name* is `ikeyman.bat` for Microsoft Windows or `ikeyman.sh` for UNIX or Linux.
7. From the menu, select **Key Database File** > **New**.
8. Enter the following values and click **OK**:

   File Name
   Name of the key database file. The default value is `key.kdb`.

   Location
   Place to store the `key.kdb` file. The default value is *ihs_install_root*`/bin.`
9. In the **Password Prompt** window, enter a password, select the **Stash a password to a file** check box, and click **OK**.

   When you select the **Stash a password to a file** check box, the password is encrypted and is saved as a `.sth` file in the same directory as the key database file.

   Note: For information about how to create a certificate request to send to a certificate authority, see Using iKeyman to create a key database file (www.ibm.com/support/docview.wss?rs=177&context=SSEQTJ&uid=swg21006430).

   A completed successfully message displays.
10. Open the *ihs_install_root*`/conf/httpd.conf` file in a text editor.

11. Add the `Keyfile` directive with the path to your key database file. Put it after the `VirtualHost` section in the file.
    For example,

    ```
    <VirtualHost *:443>
    ...
    </VirtualHost>
    KeyFile ihs_install_root/key.kdb
    ```

12. Save and close the `httpd.conf` file.
13. Extract the Cognos Analytics certificate to a file. Run the following command from the IBM Cognos Analytics server in *`ca_install`*`/bin`.

    ```
    script_name -E -T -r ca_cert_file -p NoPassWordSet
    ```

    Where *script_name* is `ThirdPartyCertificateTool.bat` for Microsoft Windows or `ThirdPartyCertificateTool.sh` for UNIX or Linux and *ca_cert_file* is the name of the certificate file.
14. Copy the certificate file to *`ihs_install_root`*`/`*`key_database_file_directory`* where *ihs_install_root* is the directory where IBM HTTP Server is installed and *key_database_file_directory* is the directory where the key database file is stored.
15. In *`ihs_install_root`*`/bin`, type the following command:

    ```
    script_name -cert -import -db ca_cert_file
    -pw NoPassWordSet -target key.kdb -target_pw key_database_file_password
    ```

    Where *script_name* is `gskcapicmd.bat` for Microsoft Windows or `gskcapicmd.sh` for UNIX or Linux and *key_database_file_password* is the password for the key database file.
16. Start IBM HTTP Server. Enter the following command in `ihs_install_root/bin`:

    ```
    script_name -k start
    ```

    Where *script_name* is `apchectl.bat` for Microsoft Windows or `./apachectl` for UNIX or Linux. On Microsoft Windows, you can also start the script as a service.
17. Verify that IBM HTTP Server is running by entering the following URI in the address field of a web browser:

    ```
    https://web_server_host_name:port
    ```

    Where *web_server_host_name* is the host name of IBM HTTP Server and *port* is the IBM HTTP Server port number.
18. Save your configuration, and restart your services.

Results

When you access the portal using `https://servername:443/ibmcognos`, you are prompted to install a certificate. To avoid being prompted by a security alert for each new session, install the certificate into one of your web browser's certificate stores.

Configuring Apache HTTP Server or IBM HTTP Server in Cognos Analytics

+

After you complete this procedure, the server can handle requests for static files (such as `.js`, `.html`, `.css`), load balance requests to IBM Cognos Analytics, and route SSO requests through the IBM Cognos Analytics gateway code.

About this task

You can use one of the sample configuration files that are provided with IBM Cognos Analytics. The sample files are in *gateway_component_install_location*`/cgi-bin/templates` where *gateway_component_install_location* is the directory where the gateway component is installed. The following table describes the sample files. Choose the file for your environment:

Environment	Sample file name
Apache 2.2 non-SSO	cognos_apache22_loadbalance.conf
Apache 2.2 SSO	cognos_apache22_loadbalance_SSO.conf
Apache 2.4 non-SSO	cognos_apache24_loadbalance.conf
Apache 2.4 SSO	cognos_apache24_loadbalance_SSO.conf
IBM HTTP Server 8.5 non-SSO	cognos_IHS85_loadbalance.conf
IBM HTTP Server 8.5 SSO	cognos_IHS85_loadbalance_SSO.conf

Procedure

1. Copy the sample configuration file to *apache_or_ihs_install_root*`/conf` and rename it to `cognos.conf`.
2. Open `cognos.conf` in a text editor and change the `BalancerMember` directive to use https and a fully qualified domain name.
   For example,

```
<Proxy balancer://mycluster>
    BalancerMember https://ica-host1.domain:9300 route=1
    BalancerMember https://ica-host2.domain:9300 route=2
</Proxy>
```

3. Ensure that the following section is present in the sample file.

```
# Rewrite Saved-Output and Viewer static references
RewriteRule ^/ibmcognos/bi/rv/(.*)$ /ibmcognos/rv/$1 [PT,L]
```

   If this section is missing, add it after the `# Rewrite Event Studio static references` section.
4. Find the `Directory` section and make sure it is pointing to the IBM Cognos Analytics installation location.
5. Save the `cognos.conf` file.

Configure Microsoft Internet Information Services

This section describes how to configure Microsoft Internet Information Services (IIS) as your web server in IBM Cognos Analytics.

Configuring WebDAV on IIS

To view and browse images in the Reporting, configure Web Distributed Authoring and Versioning (WebDAV) on your web server. Report authors can browse for images to include in reports in a way that is similar to browsing a file system. On Microsoft Internet Information Services (IIS) web servers, you must first enable the WebDAV feature, and then configure your web server to access the image location.

Procedure

1. In the Microsoft Windows **Control Panel**, click **Programs** > **Programs and Features**.

   If you are using Microsoft Windows 8 or 2012 Server, **Programs and Features** is available directly from the **Control Panel**.
2. Click **Turn Windows features on or off**.
3. If you are using Microsoft Windows 2008 Server, use the following steps:
   a) Click **Server Manager** > **Roles** > **Web Server (IIS)**.
   b) In the **Role Services** section, select **Add Role Services**.
   c) Under **Web Server** > **Common HTTP Features**, select **WebDAV Publishing**.
   d) Click **Next**, and then click **Install**.
4. If you are using Microsoft Windows 2012 Server, use the following steps:
   a) In the **Add Roles and Features Wizard**, click **Role-based or feature-based installation**, and click **Next**.
   b) Select your server, and click **Next**.
   c) Expand **Web Server (IIS)** > **Web Server** > **Common HTTP Features**, and select **WebDAV Publishing**.
   d) Click **Next** > **Next**, and then click **Install**.
5. If you are using Microsoft Windows 7 or 8, use the following steps:
   a) Expand **Internet Information Services** > **World Wide Web Services** > **Common HTTP Features**.
   b) Select **WebDAV Publishing**, and click **OK**.
6. In the **Internet Information Services (IIS) Manager** console, under **Connections**, select your server name.
   - If you are using Microsoft Windows 2012 Server, in **Server Manager**, select **IIS**, and then right-click your server name, and click **Internet Information Services (IIS) Manager**.
   - If you are using Microsoft Windows 2008 Server, in **Server Manager**, expand **Roles** > **Web Server (IIS)**, and then click **Internet Information Services (IIS) Manager**.
   - If you are using Microsoft Windows 8, from the**Control Panel**, click **Administrative Tools** to access the **Internet Information Services (IIS) Manager** console.
   - If you are using Microsoft Windows 7, from the**Control Panel**, click **System and Security** > **Administrative Tools** to access the **Internet Information Services (IIS) Manager** console.
7. Under **Connections**, expand your web server, **Sites**, and select your website.
   For example, select **Default Web Site**.
8. Double-click **WebDAV Authoring**.
9. Click **Enable WebDAV**.
10. Click **WebDAV Settings**.
11. If you have anonymous access enabled, select **True** for **Allow Anonymous Property Queries**, and click **Apply**.
12. Select the directory or virtual directory to which you want to allow WebDAV access.
13. Double-click **WebDAV Authoring**.
14. Click **Add Authoring Rule**, and add the appropriate rules for your environment.
    For example, if you installed the samples and you want to use the default path, under the `ibmcognos` virtual directory, expand `bi/samples`, and select `images`, and add an authoring rule for the image files.
15. Right-click the directory or virtual directory you added authoring rules to, and click **Edit Permissions**.
16. Click **Security**, and add the appropriate permissions.

For example, if you allow anonymous access to your web server, add permissions for the anonymous access user. You can find that user by select the website, double-clicking **Authentication**, and viewing the properties for the displayed users.

Results

With WebDAV enabled, Reporting users can add images to their reports. When users click **Browse** in the image browser, the default location for browsing is `http://`*`servername`*`/ibmcognos/bi/samples/images`. If you created another location, users can enter that location.

Configuring IIS with SSL

To configure Microsoft Internet Information Services (IIS) with secure sockets layer (SSL) you extract the IBM Cognos certificate and then add it to the truststore on IIS.

Procedure

1. Go to the *`install_location`*`/bin` directory.
2. Extract the IBM Cognos certificate by typing the following command:

   On UNIX or Linux operating systems, type `ThirdPartyCertificateTool.sh -E -T -r destination_file -p NoPassWordSet`

   On Microsoft Windows operating systems, type `ThirdPartyCertificateTool.bat -E -T -r destination_file -p NoPassWordSet`
3. Perform Copying the CA certificate to IBM Cognos servers.
4. Import the certificate to the truststore on IIS.

   For more information about how to import the certificate to the truststore on IIS, see Adding certificates to the Trusted Root Certification Authorities store for a local computer.

Configuring IIS in Cognos Analytics

Last updated: 2018-12-20

Note:

IIS Automated script is available here.

This topic describes the configuration for Microsoft Internet Information Services (IIS) to support IBM Cognos Analytics. When complete, IIS will be configured to serve static content (such as `.js`, `.html`, `.css`) directly from IIS while sending REST and other server requests to the back-end Cognos Analytics servers.

Procedure

1. Install the IIS Application Request Routing extension.
   a) Install the Application Request Routing extension for IIS by going to the following URL: http://www.iis.net/downloads/microsoft/application-request-routing
   b) When presented with the Microsoft Web Page, click on the green “Install this extension” button.

      Follow instructions to download and run the ARR extension.
   c) To ensure that the ARR extension was installed successfully, launch the IIS Manager from the Windows **Start\Administrative Tools** menu. Once the IIS Manager launches, click on the server name at the top left-hand side of the screen to display the available features. Within the middle IIS pane, the **URL Rewrite** feature should now be visible; it is installed when ARR is installed.
2. Create a new, dedicated application pool. For example, named `CAPool`.
   a) Right-click on **Application Pools**. Click **Add Application Pool**.
3. Optionally, create a server farm to provide load-balancing and failover for Cognos Analytics service requests. Include all Cognos Analytics servers that have the Application server components installed and configured.

a) Right-click on **Server Farms** in the left-hand tree and select **Create Server Farm**.

b) Name the new server farm. For example, `ca_servers`.

c) For each Cognos Analytics server, perform the following steps:

- Enter the server address. For example, `ca-host1`.
- Click **Advanced settings**, and expand **applicationRequestRouting**. Set the `httpPort` or `httpsPort` (if you're using HTTPS). For example, `9300`.

d) Click **Finish**.

e) Click **No** when prompted to allow IIS Manager to create a rewrite rule.

f) Select your server farm in the left-hand tree and double-click **Server Affinity**.

g) Select the **Client Affinity** check box.

h) Click **Apply**.

i) Select your server farm in the left-hand tree and double-click **Caching**.

j) Change **Query String Support** to **Include Query String**.

k) Click **Apply**.

l) Select your server farm in the left-hand tree and double-click **Health Test**.

m) In the **URL Test** section, enter the URL: `http://ca_servers/bi/v1/ping`

n) Click **Apply**.

o) Select your server farm in the left-hand tree and double-click **Proxy**.

p) In the **Time-out (seconds)** field, change the value to `120`.

q) Click **Apply**.

4. Right-click **Default Web Site** and then click **Add Application**.

- Alias is `ibmcognos`.
- Application pool is the one created in step 1.
- Physical path is *`install_location`*`\webcontent`

a) Enable Web Content expiry

1) Select `ibmcognos` and double-click **HTTP Response Headers**.

2) Click **Set Common Headers**.

3) Check **Expire Web Content** and set an expiry that works best for you.

b) Select `ibmcognos` and double-click **Mime Types**.

Important: Add the following mime types to your IIS configuration if they are not already present.

- `.svg : image/svg+xml`
- `.woff : application/x-font-woff`
- `.json : application/json`
- `.woff2 : font/woff2`
- `.template : text/html`
- `.txt : text/plain`

5. If you are configuring single sign-on between IIS and Cognos, right-click `ibmcognos` and click **Add Application**.

- **Alias** to `sso`.
- **Application pool** is the one you created in step 1.
- **Physical path** is *`install_location`*`\cgi-bin`

a) Select **sso** and double-click **Handler Mappings**.

b) Click **Add Module Mapping** in the right **Actions** pane.

- Request path is cisapi.
- Module is **IsapiModule**.
- Executable is install_location\cgi-bin\cognosisapi.dll
- Name is Cognos SSO.
- Click **Request Restrictions** and ensure that **Invoke Handler** is unchecked.
- Click **OK** twice.
- On the **Edit Script Map** dialog, click **Yes**.
- Select **sso** and double-click **Modules**. If the WebDAVModule appears in the list, remove it.

6. Create URL-rewrite rules to map requests to the correct handlers.

   a) Click on bi directory under **ibmcognos**.

   b) Double-click **URL Rewrite**.

   c) Add a server variable to identify the Cognos Analytics location by clicking **View Server Variables**.

   - Click **Add**.
   - Name the variable HTTP_X_BI_PATH.
   - Click **Back to Rules**.
   - Click **Add**.
   - Name the variable HTTP_X_WEBCONTENTROOT
   - Click **Back to Rules**.
   - Click **Add**.
   - Name the variable HTTP_X_FORWARDED_HOST.
   - Click **Back to Rules**.

   d) Add a rule to pass the Cognos Analytics location to the ca-host machines by clicking **Add Rules** > **Inbound Rules** > **Blank Rule**.

   - Name is Headers.
   - Pattern is (.*)
   - Action type is **none**.
   - Expand **Server variables** and
     - Click **Add**. Select HTTP_X_BI_PATH and set the value to /ibmcognos/bi/v1.
     - Click **Add**. Select HTTP_X_FORWARDED_HOST and set the value to {HTTP_HOST}.
     - Click **Add**. Select HTTP_X_WEBCONTENTROOT and set the value to /ibmcognos.
   - Clear **Stop processing of subsequent rules**.
   - Click **Apply** and **Back to Rules**.

   e) If you configured the SSO application in a previous step, add rules to map login and legacy UI service requests to the SSO handler.

   1) Click **Add Rules** > **Inbound Rules** > **Blank Rule**.

      - Name is SSO Login.
      - Pattern is v1/login$
      - Action type is **Rewrite**.
      - Rewrite URL is /ibmcognos/sso/cisapi/bi/v1/login
      - Check **Stop processing of subsequent rules**.
      - Click **Apply** and **Back to Rules**.

   2) Click **Add Rules** > **Inbound Rules** > **Blank Rule**.

      - Name is Legacy SSO.

- Pattern is `(v1/disp(/.*)?)`
- Action type is **Rewrite**
- Rewrite URL is `/ibmcognos/sso/cisapi/bi/{R:1}`
- Check **Stop processing of subsequent rules**.
- Click **Apply** and **Back to Rules**.

f) Add a rule to map Cognos Analytics REST service requests to the backend Cognos Analytics servers.

1) Click **Add Rules** > **Inbound and Outbound Rules** > **Reverse Proxy** .

   - If proxies are not already enabled, you are prompted to enable. Click **OK**.
   - Server name is `ca-host:9300/bi`

     or if you have configured a server farm, `http://ca_servers/bi`

   Select the newly created rule and click **Edit**.

   - Pattern is `(^$)|(^v1(/.*)?)|(^[^/]+\.jsp)`
   - Action type is **Rewrite**.
   - Rewrite URL is `http://ca-host:9300/bi/{R:0}`

     or if you have configured a server farm, `http://ca_servers/bi/{R:0}`
   - Check **Stop processing of subsequent rules**.
   - Click **Apply** and **Back to Rules**.

2) Click **Add Rules** > **Inbound Rules** > **Blank Rule**.

   - Name is `Event Studio`.
   - Pattern is `^(ags|cr1|prompting|ccl|common|skins|ps)/(.*)`
   - Open the **Conditions** section.
   - Change the **Logical Grouping** to **Match Any**
   - Click **Add**.
     - **Condition input** is `{HTTP_REFERER}`
     - **Check if input string** is `Matches the Pattern`
     - Pattern is `v1/disp`
     - Check **Ignore case**.
   - Click **Add**
     - **Condition input** is `{HTTP_REFERER}`
     - **Check if input string** is `Matches the Pattern`
     - Pattern is `(ags|cr1|prompting|ccl|common|skins|ps)/(.*)\.css`
     - Check **Ignore case**.
   - Action type is **Rewrite**
   - Rewrite URL is `/ibmcognos/{R:0}`
   - Check **Stop processing of subsequent rules**.
   - Click **Apply** and **Back to Rules**.

3) Click **Add Rules** > **Inbound Rules** > **Blank Rule**

   - Name is `Report Viewer`
   - Pattern is `^rv/(.*)`
   - Action type is **Rewrite**
   - Rewrite URL is `/ibmcognos/{R:0}`

- Check **Stop processing of subsequent rules**.
- Click **Apply** and **Back to Rules**.

7. Adjust request size limits.
   a) Select the `bi` directory under the **ibmcognos** application created earlier.
   b) Double-click **Request Filtering**.
   c) Click **Edit Feature Settings...** from the right-hand panel.
      - Set **Maximum URL length (bytes)** to 8192.
      - Set **Maximum query string (bytes)** to 8192.
      - Click **OK**.
   d) Double-click **Request Filtering**.
   e) Select **Headers** tab and click **Add Header**.
   f) In **Header Box**, type the header field name as `Referer`.
   g) In the **Size Limit** box, type 8192.
   h) Click **OK**.
   i) Repeat process for a header field name entitled `Cookie` with the **Size Limit** of `4096.`
   j) Click **OK**.
   k) Click the **ibmcognos** virtual directory.
   l) In the **Home** view, **Management** section, double-click **Configuration Editor**.
   m) In the **Section** drop-down list, expand **system.web**, and select **httpRuntime**.
   n) Set the property **maxQueryStringLength** to 8192.
   o) Apply the configuration change.
8. Configure IIS to allow to pass through the custom 441 errors that are used for recoverable exceptions from CAM. Otherwise, IIS can block these errors, and the customer sees the "Invalid Logon Response" error when trying to log on.
   a) Click the `ibmcognos` virtual directory.
   b) In the Home view, **Management** section, double-click **Configuration Editor**.
   c) In the **Section** drop-down list, expand **system.webServer**, and select **httpErrors**.
   d) Set the **existingResponse** property to **PassThrough**.
   e) Apply the configuration change.
9. If you configured the SSO application in previous steps, enable **Windows Authentication**.
   a) Select the SSO application. For Microsoft Edge browser, select the `ibmcognos` application.
   b) Double-click **Authentication**. Disable **Anonymous Authentication**, and enable **Windows Authentication**.

   Cognos Analytics should now be available at: `http://iis-host/ibmcognos`.

   Note: If you configured a multi level virtual directory folder above the ibmcognos application, e.g. Default Web Site > MyVirtualDirectoryFolder > ibmcognos , use /MyVirtualDirectoryFolder/ibmcognos instead of /ibmcognos in the URL-rewrite rules you created in Step 6.

Configuring the CGI gateway on IIS version 7 or 8

If you are using Microsoft Internet Information Services (IIS) version 7 or later, configure the CGI gateway. This is required for single sign-on.

The CGI gateway is available for 32-bit and 64-bit web servers.

About this task

If you are using Microsoft IIS as your web server and you plan to run more than one IBM Cognos Analytics product, or several instances of the same product, on one computer, you must create a separate application pool for each product or instance and then associate the aliases for that product or instance to the application pool.

For more information about creating an application pool, see your web server documentation.

Procedure

1. In the Microsoft Windows **Control Panel**, click **Programs** > **Programs and Features**.

   If you are using Microsoft Windows 8 or 2012 Server, **Programs and Features** is available directly from the **Control Panel**.
2. Click **Turn Windows features on or off**.
3. If you are using Microsoft Windows 2008 Server, use the following steps:
   a) Click **Server Manager** > **Roles** > **Web Server (IIS)**.
   b) Ensure that **Common HTTP Features**, or the features you require are enabled.
   c) If **CGI** is set to **Not installed**, select **CGI** and click **Add Role Service**.
4. If you are using Microsoft Windows 2012 Server, use the following steps:
   a) In the Add Roles and Features Wizard, click **Role-based or feature-based installation**, and click **Next**.
   b) Select your server, and click **Next**.
   c) Select **Web Server (IIS)**, if it is not already installed, ensure that **Common HTTP Features** is selected, and click **Next** until you get to the **Role Services** section of the wizard.
   d) Expand **Application Development**.
   e) Select **CGI** if it is not already selected, and click **Next**.
   f) Click **Install**.
5. If you are using Microsoft Windows 7 or 8, use the following steps:
   a) Select **Internet Information Services** if it is not already selected.
   b) Expand **Internet Information Services** > **World Wide Web Services**.
   c) Ensure that **Common HTTP Features**, or the features you require are enabled.
   d) Expand **Application Development Features**.
   e) If **CGI** is not selected, select **CGI**.
   f) Click **OK**.
6. In the **Internet Information Services (IIS) Manager** console, under **Connections**, select your server name.
   - If you are using Microsoft Windows 2012 Server, in **Server Manager**, select **IIS**, and then right-click your server name, and click **Internet Information Services (IIS) Manager**.
   - If you are using Microsoft Windows 2008 Server, in **Server Manager**, expand **Roles** > **Web Server (IIS)**, and then click **Internet Information Services (IIS) Manager**.
   - If you are using Microsoft Windows 8, from the **Control Panel**, click **Administrative Tools** to access the **Internet Information Services (IIS) Manager** console.
   - If you are using Microsoft Windows 7, from the **Control Panel**, click **System and Security** > **Administrative Tools** to access the **Internet Information Services (IIS) Manager** console.
7. Double-click **ISAPI and CGI Restrictions**.
8. Under **Actions**, click **Add**.
9. Enter the path to the `cognos.cgi` file. The file is in the *`install_location`*`\cgi-bin` directory.

   You must enter the full path, including the file name. If the path includes spaces, ensure you use quotation marks around the path. For example, enter:

   ```
   "C:\Program Files\ibm\cognos\analytics\cgi-bin\cognos.cgi"
   ```
10. Enter a **Description**, such as `CognosCGI`.

11. Select **Allow extension path to execute**, and click **OK**.
12. Under **Connections**, expand **Sites**, and under your website, add the virtual directories as shown in the table:

Table 9: Required virtual directories

Alias	**Location**
ibmcognos	`install_location/webcontent`
ibmcognos/cgi-bin	`install_location/cgi-bin`

Important: `bi` is the default value that is used in the **Gateway URI** and **Controller URI for gateway** values in IBM Cognos Configuration. If you do not use `bi` for the Alias values, ensure that you change the **Gateway URI** and **Controller URI for gateway** values to match the values you use.

13. Select the cgi-bin virtual directory that you created.
14. Double-click **Handler Mappings**.
15. Under **Actions**, click **Add Module Mapping**.
    a) In **Request Path**, type `cognos.cgi`.
    b) In **Module**, select `CgiModule`.
    c) Leave **Executable (optional)** blank.
    d) In **Name**, enter a name for the entry, such as `CognosCGI`.
    e) Click **OK**.
16. Configure the reverse proxy.

This procedure provides the steps required to setup the reverse proxy to allow IIS to rewrite the gateway requests and pass them to the application tier. These steps assume a two server architecture where the IBM Cognos Analytics gateway is installed on `Server1_Gateway` and the IBM Cognos Analytics application is installed on `Server2_Application`

a) On the `Server1_Gateway` server, launch IIS Manager and select the "**bi**" folder in the `ibmcognos` virtual directory set up previously.
b) In the features view, start the **URL Rewrite** feature.
c) Within the **Actions** pane, click on **Add Rule(s)**, and then select **Reverse Proxy**. Click **OK**.
d) In the **Add Reverse Proxy Rule** dialog box, within the **Inbound Rules** section, fill in the **Enter the server name or the IP address...** field in the following format. `<Server2_Application:Port>/bi`. For example, `Server2_Application:9300/bi`
e) Ensure the **Enable SSL Offloading** check box is checked, and then click **OK**.
f) On the **Rules** page, in the **Action** pane, click on **View Server Variables**.
g) Click **Add** and add a variable named HTTP_X_BI_PATH. Once completed, click **OK** to create the variable.
h) Within the **Actions** pane, click **Back to Rules**.
i) Select the previously created rule and in the **Inbound rules** pane on the right hand side, click **Edit...**
j) Expand the **Server Variables** section.
k) Inside the **Server Variables** section, click the **Add** button.
l) In the **Set Server Variable** dialog, select the **HTTP_X_BI_PATH** server variable and set the **Value** field to `/ibmcognos/bi/v1`
m) Ensure the **Replace existing value** check box is checked.
n) Click **OK** to save, and then, in the **Action** pane, click **Apply**.
o) In the **Action** pane on the upper right, click **Back to Rules** to finish defining the rule.

p) Test the configuration by entering the following URL pattern using a browser: `http(s)://<web_server>:<web_server_port>/<alias>/bi/`. For this example the URL would be: `http://Server1_Gateway:80/ibmcognos/bi/`.

Results

Users can access the CGI gateway by entering `http://servername/ibmcognos/bi/` in their web browsers.

Testing the gateway

You can test the installation using a web browser.

Procedure

1. Ensure that your web server is running.
2. Open a web browser.
3. In the address field, type the **Gateway URI** from IBM Cognos Configuration. For example,

   `http://host_name:port/ibmcognos`

   The **Welcome** page of the IBM Cognos Analytics portal appears.

Chapter 5. Configuring optional modeling components

After you install and configure IBM Cognos Analytics server components, you can install and configure IBM Cognos Framework Manager, the modeling component for reporting, and IBM Cognos Transformer, the modeling tool for creating PowerCubes.

Install Framework Manager and Transformer to a different location than Cognos Analytics.

IBM Cognos Framework Manager

IBM Cognos Framework Manager is the metadata modeling tool for IBM Cognos Analytics.

You can install it on the same computer as other IBM Cognos Analytics components, or on a different computer.

If you upgraded from an older version of Framework Manager, you can use the same models and projects that you used with the older version. To upgrade existing projects, you must open them in the new version of Framework Manager.

If you are upgrading Framework Manager from an older version, you must first uninstall the older version of Framework Manager. For more information, see Chapter 10, "Uninstalling IBM Cognos Analytics," on page 211.

Before you install Framework Manager, close all programs that are currently running to ensure that the installation program copies all the required files to your computer.

Also, ensure that you have administrator privileges for the Windows computer you are installing on. If you are not an administrator, ask your system administrator to add you to the Administrator group on your computer. Administrator privileges are also required for the account that is used to run Framework Manager.

Install and configure all IBM Cognos Analytics server components before you install Framework Manager.

Install to a directory that contains only ASCII characters in the path name. Some servers do not support non-ASCII characters in directory names. Installing Framework Manager in directory that has an apostrophe in the path name can result in the help not opening properly.

To help you manage, share, and secure different versions of your metadata, you can configure Framework Manager to use an external source control system. For more information, see the section about using external repository control in the *IBM Cognos Framework Manager User Guide*.

System requirements for IBM Cognos Framework Manager

Before you install IBM Cognos Framework Manager, ensure that the Windows computer meets IBM Cognos Analytics software and hardware requirements. The size of your models determines the hardware requirements, such as disk space.

The following table lists the minimum hardware and software requirements to run Framework Manager.

Table 10: System requirement for Framework Manager

Requirement	Specification
Operating system	Windows

Table 10: System requirement for Framework Manager (continued)

Requirement	Specification
RAM	Minimum: 512 MB Optimal: 1 GB
Disk space	Minimum: 500 MB of free space on the drive that contains the temporary directory that is used by IBM Cognos Analytics
Database	Database client software must be installed on the same computer as Framework Manager if you are using compatible query mode Database connectivity set up
Other	Microsoft Data Access Component (MDAC) 2.6 or later for use with product samples

To help you manage, share, and secure different versions of your metadata, you can configure Framework Manager to use an external source control system. For more information, see the section about using external repository control in the Framework Manager *User Guide*.

Installing IBM Cognos Framework Manager

For a complete installation of IBM Cognos Analytics, you must install Cognos Framework Manager on a Windows computer.

The installation location must be different than the IBM Cognos Analytics installation location.

Procedure

1. Go to the location where the installation files were downloaded and extracted, and double-click the `installer.exe` file.
2. Point to appropriate repository and select **IBM Cognos Analytics Tools** and select **IBM Cognos Framework Manager**.
3. Select the language to use for the installation.

   The language that you select determines the language of the user interface. All supported languages are installed. You can change the user interface to any of the installed languages after installation.
4. Follow the directions in the installation wizard to copy the required files to your computer.
5. Secure the installation directory from unauthorized access.

What to do next

Default settings are used for the configuration. You can change these default settings during the installation or later, to better suit your environment.

Configuring IBM Cognos Framework Manager

You must configure IBM Cognos Framework Manager to communicate with IBM Cognos Analytics and its components.

Before you begin

Install and configure IBM Cognos Analytics before you configure Framework Manager. You must first install and configure Content Manager, and start the **IBM Cognos** service on at least one Content Manager computer. This ensures that the certificate authority service issues a certificate to the Framework Manager computer.

You also need to configure the data sources that you plan to use in Framework Manager projects.

About this task

If you install Framework Manager on the same computer as IBM Cognos Analytics (to a different directory), configuration is not required if the following conditions apply:

- Web server is configured to use the default virtual directories.
- Default ports, resources, and cryptographic settings are used.

When Framework Manager is installed outside the network firewall that protects the application tier components, communication issues with the dispatcher can arise. To avoid such issues, you can either install Framework Manager with the application tier components or install and configure a gateway that is dedicated to Framework Manager - dispatcher communications. For more information, see "Configuring Framework Manager inside the network firewall" on page 89 or "Configuring Framework Manager outside the network firewall" on page 90.

Procedure

1. On the computer where you installed Framework Manager, start IBM Cognos Configuration.
2. In the **Explorer** pane, click **Environment**.
3. Specify appropriate values for the following settings:

   Gateway URI

   Default: `http://`*`ca_server`*`:`*`port`*`/bi/v1/disp`

   Example: `http://my_ca_server:`*`9300`*`/bi/v1/disp`

   This URI must always be the same as for Cognos Analytics.

   If the URI contains **localhost**, replace **localhost** with a fully-qualified host name or IP address.

   Dispatcher URI for external applications

   Default: `http://`*`ca_server`*`:`*`port`*`/p2pd/servlet/dispatch`

   Example: `http://my_ca_server:9300/p2pd/servlet/dispatch`

   If the URI contains **localhost**, replace **localhost** with a fully-qualified host name or IP address.
4. From the **File** menu, click **Save**.

Results

Framework Manager is configured to communicate with IBM Cognos Analytics.

Configuring Framework Manager inside the network firewall

Use the following steps to set up communication between Framework Manager and IBM Cognos Analytics components when Framework Manager is installed inside a network firewall.

Procedure

1. On the computer where you installed Framework Manager, start IBM Cognos Configuration.
2. In the **Explorer** window, click **Environment**.
3. In the **Properties** window, for the **Gateway URI**, type the appropriate value.

   Use the HTTPS or HTTP protocol to select SSL or non-SMS communication.
4. Change the host name portion of the **Gateway URI** from localhost to either the IP address or the host name of the computer where the Gateway component is installed.
5. Specify the value for the **Dispatcher URI for external applications** by typing the URI of the server where Application Tier Components are installed.

   This value is the same as the **Internal dispatcher URI** property on your Application Tier Components computer.
6. In the **Explorer** window, under **Cryptography**, click **Cognos**, the default cryptographic provider.

7. Under the **Certificate Authority settings** property group, for the **Password** property, type the same password that you configured on the default active Content Manager computer.
8. From the **File** menu, click **Save**.

Configuring Framework Manager outside the network firewall
When Framework Manager is installed outside the network firewall, you can install and configure a gateway that is dedicated to communications with the dispatcher.

Procedure

1. Set up a dedicated gateway for Framework Manager.
2. On the gateway computer, open IBM Cognos Configuration, and change the property **Dispatcher URIs for gateway** to the URI that is specified for **Internal dispatcher URI** on your application tier components computer.
3. On the Framework Manager computer, start IBM Cognos Configuration.
4. In the **Explorer** window, click **Environment**.
5. In the **Properties** window, for **Gateway URI**, type the appropriate value for the server that you are using as the dedicated gateway.
   - If your web server is configured for the ISAPI gateway, replace `cognos.cgi` with `cognosisapi.dll`.
   - If your web server is configured to use Apache modules, use the following syntax:

     `http://`*`host_name:port`*`/ibmcognos/cgi-bin/`*`module_alias`*
6. Change the localhost portion of the **Gateway URI** to either the IP address or the host name of the dedicated gateway server.
7. For the **Dispatcher URI for external applications**, type the URI that is specified for **Internal dispatcher URI** on the server where application tier components are installed.
8. In the **Explorer** window, under **Cryptography**, click **Cognos**, the default cryptographic provider.
9. Under the **Certificate Authority settings** property group, for the **Password** property, type the same password that you configured on the default active Content Manager computer.
10. From the **File** menu, click **Save**.

Results
Framework Manager is configured to communicate with IBM Cognos Analytics and its components.

Setting variables for data source connections for Framework Manager

The IBM Cognos Analytics modeling tools create and manage metadata. Framework Manager creates and manages metadata for the reporting functions. Because metadata is derived from data sources in multi-platform or multilingual environments, there are several things you must think about or do when you set up the data source environment for Framework Manager. Commonly, these things depend on the other technology you use for your data or import source.

If you upgraded from an older version of Framework Manager, you are not required to set up anything in the data source environment. You must set up the data source environment only if you installed Framework Manager in a different location from the older version.

Users operating in different languages can connect to an MSAS 2005 data source from the same instance of IBM Cognos Analytics. Modelers must create a separate package for each language. Users can run reports in any language.

For more information about data source connections, see the IBM Cognos *Administration and Security Guide*.

Ensure that you install the appropriate fonts to support the character sets and currency symbols you use. For Japanese and Korean currency symbols to appear correctly, you must install the additional fonts from the Supplementary Language Documentation disk.

Perform the following steps in the location where you installed Framework Manager.

Procedure

1. Set the environment variable for multilingual support:

   - For Oracle, set the NLS_LANG (National Language Support) environment variable on each computer where Framework Manager and IBM Cognos Analytics server are installed by typing the following command:

     ```
     NLS_LANG = language_territory.character_set
     ```

     Examples are:

     ```
     NLS_LANG = AMERICAN_AMERICA.UTF8
     ```

     ```
     NLS_LANG = JAPANESE_JAPAN.UTF8
     ```

     The value of the variable determines the locale-dependent behavior of IBM Cognos Analytics. Error messages, sort order, date, time, monetary, numeric, and calendar conventions automatically adapt to the native language and locale.

   - For IBM Db2, set the DB2CODEPAGE environment variable to a value of 1252.

     For more information about whether to use this optional environment variable, see the Db2 documentation.

   No settings are required for SAP BW. SAP support only a single code page on non-Unicode SAP BW systems.

2. For Oracle, add `$ORACLE_HOME/lib` to your LD_LIBRARY_PATH variable.

   When you set the load library paths, ensure that the 32-bit Oracle libraries are in the library search path, which is usually the `$ORACLE_HOME/lib` directory or the `$ORACLE_HOME/lib32` directory if you installed a 64-bit Oracle client.

3. For SAP BW, configure the following authorization objects so that the modeling tool can retrieve metadata.

   Where default values are specified, you may want to modify the values on the SAP system.

   - S_RFC

     Set the **Activity** field to 16.

     Set the **Name of RFC to be protected** field to SYST, RSOB, SUGU, RFC1, RS_UNIFICATION, RSAB, SDTX, SU_USER.

     Set the **Type of RFC** object to be protected field to FUGR.

   - S_TABU_DIS

     Set the **Activity** field to 03.

     Set the **Authorization Group** field to &NC&.

     Note: &NC& represents any table that does not have an authorization group. For security reasons, create an authorization group and assign the table RSHIEDIR to it. The new authorization group restricts the user's access to the table only, which is needed by the modeling tool. Create the authorization group as a customization in the SAP system.

   - S_USER_GRP

     Set the **Activity** field to 03, 05.

     Set the **User group in user master main** field to the default value.

   - S_RS_COMP

     Set the **Activity** field to the default value.

     Set the **Info Area** field to *InfoArea Technical Name*.

Set the **Info Cube** field to the value: *InfoCube Technical Name*.

Set the **Name (ID) of reporting components** field to the default value.

Set the **Type of reporting components** field to the default value.

- S_RS_COMP1

  Set the **Activity** field to the default value.

  Set the **Name (ID) of reporting components** field to the default value.

  Set the **Type of reporting components** field to the default value.

  Set the **Owner (Person Responsible)** field to the default value.

- S_RS_HIER

  Set the **Activity** field to 71.

  Set the **Hierarchy Name** field to *Hierarchy Name*.

  Set the **InfoObject** field to *InfoObject Technical Name*.

  Set the **Version** field to *Hierarchy Version*.

- S_RS_ICUBE

  Set the **Activity** field to 03.

  Set the **InfoCube sub-object** field to the values DATA and DEFINITION.

  Set the **Info Area** field to *InfoArea Technical Name*.

  Set the **InfoCube** field to *InfoCube Technical Name*.

For more information about SAP BW authorization objects, see Transaction SU03.

Testing the Framework Manager installation

You can test your configuration by starting the application and creating a project.

Procedure

To start Framework Manager, from the **Start** menu, click **All Programs** > **IBM Cognos Framework Manager** > .

On Microsoft Windows 8 or Windows 2012 Server, double-click the **Framework Manager** icon on the **Start** panel.

You may be prompted to upgrade if the model schema version is older than the currently supported version.

If you see the **Welcome** page of Framework Manager, your installation is working.

Chapter 6. Configuration options

After you install and configure IBM Cognos components, you can change the configuration for your environment. Initially, default property settings are used to configure the components. However, you can change these default settings if existing conditions make the default choices inappropriate, or to better suit your environment.

For example, you can configure features for IBM Cognos Application Firewall or specify the amount of resources that IBM Cognos components use. Also, you can deliver IBM Cognos content using another portal by configuring Portal Services.

You can configure IBM Cognos components to use other resources, such as using an authentication provider and then enabling single signon for the database connection and the users.

If you use a load-balancing scheme in your environment, you can change settings to improve performance. For example, you can balance requests among dispatchers by changing their processing capacity or by setting the minimum and maximum number of processes and connections. For more information about tuning server performance, see the *Administration and Security Guide*.

For all Microsoft Windows operating system and most UNIX and Linux operating system installations, use IBM Cognos Configuration to configure your settings. However, if the console attached to the UNIX or Linux computer on which you are installing IBM Cognos components does not support a Java-based graphical user interface you must manually edit the `cogstartup.xml` file in the `*install_location*/configuration` directory, and then run IBM Cognos Configuration in silent mode.

Use these optional configuration tasks to customize your configuration so that IBM Cognos components easily integrate into your existing environment.

Changing the version of Java used by IBM Cognos Analytics components

IBM Cognos Analytics components require a Java Runtime Environment (JRE) to operate.

You can change the Java version in situations where you want to use IBMCognos Analytics components with an application server that requires a specific JRE version or you already use a JRE version with other applications. You change Java versions by setting the JAVA_HOME environment variable.

JAVA_HOME

Set a JAVA_HOME environment variable if you want to use your own Java.

Ensure that the JRE version is supported by IBM Cognos products.

On Microsoft Windows operating systems, if you do not have a JAVA_HOME variable, the JRE files that are provided with the installation are used.

To verify that your JRE is supported, see the IBM Software Product Compatibility Reports page (www.ibm.com/support/docview.wss?uid=swg27047186).

Unrestricted JCE Policy File

JREs include a restricted policy file that limits you to certain cryptographic algorithms and cipher suites. If you require a wider range of cryptographic algorithms and cipher suites than are shown in IBM Cognos Configuration, you can download and install the unrestricted JCE policy file.

For Java that is provided by IBM, the unrestricted JCE policy file is available on the IBM website (www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=jcesdk).

Steps

1. Launch Cognos Configuration.

2. Click **File** > **Export As...** and export the configuration to a text file such as `export_cogstartup.xml` in the `configuration` folder. Exit Cognos Configuration.
3. Backup the following files and folders:
   - **Files**
   - *install_location/configuration/cogstartup.xml*
   - *install_location/configuration/caSerial*
   - **Folders**
   - *install_location/configuration/csk*
   - *install_location/configuration/certs*
4. Remove the folders and files you backed up, **except** the folder `install_location/configuration/certs/mobile`. Remove all of the other files in the `install_location/configuration/certs` folder.
5. Rename the configuration backup file you created in **step 2** to `cogstartup.xml`.
6. Set the JAVA_HOME system environment variable to the JRE you want to use. Make sure this JRE has bcprov ready in the `jre/lib/ext folder`.
7. Launch Cognos Configuration, save the configuration, and restart the server. As an alternative, use the command line from the `install_location/bin64` folder, and run this command: `cogconfig.bat -s`.

   This will regenerate the keys for the new JRE.

Changing Default Configuration Settings

When you install IBM Cognos components, the installation uses default configuration settings. If you have any reason not to use these default values, such as a port is being used by another process, use IBM Cognos Configuration to change the value.

If you change the value of a property, you must save the configuration and then restart the IBM Cognos service to apply the new settings to your computer.

For distributed installations, ensure that you configured all computers where you installed Content Manager before you change default configuration settings on other IBM Cognos computers. For example, you can

- change a URI
- manage the configuration group
- manage the configuration server
- configure cryptographic settings
- configure IBM Cognos components to use IBM Cognos Application Firewall
- configure temporary file properties
- configure the gateway to use a namespace
- enable and disable services
- configure fonts
- change the default font for reports
- save report output to a file system
- change the location of map charts for Reporting
- change the notification database

After you change the default behavior of IBM Cognos components to better suit your IBM Cognos environment, you can , configure an authentication provider, and install and configure Framework Manager.

Port and URI settings

You can change certain elements in a URI depending on your environment. An IBM Cognos URI contains the following elements:

Additional information about ports is available in the topic Review the default port settings

- For a Content Manager URI, Dispatcher URI for external applications, or dispatcher URI

  `protocol://host_name_or_IP:port/context_root/alias_path`
- For a Gateway URI or a Web content URI

  `protocol://host_name_or_IP:port/virtual_directory/gateway_application`

  or

  `protocol://host_name_or_IP:port/context_root/alias_path`

  Important: For HTTPS/SSL configurations, make sure to use fully qualified hostname for URIs.

  The elements are described in the following table:

Table 11: IBM Cognos URI elements and descriptions

Element	Description
protocol	Specifies the protocol used to request and transmit information, either Hyper Text Transfer Protocol or Hyper Text Transfer Protocol (Secure). **Example:** http or https
host name or IP	Specifies the identity of the host on the network. You can use an IP address, a computer name, or a fully qualified domain name. In a distributed installation, you must change the localhost element of a URI. In a mixed environment of UNIX and Microsoft Windows operating system servers, ensure that host names can be resolved to IP addresses by all servers in the environment. **Example:** localhost or 192.168.0.1 or [2001:0db8:0000:0000:0000:148:57ab]:80
port	Specifies the port on which the host system listens for requests. The default port for the IBM Cognos Analytics services is 9300. The default port for a web server is 80. **Example:** 9300 or 80
context root	Used by the application server to determine the context of the application so that the request can be routed to the correct Web application for processing. **Example:** p2pd
alias path	Used by the application server to route a request to the correct component within a Web application. The alias path must not be modified or IBM Cognos components will not function properly. **Example:** servlet/dispatch

Table 11: IBM Cognos URI elements and descriptions (continued)

Element	Description
virtual directory	Used by the Web server to map a virtual directory or alias to a physical location. For example, in the default Gateway URI of http://localhost:80/ibmcognos/bi/v1/disp, the virtual directory is ibmcognos/cgi-bin. **Example:** ibmcognos/
gateway application	Specifies the name of the Cognos gateway application that is used. For example, if you are accessing IBM Cognos components using a Common Gateway Interface (CGI), then the default gateway application would be cognos.cgi. **Example:** cognos.cgi

If you are using collaboration with IBM Connections, ensure that you include the full domain for all hostname entries in IBM Cognos Configuration. For example, if your computer is named MyComputer and your domain is **MyCompanyName.com**, then for the host_name_or_IP value, use **MyComputer.MyCompanyName.com**. The domain must be included in order for IBM Connections to allow access.

Changing a port or URI setting
Use the following procedure to change URI properties in IBM Cognos Configuration.

Procedure

1. Start IBM Cognos Configuration.
2. In the **Explorer** window, click the appropriate group or component:
   - To change an element for the dispatcher, click **Environment**.
   - To change an element for the local log server, under **Environment**, click **Logging**.
3. In the **Properties** window, click the **Value** box next to the URI property that you want to change.
4. Select the element and type the new information.
   - To change the port used by the local dispatcher, change the value of the internal dispatcher URI property. Because the change affects all the URIs that are based on the local dispatcher, you must change the URIs of all local components.
   - If you change the dispatcher port in the dispatcher URI, ensure that you specify the new port number when you configure remote computers that use the dispatcher, Content Manager, or Software Development Kit services on this system.
   - For HTTPS/SSL configurations, make sure to use fully qualified hostname for URIs.
5. From the **File** menu, click **Save**.

Verifying the Configuration Settings

Use this feature to verify settings in Cognos Configuration and avoid conflicts.

Procedure

1. Start **Cognos Configuration**.
2. Select action item, then select **Verify**.
3. Without starting the Cognos Analytics server, the following action items can be verified to ensure validity.

- **Environment** > **External Dispatcher URI**
- **Environment** > **Internal Dispatcher URI**
- **Environment** > **Dataset service port number**
- **Environment** > **Logging** > **Local log server port number**
- **Environment** > **Configuration Group** > **Member synchronisation port**
- **Environment** > **Configuration Group** > **Member coordination port**

4. Verify if the settings are configured properly in the **Environment** > **Configuration Group** section. These settings need to be configured to match with the active Content Manager server.

Managing the Configuration Group

The configuration group defines a group of servers that share configuration. This is critical in multi-server installations so that configuration values remain available and consistent on all nodes, even after network partitions. The configuration group contact host runs on the same instance as the active content manager.

About this task

- In an **Easy** installation, these values are set for you.
- For a **Custom First** installation, with the machine configured as the active Content Manager, these values will be set for you.
- For a **Custom** installation, where the Content Manager is configured as a standby, or you fail the gateway URL validation during installation but choose to continue, you will need to configure these properties according to the following steps.

Procedure

1. Start Cognos Configuration.
2. In the **Explorer** window, under **Local Configuration**, click **Environment**.
3. Click **Configuration Group**.
4. To set the correct values:

   - If this is the active Content Manager server installation, you can set the values for the local server by right-clicking property names, and then clicking **Reset to Default**.
   - If this is the standby Content Manager server install, or an Application tier install, you need to set the values.

     a. Right-click **Configuration Group**, click on the **Retrieve** button to launch **Retrieve Configuration Servers** dialog.

        If the active Content Manager is SSL enabled, you can retrieve the configuration group properties **after** Content Manager URL and other properties have been correctly configured and saved.

     b. Enter the proper information to access the active Content Manager server, and then click **OK**.

        User ID - The ID with administration privileges on the server.
        Password - The password for the User ID.
        Namespace ID - The value can be found in the **Security**, **Authentication** resource. For example, `CognosEx`
        Cognos Analytics URL - The URL used to run Cognos Analytics. For example, `http://myserver:9300/bi`

   - If you cannot retrieve the values using the **Retrieve** option, you can set the values manually. Follow the guidance at the bottom of the property window for each of the properties.

     Make sure the two ports under **Local Member Settings** are two different local ports that are not in use. If all your applications on the machine were running during the installation, these ports should already be set with available ports.

Important: These ports must be open to inbound and outbound traffic.

- **Member synchronization port** is the local port used for network communication that transfers and synchronizes configuration information from one server to another. Every install needs to be able to talk to the `MutualAuthSSLHttpEndpoint` on the other installs. For example, any firewall between application and data tier needs to be open on that port. The httpEndpoint is used strictly for internal communication from one Cognos Analytics instance to another. The default is 4300.
- **Member coordination port** is the local port used for network communication for group coordination. This port is used to discover and join a group, and to maintain an up to date list of configuration group members. On the primary Content Manager install group contact port is the same port. Each install needs to be able to talk to any of the other installs on the group coordination port, so again, any firewall between tiers of the installation needs to be open for that port. The default is 5701.

5. Save the configuration.

Configuring Cryptographic Settings

IBM Cognos components require a cryptographic provider; otherwise they will not run. If you delete the default cryptographic provider, you must configure another provider to replace it.

You can configure the following cryptographic settings:

- general cryptographic settings
- settings for the default cryptographic provider
- settings for a cryptographic provider in an Entrust security infrastructure

Configuring general cryptographic settings

In a distributed installation, IBM Cognos computers communicate with Content Manager to establish trust and obtain some cryptographic keys from Content Manager.

If you change the cryptographic keys in Content Manager, such as by changing application servers or reinstalling Content Manager, you must delete the cryptographic keys on the other IBM Cognos computers. You must then save the configuration on each computer so that they obtain the new cryptographic keys from Content Manager. In addition, all IBM Cognos components in a distributed installation must be configured with the same cryptographic provider settings.

Also, in a distributed environment, the symmetric key should only be stored on computers where Content Manager has been installed.

You can configure the following general cryptographic settings:

- standards conformance

  Specifies which cryptographic standard to be used, IBM Cognos or NIST SP 800-131A.
- common symmetric key store (CSK) properties

  The CSK is used by IBM Cognos to encrypt and decrypt data.
- secure sockets layer (SSL) settings

  These include mutual authentication, confidentiality and SSL Transport Layer Security settings.

  Note: Transport Layer Security consists of a set of encryption rules that uses verified certificates and encryption keys to secure communications over the Internet. TLS is an update to the SSL protocol. Choose from 1.1, 1.2, or the combination setting.
- advanced algorithm settings

  These include signing and digest algorithms.

Procedure

1. Start IBM Cognos Configuration.

2. In the **Explorer** window, under **Security**, click **Cryptography**.
3. In the **Properties** window, change the default values by clicking the **Value** box and then selecting the appropriate value:

   - Options for standards conformance enforrcement include IBM Cognos and NIST SP 800-131A. This value may cause the save operation to fail if other parameters are not allowed in the selected standard. You must change the selected algorithm or the standards conformance. You may need to install the JRE's unlimited jurisdiction policy files to enable all the supported algorithms. They are available from IBM.
   - On computers that do not contain Content Manager, if you do not want to store the CSKs locally, under **CSK settings**, change **Store symmetric key locally** to **False**.

     When **Store symmetric key locally** is **False**, the key is retrieved from Content Manager when required. The **Common symmetric key store location** property is ignored.
   - If you want the computers at both ends of a transmission to prove their identity, under **SSL Settings**, change **Use mutual authentication** to **True**.

     Do not change the **Use confidentiality** setting.
   - If you want to change the digest algorithm, for the **Digest algorithm** property, select another value.
4. From the **File** menu, click **Save**.
5. Test the cryptographic provider on a gateway computer only. In the **Explorer** window, right-click **Cryptography** and click **Test**.

   IBM Cognos components check the availability of the symmetric key.

Results

After you configure the cryptographic settings, passwords in your configuration and any data you create are encrypted.

Configuring the default cryptographic provider

You can configure some cryptographic settings for the default cryptographic provider.

The following settings can be configured:

- Algorithms and ciphersuites
- Identity name settings
- Crypto key store settings

  The crypto key pair includes the private key that is used to encrypt data, and the public key that is used to decrypt data.
- Certificate authority settings

  The certificate authority (CA) is either the default CA or a different CA.
- Subject Alternative Name settings

  The Subject Alternative Name (SAN) is used to validate the origin of an SSL certificate.

Procedure

1. If you are using a JRE other than the one provided with IBM Cognos server, go to the `*install_location*/jre/lib/ext`.
2. Copy `bcprov-jdk*version*.jar` to `*JRE_location*/lib/ext`.
3. If you are using a JRE other than one IBM provides, you must also download and install the unrestricted Java Cryptograph Extension (JCE) policy file for your JRE to ensure that all available algorithms and cipher suites are shown in IBM Cognos Configuration.
4. Start IBM Cognos Configuration.
5. In the **Explorer** window, under **Security**, **Cryptography**, click **Cognos**.
6. In the **Properties** window, change the properties as needed.

Tip: For detailed information about each property, view the property description in IBM Cognos Configuration when you click the property.

- To configure the confidentiality algorithm, under the appropriate property, **Confidentiality algorithm** or **PDF Confidentiality algorithm**, click in the **Value** column and then select the algorithm from the drop-down list.

  The value of a confidentiality algorithm determines how data is encrypted by IBM Cognos components. For example, database passwords entered in IBM Cognos Configuration are encrypted when you save the configuration. The algorithm selected when the data is encrypted must also be available for the data to be decrypted at a later date.

  The availability of confidentiality algorithms can change if there are changes to your environment. For example, if your Java Runtime Environment (JRE) has changed or if you have installed other cryptographic software on the computer. You must ensure that the **Confidentiality algorithm** that was selected when the data was encrypted is also available when you want to access the data.

  If you have made changes to a computer, such as upgraded the JRE or installed software that has upgraded the JRE, this may affect the availability of confidentiality algorithms. To ensure that the available algorithms and cipher suites are shown in IBM Cognos Configuration, download and install the unrestricted Java Cryptography Extension (JCE) policy file. For Java that IBM provides, the unrestricted JCE policy file can be downloaded from Unrestricted JCE policy files (https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=jcesdk).
- To adjust the cipher suites, under **Supported ciphersuites**, click in the **Value** column and then click the edit icon ✎.

  Remove the cipher suites that are not applicable and move the remaining cipher suites up or down in the list so that the cipher suites in the highest range are higher in the list.

  Do not mix cipher suites in the 40- to 56-bit range with cipher suites in the 128- to 168-bit range.
- To change the location of the crypto keys, under **Encryption key settings**, change **Encryption key store location** to the new location.
- To use another certificate authority, under **Certificate Authority settings**, change **Use third party CA** to **True**.

  For more information, see "Configuring IBM Cognos components to use another certificate authority" on page 117.
- If configuring for HTTPS/SSL, change the **Server common name** from CAMUSER to the fully qualified domain name of the server.
- To configure the **Subject Alternative Name**, specify **DNS names**, **IP addresses**, and **Email addresses** (optional) that are associated with the server certificate. The values are added to the Subject Alternative Name extensions in the server certificate. You can specify multiple values for each property. Separate the values using the space character.

7. From the **File** menu, click **Save**.

Results

If you use another certificate authority (CA) server, configure IBM Cognos components to use the CA. For more information, see "Configuring IBM Cognos components to use another certificate authority" on page 117.

Configure Cryptographic Provider Settings in an Entrust Security Infrastructure

To configure encryption in an Entrust security infrastructure, you replace the default cryptographic provider in IBM Cognos Configuration with a provider that you configure for Entrust and then you update security files in your IBM Cognos environment.

Before you begin

Ensure that the key store passwords match the one in your Entrust Profile (EPF).

To prevent gateway errors, ensure that the Internet Guest Account has read and write permission to the Entrust `.epf` file and read permission to the Entrust `.ual` file.

Procedure

1. If you are using a JRE other than the one provided with IBM Cognos server, go to the *install_location*/jre/lib/ext.
2. Copy bcprov-jdk*version*.jar to *JRE_location*/lib/ext.
3. Ensure that the following files from IBM Cognos and Entrust exist in the location where the JRE is installed:
   - From the Entrust Authority Security Toolkit that you download from Entrust, copy the `.jar` file, such as `enttoolkit.jar`, to *JRE_location*/lib/ext.
4. To ensure that all available algorithms and cipher suites are shown in IBM Cognos Configuration, download and install the unrestricted Java Cryptography Extension (JCE) policy file. For Java that IBM provides, the unrestricted JCE policy file can be downloaded from Unrestricted JCE policy files (https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=jcesdk).
5. Start IBM Cognos Configuration.
6. In the **Explorer** window, under the **Security** group, click **Cryptography**.
7. In the **Properties** window, under **Advanced algorithm settings**, change the **Digest algorithm** to the appropriate message digest or secure hash algorithm for your security policy.
8. In the **Explorer** window, under the **Security** group and the **Cryptography** component, right-click the **IBM Cognos** resource, and click **Delete**.
9. Under the **Security** group, right-click **Cryptography**, and click **New resource** > **Provider**.
10. In the **Name** field, type a name for the encryption service you are creating.
11. In the **Type** field, click the arrow, and click **Entrust**, and then click **OK**.

    A branch with the name you assigned appears under **Cryptography**.
12. Click the branch you created.

    Resource properties appear in the properties window.
13. In the **Resource Properties** window, enter the appropriate values, as listed in the following table:

Table 12: Cryptography property values and descriptions

Property	**Description**
INI file location	The location of the Entrust initialization file (.ini).
Identity file distinguished name (DN)	The distinguished name associated with the profile of the Entrust identity.
Identity file location	The location of the Entrust identity profile file (.epf).
Use Entrust Server Login	The parameter that controls whether users must enter a password to log on to the Entrust PKI.
Identity file password	The Entrust Profile password, which must match the one in your Entrust Profile (EPF).
Confidentiality algorithm	The level of encryption that is required to comply with your security policy.

Table 12: Cryptography property values and descriptions (continued)

Property	Description
PDF Confidentiality algorithm	The encryption algorithm to use when encrypting PDF data.
Supported ciphersuites	The cipher suites that are supported in your security environment. Remove the ones that are not applicable and rearrange the remaining cipher suites from highest to lowest. This ensures that the most secure cipher suite is used first.
Signing Key Store Location	The location of the key store that contains the signing key pairs.
Encryption Key Store Location	The location of the key store that contains encryption key pairs.

Important: Record your passwords in a secure location.

14. From the **File** menu, click **Save**.
15. Update to Entrust Java Toolkit 7.2 SP2 Patch 170072.

IBM Cognos Application Firewall

IBM Cognos Application Firewall analyzes and validates HTTP and XML requests before they are processed by IBM Cognos servers. IBM Cognos Application Firewall may modify these HTTP and XML requests.

IBM Cognos Application Firewall protects IBM Cognos Web products from malicious data. The most common forms of malicious data are buffer overflows and cross-site scripting (XSS) attacks, either through script injection in valid pages or redirection to another Web site.

You can track firewall activity by checking the log file, which contains rejected requests. By default, log messages are stored in the `*install_location*/logs/cogaudit.log` file.

If you are using the collaboration features with IBM Connections, you must add the host name, domain, and port number on which IBM Connections is running to the **Valid domains and hosts** property for the Cognos Application Firewall.

All Cognos Application Firewall settings must be the same for all computers where IBM Cognos Application Tier Components are installed within a distributed environment. For example, if Cognos Application Firewall is disabled on some computers and enabled on others, unexpected behavior and product errors may result.

The following types of URLs are accepted by Cognos Application Firewall validation:

- fully qualified (absolute) URLs

  in the format *protocol*://*host*:*port*/*path*, where *protocol* is http or https and *host* is validated against the valid domain list
- URLs relative to the Web installation directory

  in the format /*Web_installation_root*/.* where *Web_installation_root* is the gateway Web directory, based on the ibmcognos alias that you configured on your Web server.

  For example,

  /ibmcognos/ps/portal/images/action_delete.gif
- specific allowed URLs, including the following (all case insensitive)

about:blank

JavaScript:window.close( )

JavaScript:parent.close( )

JavaScript:history.back( )

parent.cancelErrorPage( )

doCancel( )

Configuring IBM Cognos components to use IBM Cognos Application Firewall

Using IBM Cognos Configuration, you can change settings for other XSS tool support, and you can add host and domain names to the IBM Cognos list of valid names.

Procedure

1. Start IBM Cognos Configuration in each location where Application Tier Components are installed.
2. In the **Explorer** window, under **Security,** click **IBM Cognos Application Firewall**.
3. In the **Properties** window, for the **Enable CAF validation** property, set the appropriate values.

   By default, IBM Cognos Application Firewall is enabled.

   Important: The IBM Cognos Application Firewall is an essential component of IBM Cognos security, helping to provide protection against penetration vulnerabilities. Disabling the IBM Cognos Application Firewall will remove this protection. Under normal circumstances, do not disable the IBM Cognos Application Firewall.
4. If you are using another XSS tool that checks for specific characters in GET request parameters, in the **Properties** window, for the **Is third party XSS checking enabled** property, change the value to **True**.

   The default characters that are prohibited include >, <, and '.
5. Add host and domain names to the IBM Cognos list of valid names:

   - For the **Valid domains and hosts** property, click the value and then click the edit icon ✏.
   - In the **Value - Valid domains or hosts** dialog box, click **Add**.

     You must include the domains from all hyperlinks that are added in the portal. For more information, see the topic about creating a URL in the *IBM Cognos Analytics Administration and Security Guide*.

     Tip: If you are using drill-through from IBM Cognos Series 7 to reports in IBM Cognos Analytics, add the hostnames of the IBM Cognos Series 7 gateway servers to the list.
   - In the blank row of the table, click and then type the host or domain name.

     To allow a domain and all its sub-domains, use a wildcard character at the begining of the domain name.

     For example, ***.mycompany.com**

     If you are using the collaboration features with IBM Connections, you must add the host, domain, and port number for the IBM WebSphere profile where you have installed IBM Connections. For example, if you installed IBM Connections on a computer named **myserver**, and your domain is **mycompany.com**, you would add **myserver.mycompany.com:9080**, where 9080 is the IBM WebSphere port number on which IBM Connections is running.
   - Repeat the previous two bulleted steps for each name to be added.
   - Click **OK**.

   IBM Cognos Application Firewall validates domain and host names to protect URLs that are created. By default, IBM Cognos Application Firewall considers domain names derived from the environment configuration properties to be safe domain names. Adding names to the list of valid names and hosts is useful when you need to redirect requests to non-IBM Cognos computers using the Back or Cancel functions or when using drill-through to different IBM Cognos product installations.

6. Save the configuration.
7. Restart the services.

Encrypt Temporary File Properties

Temporary files are used in IBM Cognos Analytics to store recently viewed reports and to store data used by the services during processing. You can change the location of the temporary files and you can choose to encrypt their content.

By default, IBM Cognos components store temporary files in the *install_location*\temp directory and the files are not encrypted.

For optimum security, deny all access to the temp directory, except for the service account used to start the IBM Cognos services. Read and write permissions are required for the service account.

Procedure

1. Start IBM Cognos Configuration.
2. In the **Explorer** window, click **Environment**.
3. In the **Properties** window, for the **Temporary files location** property, specify the new location.
4. If you require the content of temporary files to be encrypted, set the **Encrypt temporary files** property to **True**.
5. Ensure that the user account under which IBM Cognos Analytics components run have the appropriate privileges to the temporary files location. For example:
   - on Microsoft Windows operating systems, full control privileges
   - on UNIX or Linux operating systems, read-write privileges

Configure the Gateway to Use a Namespace

If IBM Cognos components use multiple namespaces, or if anonymous access is enabled and IBM Cognos components use one namespace, you can configure the gateway to connect to one namespace. Users logged onto the Web server where the gateway is located are not prompted to choose an authentication source. For example, if you have two Web servers, you can configure each Web server to use a different namespace.

Procedure

1. On the computer where the gateway is located, start IBM Cognos Configuration.
2. In the **Explorer** window, click **Environment**.
3. In the **Properties** window, in the **Value** box next to the **Gateway namespace** property, type the Namespace ID of the namespace that you want to use.
4. From the **File** menu, click **Save**.
5. Restart your Web server.

Enable and Disable Services

In a distributed installation, you can send certain types of requests to specific computers by enabling or disabling the installed services.

For example, to dedicate a computer to running and distributing reports, you can disable the presentation service on an Application Tier Components computer.

Note: The default values for dispatcher service and presentation service are false on computers that only have Content Manager installed. On all other types of installations, the default values are true.

If you installed all components on several computers, you can disable appropriate services on each computer to get the distributed configuration you require. Requests are only sent to dispatchers where a given service is enabled.

Disabling a service prevents the service from loading into memory. When disabled, services do not start and therefore do not consume resources. The service does not run until you enable it.

If you disable the dispatcher service, the dispatcher-related services are disabled. Only dispatcher services that are enabled can process requests.

Restriction: When restarting services manually, (if applicable) the `ApacheDS - cognos` service must be started before the `IBM Cognos` service.

Enabling and disabling services

Use the following procedure to disable selected services on components in a distributed installation.

Procedure

1. Start IBM Cognos Configuration.
2. In the **Explorer** window, under **Environment**, click **IBM Cognos services**.
3. In the **Properties** window, click the **Value** next to the service that you want to disable or enable.

   By default, all services are enabled.
4. Click the appropriate state for the services:

   - To disable the service, click **False**.
   - To enable the service, click **True**.

   When restarting services manually, (if applicable) the `ApacheDS - cognos` service must be started before the `IBM Cognos` service.
5. From the **File** menu, click **Save**.

Configuring fonts

IBM Cognos products use fonts to render PDF reports on the IBM Cognos server. They also use fonts to render charts used in PDF and HTML reports.

To show output correctly, fonts must be available where the report or chart is rendered. For charts and PDF reports, the fonts must be installed on the IBM Cognos server. If a requested font is not available, IBM Cognos components substitute a different font.

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

Use the following checklist if you want to use a new font in your reports.

__ • Add the font to the list of supported fonts.

__ • Specify the file location of the new font.

__ • Map the new font to the physical font name, if required.

Considerations to support Simplified Chinese

IBM Cognos products support the GB18030-2000 character set, which is used in the encoding of Simplified Chinese locales.

If you install on Microsoft Windows, support is provided for the GB18030-2000 character set in the SimSun-18030 font that is provided by Microsoft.

On operating systems other than Windows, you must install a font that supports GB18030-2000.

Add Fonts to the IBM Cognos Environment

You can add fonts to the list of supported fonts in your IBM Cognos environment if you want to generate reports that use fonts that are currently not available. You can also remove fonts. By default, IBM Cognos components use a set of global fonts, which are available on all IBM Cognos server computers.

Procedure

1. On each Content Manager computer, start IBM Cognos Configuration.
2. From the **Actions** menu, click **Edit Global Configuration**.
3. Click the **Fonts** tab.
4. Click **Add**.

   Tip: To remove a font from the list of supported fonts, click the box next to the font name and then click **Remove**.
5. In the **Supported Font Name** box, type the font name and then click **OK**.
6. From the **File** menu, click **Save**.

   All global fonts, including new fonts that you add, must be installed on all IBM Cognos computers in your environment.

Results

If a global font is not installed on all IBM Cognos computers, you must map the global font to an installed, physical font.

Specifying the location of available fonts

You must specify the installation location of all fonts, including fonts that you add to the list of supported fonts.

By default, the list of fonts consists of fonts that are installed in the *install_location*\bin\fonts directory of the IBM Cognos computer. If IBM Cognos components are installed on a Microsoft Windows operating system computer, they also use the fonts that are installed in the Windows font directory.

You specify the font location on all computers where Application Tier Components are installed.

Procedure

1. On each Application Tier Components computer, start IBM Cognos Configuration.
2. In the **Explorer** window, click **Environment**.
3. In the **Properties** window, for the **Physical fonts locations** property, specify the location of the fonts.

   If there are multiple font paths, separate each path by a semicolon (;).

   If you are using an application server other than one that is provided with IBM Cognos Analytics, enter the fully qualified path to the font location. For example: *install_location*\bin\fonts.
4. From the **File** menu, click **Save**.

Map Supported Fonts to Installed Fonts

You can substitute global fonts, which are not installed on the computer, for physical fonts.

You map fonts on each computer where the Application Tier Components are installed.

For example, you add a font to the list of supported fonts that is not installed on the IBM Cognos computer. You can specify which font to use as a substitute.

If you want to print reports faster by using the built-in PDF fonts, you can map a global font such as Arial to one of the built-in PDF fonts, such as Helvetica-PDF, using the following steps. You can also select one of the built-in PDF fonts for a text object in Reporting or Query Studio. For more information, see the *Query Studio User Guide* or the *Reporting User Guide*.

No mapping is required if you add a font to the supported font list that is installed on IBM Cognos computers. However, you must specify the location of the font.

Procedure

1. On each Application Tier Components computer, start IBM Cognos Configuration.
2. In the **Explorer** window, click **Environment**.

3. In the **Properties** window, click the **Value** box next to the **Physical fonts map** property, and then click the edit icon ✎.

   The **Value - Physical fonts map** dialog box appears.
4. Click **Add**.

   Tip: To remove a font, select the check box next to the font and click **Remove**.
5. In the **Global Font Name** box, type the name of the font you added to the supported font list.
6. Click the **Physical Font Name** box.
7. If you know the physical font name, type it. Otherwise, click the edit icon ✎.

   In the **Physical Font Name** dialog box, click **Search Now** and then click a font name from the results.
8. Repeat steps 4 to 7 for each global font that requires mapping.
9. Click **OK**.
10. From the **File** menu, click **Save**.

Results

Now, if required, you must specify the installation location of the fonts.

Using system fonts in IBM Cognos Configuration

You can set IBM Cognos Configuration to use your system fonts on Microsoft Windows operating systems.

Note: If you enable system font settings, you cannot change the font settings within IBM Cognos Configuration.

Procedure

1. Go to the *install_location*/configuration directory.
2. Open the cogconfig.prefs file in a text editor.
3. Add the following line:

```
UseSystemDisplaySetting=true
```

4. Save and close the file.
5. Restart IBM Cognos Configuration.

Change the default font for PDF reports

You can change the default font that IBM Cognos Analytics components use for PDF reports. You see this default font when you open a report.

You change the default font on the computer where Content Manager is installed. The font then becomes the default for all computers in your installation. You change the font used for PDF reports using IBM Cognos Configuration.

Ensure that the default font is installed on all computers in your IBM Cognos installation.

To ensure that GB18030 characters are displayed correctly in PDF reports, set the default font to SimSun-GB18030.

Procedure

1. On each Content Manager computer, start IBM Cognos Configuration.
2. From the **Actions** menu, click **Edit Global Configuration**.
3. Click the **General** tab.
4. In the **Value** box, for **Default font**, type the font you want to use as the default for reports.
5. Click **OK**.

6. From the **File** menu, click **Save**.
7. On all Application Tier Components computers, ensure that the installation location of the default font is specified in the **Physical fonts locations** property (under **Environment** in the **Explorer** window) or that the font is in the Windows font directory.

Configure Embedded Fonts for PDF Reports

When a PDF report opens in Adobe Reader, all the fonts used in that report must be available. Fonts must be either embedded in the report or installed on the user's computer. If a font is not available in either of these locations, Adobe Reader tries to substitute an appropriate font. This substitution may cause changes in the presentation of the report or some characters may not be displayed.

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

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

Procedure

1. On the Content Manager computer, start IBM Cognos Configuration.
2. In the **Explorer** window, click **Environment**.
3. In the **Properties** window, under **Font Settings**, click the value for **Fonts to embed (Batch report service)** or **Fonts to embed (Report service)**, and then click the edit icon ✎.
4. If you are not using the default fonts directory or if you want to add a path to an additional directory, in the **Fonts to Embed in PDF Reports** dialog box, specify the new path in the font paths box.

   Tip: Click **Search Now** to get a list of the available fonts in the specified path or paths.
5. For a font that will always be available on users' computers, scroll to the font name, and click the **Never** check box.

   IBM Cognos Analytics does not embed the font with any reports. Adobe Reader picks up the font from the user's computer when the report is opened.
6. For a font that may not always be available on the users' computers, scroll to the font name and click the **Always** check box.

   IBM Cognos Analytics embeds the font with all reports that use it. Adobe Reader uses the embedded font when the report is opened.
7. Click **OK**.

Saved Report Output

By default, report output files are saved in the content store. You have the option of saving a copy of the report output in another file location that is outside or inside IBM Cognos Analytics. If you use this option, a descriptor file with an _descr extension is also saved. Saved files are not managed by IBM Cognos Analytics.

Save Report Output Outside IBM Cognos Analytics

If you configure a file system location that is outside of IBM Cognos Analytics, you can then share the report output with external applications or people who don't have IBM Cognos Analytics. This is how most report output files are saved.

To use this feature, you must first configure a root directory in IBM Cognos Configuration. An administrator must then set the file location in IBM Cognos Administration. For more information, see the topic about setting a file location for report output saved outside of IBM Cognos Analytics, in the *IBM Cognos Analytics Administration and Security Guide*.

Report outputs will always be written to the directory configured for each Delivery Service instance. In order to avoid having report outputs written to multiple locations, ensure that you are either running only one instance of the Delivery Service, or configure all service instances to use a shared network file location. Any Dispatcher running the Delivery Service must have access to the file system or be disabled on all systems not intended to save report output.

Procedure

1. Create a directory for your file system.

   Tip: Ensure that the directory is accessible to users and separate from the installation directory. For example, in a distributed installation on Microsoft Windows, an archive folder such as \\servername\directory could be used.
2. On the Content Manager computer, start IBM Cognos Configuration.
3. From the **Actions** menu, click **Edit Global Configuration**.
4. In the **Global Configuration** window, click the **General** tab.
5. For **Archive Location File System Root**, type a URI using the format

   ```
   file://directory
   ```

   where *directory* is the directory that you created in step 1.

   The file:// portion of the URI is required. Windows UNC names, such as \\servername\directory, can be used. If so, the URI must be formatted as follows:

   ```
   file://\\servername\directory
   ```

   Tip: Ensure that you do not use a mapped drive when running Cognos as a Microsoft Windows service.
6. To confirm that the correct location will be used, click **Test**.
7. Click **OK**.
8. From the **File** menu, click **Save**.

Results

The administrator must now configure the file location. For information, see the topic about setting a file location for report output saved outside of IBM Cognos Analytics, in the *IBM Cognos Analytics Administration and Security Guide*.

Save Report Output Inside IBM Cognos Analytics

If you configure a file system location that is inside IBM Cognos Analytics, you can then use the report output again. This may also be useful for archive purposes, because files that are saved in the content store may be deleted regularly due to retention rules.

To use this feature, you must first enable the **Save report outputs to a file system** property in IBM Cognos Configuration. An administrator must then configure the file location using the CM.OutPutLocation parameter in IBM Cognos Administration. For more information, see the topic about setting a file location for report output saved inside IBM Cognos Analytics, in the *IBM Cognos Analytics Administration and Security Guide*.

Report outputs will always be written to the directory configured for each Delivery Service instance. In order to avoid having report outputs written to multiple locations, ensure that you are either running only one instance of the Delivery Service, or configure all service instances to use a shared network file location. Any Dispatcher running the Delivery Service must have access to the file system or be disabled on all systems not intended to save report output.

To protect the security of the report output when using this feature, the file system must have third-party encryption.

Procedure

1. Create a directory for your file system.

   Tip: Ensure that the directory is accessible to authorized users only.
2. On the Content Manager computer, start IBM Cognos Configuration.
3. In the **Explorer** window, click **Data Access** > **Content Manager**.
4. For the **Save report outputs to a file system** property, click **True**.
5. To test the connection to the report output directory, from the **Actions** menu, click **Test**.
6. From the **File** menu, click **Save**.

Results

The administrator must now configure the file location using the CM.OutPutLocation parameter. For information, see the topic about setting a file location for report output saved inside IBM Cognos Analytics, in the *IBM Cognos Analytics Administration and Security Guide*.

Changing the location of temporary report output

When users run interactive reports, the report output is stored in Content Manager or in a temporary session cache in the local report file system. You can change the location of the temporary session cache to a remote computer such as a shared directory on a Microsoft Windows based system or a common mounted directory on a UNIX or Linux based system.

By default, the location of the temporary session cache on the report file system is `install_location/temp/session`. The `session` directory is created by the report server when the first request from a user session is received.

Procedure

1. Start IBM Cognos Configuration on the computers where Application Tier Components are installed.
2. In the **Explorer** window, click **Environment**.
3. In the **Properties** window, click the value for **Temporary files location**, and then click the edit icon ✎.
4. In the **Select Folder** dialog box, use the **Save in** box to locate the computer and directory, and then click **Select**.
5. From the **File** menu, click **Save**.

   When a user runs an interactive report session, the temporary report output is now stored in the new location.

Changing the location of legacy Map Manager maps for Reporting

IBM Cognos Analytics comes with a set of sample map charts that you can use in Reporting. You can change the location of the map charts by using IBM Cognos Configuration.

Note: This information applies only to the legacy Map Manager maps you can use in reports.

By default, the map charts are stored in the `install_location/maps` directory on the Application Tier Components computer.

For more information about using map charts, see the Reporting *User Guide*.

For information about using custom maps from other sources, see the Map Manager *Installation and User Guide*.

Procedure

1. On the Application Tier Components computer, start IBM Cognos Configuration.
2. In the **Explorer** window, click **Environment**.

3. In the **Properties** window, click the value for **Map files location**.
4. Click the edit button ✏.
5. In the **Select Folder** window, navigate to the directory you want and then click **Select**.
6. From the **File** menu, click **Save**.

Tuning WebSphere Liberty Profile

In production environments, tune the WebSphere Liberty Profile to allow for the maximum number of concurrent users you expect by adjusting the coreThreads and maxThreads values in the Advanced properties of the resources. These values set the core and maximum executor thread counts.

Procedure

1. Start IBM Cognos Configuration.
2. In the **Explorer** window, under **Environment**, under **IBM Cognos services** click the Resources name (default is **IBM Cognos**).
3. In the **Properties** window, next to **Advanced properties,** click inside the **Value** box, and then click the edit icon ✏.
4. Adjust the parameter values as needed.

   Table 13: Service Resource parameter names and values

Parameter Name	**Value**
coreThreads	The core number of threads that the WebSphere Liberty Profile server starts up with. If this value is less than 0, a default value is used. This default value is calculated based on the number of hardware threads on the system.
maxThreads	The maximum number of threads that can be associated with the WebSphere Liberty Profile server.

   For more information, refer to the WebSphere Liberty Profile knowledge center, Tuning the Liberty profile (https://www.ibm.com/support/knowledgecenter/en/SSEQTP_liberty/com.ibm.websphere.wlp.doc/ae/twlp_tun.html).
5. From the **File** menu, click **Save**.

Enabling session replication for standby Content Manager services

The session replication feature allows for seamless IBM Cognos Content Manager failover between an active Content Manager service and a standby Content Manager service.

With session replication enabled, user session data are replicated among all Content Manager instances. If the active Content Manager fails, the user session data is preserved and users continue to use the application without disruption.

Session replication uses two ports to securely communicate with the different IBM Cognos Content Managers configured within a single environment.

Procedure

1. On a computer where the IBM Cognos Content Manager is installed, start IBM Cognos Configuration.
2. In the **Explorer** pane, under **Security**, click **Replication**.

3. Specify the following properties:
   a) Set **Enable replication** to **True**.
   b) In the **Peer listener port number** value box, enter a port number.

      A value of 0 selects the first available dynamic port during the IBM Cognos service startup.
   c) In the **RMI replication port number** value box, enter a port number.

   Note: The **Advanced properties** should be used only under guidance from IBM Technical Support.
4. Save the configuration and restart the IBM Cognos service.
5. Repeat the steps for each Content Manager instance in your environment.

   The port numbers that you specify do not need to be identical for each Content Manage instance.

Use an external object store for report output and datasets

You can configure Content Manager to store report output and datasets to a local drive or network share by defining an external object store. Report output is available through the portal and IBM Cognos SDK, but the report output is not stored in the content store database.

Using an external object store for report output reduces the size of the content store and provides performance improvements for Content Manager.

Before you begin

Ensure that you do the following before you create an external object store connection.

- Provide Content Manager computers with access to the file location of the external object store.
- Provide the user account that runs the IBM Cognos service with read and write access to the file location.
- Create the content store.

Procedure

1. Start IBM Cognos Configuration.
2. In the **Explorer** window, under **Data Access** > **Content Manager**, right-click the name of your **Content Store**, and then click **New resource** > **External Object Store**.
3. In the **New Resource - External Object Store** window, type a unique name for your file system repository, and click **OK**.

   You can have only one external object store.
4. Click the name for the repository.
5. In the **External Object Store - Resource Properties** window, click inside the value field, click edit, and when the **URI values** window opens, type the path to your file system location, where file-system-path is the full path to an existing file location.

   Table 14: Examples of URI values

File system	URI value
Windows	`file:///c:/file-system-path` `file://host/share/file-system-path`
UNIX or Linux	`file:///file-system-path`

   Note: Relative paths, such as `file:///../file-system-path` and drive mappings are not supported.

In a distributed installation, all Content Managers must have read and write access to the file system location. To improve performance when reading outputs, Application Tier Components, essentially the repository service, should have read access to the file system location. If they do not have read access, requests are routed to the active Content Manager.

6. Restart the IBM Cognos service.

Verify access to the external object store

Use IBM Cognos Configuration to verify that IBM Cognos components can connect to the external object store.

Procedure

1. Start IBM Cognos Configuration.
2. From **Explorer** > **Data Access**, right-click the name of your external object store connection.
3. Click **Test**.

   IBM Cognos Configuration verifies access to the external object store file location.

   You can also test this connection by right-clicking **Local Configuration** and selecting **Test**.

Customizing Server-side Printing for UNIX and Linux Platforms

The way in which the IBM Cognos Analytics portal handles server printing can differ depending on your platform.

For this reason, you can customize the way in which the portal handles the printing of PDF format reports for UNIX and Linux platforms by configuring the *rsprintpdf.sh* file.

The *rsprintpdf.sh* file should not be configured for Microsoft Windows operating system print servers.

When a user selects **Run with Options**, changes the **Format** to PDF, selects **Print the Report** from the **Delivery** section, and then specifies additional formats through **advanced options** such as Landscape orientation, A4 paper size or a **Time and Mode** to run the report, problems might occur when printing to a UNIX or Linux print server. The output might not be generated, or it might appear cropped or incorrectly orientated.

Procedure

1. Open the *rsprintpdf.sh* file located in the *install_location/bin directory*.
2. In a text editor, customize the section that is specific to your print server's platform, for example AIX, or Linux.
3. Use the following information for customization. The information is passed to the *rsprintpdf.sh* script by the server process as command line options.

Table 15: Customization options for the printing of PDF format reports

Option	Name	Description
-p	printer	Specifies the print queue. If no print queue is specified, the default queue is used.
-o	orientation	Specifies the page orientation for a file, for example landscape or portrait. If no orientation is specified, portrait orientation is used.
-m	media	Specifies the media size of the output, for example letter or A4 paper size. If no media, or no height or width are specified, the default paper tray is used.

Table 15: Customization options for the printing of PDF format reports (continued)

Option	Name	Description
-h	height	For custom page sizes. Specifies the height of the page in points. It is valid only if specified with the -w option, and without the -m option.
-w	width	For custom page sizes. Specifies the width of the page in points. It is valid only if specified with the -h option, and without the -m option.
-L	log file	Specifies a path to a user-specified file for logging error messages. The default filename for the log file is *rsprintpdf.errors.log*.

4. **Tip**: Keep a copy of the *rsprintpdf.sh* file in case it should be overwritten by a future software upgrade.

Change the notification database

By default, the notification server uses the same database that Content Manager uses for the content store. You can use a separate database for notification in situations where you run large volumes of batch reports and email.

Using a separate database for notification involves the following tasks:

- Creating a notification database.

  For IBM Db2, Oracle, Microsoft SQL Server, use the same procedure that was used to create the content store database. Use the instructions in Guidelines for creating the content store.

  Note: If you are using Db2, you cannot generate a script to create the notification database in the same way as you can the content store.

  For Db2 on z/OS, use the instructions in "Suggested settings for creating a notification database on IBM Db2 on z/OS " on page 114.
- Setting up the database connectivity.

  You can use the same procedure as to set the connectivity for the content store database, "Set up database connectivity for the content store database" on page 41.
- Changing the connection properties for the notification database.

  Use the instructions in "Change the Connection Properties for the Notification Database" on page 115.

Suggested settings for creating a notification database on IBM Db2 on z/OS

The database you create for the notification database must contain the specified configuration settings.

To ensure a successful installation, use the following guidelines when creating the notification database.

Use the following checklist to help you help you set up the notifications database in Db2 on z/OS.

__ • Create a database instance, storage group, and a user account for the notification database.

A user must have permissions to create and delete tables in the database.

IBM Cognos Analytics uses the credentials of the user account to communicate with database server.

__ • Ensure you reserve a buffer pool with a page size of 32 k, and a second one with a page size of 4 k for the database instance.

__ • Administrators must run a script to create tablespaces to hold Large Objects and other data for the notification database to use the tablespaces.

For information about running the script, see "Creating tablespaces for a notification database on IBM Db2 for z/OS " on page 115.

__ • Your database administrator must back up IBM Cognos Analytics databases regularly because they contain the IBM Cognos data.

To ensure the security and integrity of databases, protect them from unauthorized or inappropriate access.

Creating tablespaces for a notification database on IBM Db2 for z/OS

If you are using Db2 for z/OS, a database administrator must run scripts to create a set of tablespaces required for the notification database. The scripts must be modified to replace the placeholder parameters with ones that are appropriate for your environment.

Ensure that you use the naming conventions for Db2 for z/OS. For example, all names of parameters must start with a letter and the length must not exceed 6 characters. For more information, see the Db2 Knowledge Center.

Procedure

1. Connect to the database as a user with privileges to create and drop tablespaces and to allow execution of SQL statements.
2. To create the notification tablespaces, go to the `*install_location*/configuration/schemas/delivery/zosdb2` directory.
   a) Make a backup copy of the `NC_TABLESPACES.sql` script file and save the file to another location.
   b) Open the original `NC_TABLESPACES.sql` script file and use the following table to help you to replace the placeholder parameters with ones appropriate for your environment.

Table 16: Tablespace parameter names and descriptions for the Db2 notification database on z/OS

Parameter Name	Description
NCCOG	Specifies the name of the notification database.
DSN8G810	Specifies the name of the storage group.
BP32K	Specifies the name of the buffer pool.

   Not all of the parameters listed are in the script, but might be added in the future.

   c) Save and run the script.

   For example,

```
db2 -tvf NC_TABLESPACES.sql
```

   d) Open the `NC_CREATE_DB2.sql` script file and replace the NCCOG placeholder parameter with the name of the notification database.
   e) Save the script.

   The Job and Scheduling Monitor services will automatically run the script. However, you may choose to run it yourself.

Change the Connection Properties for the Notification Database

After you create a separate database for notification, you must configure IBM Cognos components to use the new database.

You must configure all Content Managers and Application Tier Components to use the same notification database.

Procedure

1. In each location where Content Manager or Application Tier Components is installed, start IBM Cognos Configuration.
2. In the **Explorer** window, under **Data Access**, click **Notification**.
3. Identify the database that is used for notification:
   - In the Explorer window, right-click **Notification** and select **New resource** > **Database**.
   - Type a name for the database resource.
   - Select the type of database from the pull-down menu.
   - Click **OK**.
4. In the **Properties** window, enter the values for the notification database resource.
5. From the **File** menu, click **Save**.
6. Test the notification. In the **Explorer** window right-click **Notification** and click **Test**.

   This tests the database connection and the mail server connection.

   If you have been using the content store database for notification, the schedules will be replicated in the tables of the new notification database.

Results

Ensure that the values used to identify the notification database resource are the same on all Content Manager and Application Tier Components computers. To use the default notification database, you do not have to edit the values in the **Properties** window.

Change the security standard compliance for IBM Cognos trust stores

By default, the IBM Cognos trust stores that are used for SSL communications include only certificates that are qualified for the NIST SP800-131a standard. You can change the certificates available to you by using the ThirdPartyCertificateTool.

You can add non-NIST SP800-131a standards and you can also remove the non-NIST SP800-131a standards you have added.

Restore non-NIST SP800-131a standard certificates to IBM Cognos trust stores

By default, the IBM Cognos trust stores includes only certificate authority (CA) certificates that are qualified for the NIST SP800-131a standard. If you use other certificates, such as SHA1 or 1024-bit CA certificates, you must add these certificates to the trust store individually. Or, you add these certificates from the trust store of the JRE you are using with the ThirdPartyCertificateTool restore command.

Tip: The examples in this topic use the default password, `NoPassWordSet`. If you change the **Key store password**, and the **Certificate Authority settings** password in IBM Cognos Configuration, ensure you use the password that you set.

Before you begin

On UNIX or Linux operating systems, ensure that you set a JAVA_HOME environment variable before you use the `ThirdPartyCertificateTool`.

On Microsoft Windows installations, you can run the tool with `-java:local` to use the JRE that is provided with the installation. For example,

```
ThirdPartyCertificateTool.bat -java:local -R
```

Procedure

1. Go to the `install_location/bin` directory.

2. Restore the non-NIST SP800-131a standard certificates by typing the following command:

   On UNIX or Linux operating systems, type

   ```
   ThirdPartyCertificateTool.sh -R -p NoPassWordSet
   ```

   On Windows operating systems, type

   ```
   ThirdPartyCertificateTool.bat -R -p NoPassWordSet
   ```

Remove non-NIST SP800-131a standard certificates from the IBM Cognos trust stores

If you have added non-NIST SP800-131a certificates to the IBM Cognos trust stores, such as SHA1 or 1024-bit CA certificates, you can remove those certificates with the ThirdPartyCertificateTool.

Tip: The examples in this topic use the default password, `NoPassWordSet`. If you change the **Key store password**, and the **Certificate Authority settings** password in IBM Cognos Configuration, ensure you use the password that you set.

Before you begin

On UNIX or Linux operating systems, ensure that you set a JAVA_HOME environment variable before you use the `ThirdPartyCertificateTool`.

On Microsoft Windows installations, you can run the tool with `-java:local` to use the JRE that is provided with the installation. For example,

```
ThirdPartyCertificateTool.bat -java:local -N
```

Procedure

1. Go to the `install_location/bin` directory.
2. Type the following command:

   On UNIX or Linux operating systems, type

   ```
   ThirdPartyCertificateTool.sh -N -p NoPassWordSet
   ```

   On Windows operating systems, type

   ```
   ThirdPartyCertificateTool.bat -N -p NoPassWordSet
   ```

Configuring IBM Cognos components to use another certificate authority

By default, IBM Cognos Analytics components use their own certificate authority (CA) service to establish the root of trust in the IBM Cognos security infrastructure. However, you can configure IBM Cognos components to use a certificate from another certificate authority, such as iPlanet or Microsoft.

To use another CA certificate, you must use the following process:

1. "Create certificate signing request (CSR) files" on page 119.

   Part of this task requires you to submit the CSRs to your certificate authority and generate the certificates. For more information about that process, see your CA documentation.
2. "Import the CA certificates into IBM Cognos components" on page 120
3. "Configure IBM Cognos components to use certificates generated by your CA" on page 121.

ThirdPartyCertificateTool commands and examples

Some tasks use a command-line tool named `ThirdPartyCertificateTool`. The following tables list the options for this command-line tool.

ThirdPartyCertificateTool commands

Table 17: Main operation mode

Command	Description
-c	Creates a certificate signing request (CSR).
-i	Imports a certificate.
-E	Exports a certificate.

Table 18: Operation modifiers

Command	Description
-e	Work with the crypto identity.
-T	Work with the truststore (used only with -i and -E).

Table 19: Information flags

Command	Description
-d	Distinguished name (DN) to use for certificate.
-r	CSR or certificate file location (depends on mode).
-t	Certificate authority chain file. Can be either PEM, binary PKCS#7 CA certificate chain, or a single DER-format CA certificate.
-p	Keystore password. If -p is not included, NoPassWordSet is used as a default password.
-a	Key pair algorithm: RSA. RSA is the default value.
-P	Creates a CA keystore that includes the certificate authorities that are trusted by the current JRE.
-N	Sets the CA truststore to use the NIST SP800-131a standard.
-R	Restores non-NIST SP800-131a certificates back to the truststore.

The sample values from the following table are used:

Table 20: Sample values

Property	Value
Encryption certificate DN	A unique value, formatted as: `CN=EncryptCert,O=MyCompany,C=CA`

Table 20: Sample values (continued)

Property	Value
Keystore password	The default password: NoPassWordSet This value must match the passwords in IBM Cognos Configuration under **Security** > **Cryptography** > **Cognos**. If you change the default values for **Signing key store password**, **Encryption key store password**, and **Certificate Authority key store password**, ensure you use the passwords that you set.

ThirdPartyCertificateTool examples

Table 21: ThirdPartyCertificateTool examples

Example	Command
To create a new crypto keypair and PKCS#10 CSR:	`ThirdPartyCertificateTool.bat -c -e -d cn=Me,o=MyCompany,c=CA -r crypto.csr -a RSA -p password`
To import the third party CA generated crypto certificate and PKCS#7 CA certificate chain:	`ThirdPartyCertificateTool.bat -i -e -r crypto.cer -p password -t cacert.p7b`
To import the third party CA generated crypto certificate and PEM CA certificate chain:	`ThirdPartyCertificateTool.bat -i -e -r crypto.cer -p password -t cacert.pem`
To add `ca.cer` as a trusted certificate:	`ThirdPartyCertificateTool.bat -i -T -r ca.cer -p password -t cacert.cer`
To export the crypto certificate to `crypto.cer`:	`ThirdPartyCertificateTool.bat -E -e -r crypto.cer -p password`
To export the IBM Cognos CA certificate to `ca.cer` (when NOT using a third party CA):	`ThirdPartyCertificateTool.bat -E -T -r ca.cer -p password`
To remove all non-NIST SP800-131a CA certificates, and set CA trust store to NIST SP800-131a standard:	`ThirdPartyCertificateTool.bat -N -p password`
To restore JRE non-NIST SP800-131a certificates back to CA trust store:	`ThirdPartyCertificateTool.bat -R -p password`

Create certificate signing request (CSR) files

To obtain a certificate from a certificate authority (CA), you must first generate certificate signing request (CSR) files for the crypto key from the IBM Cognos keystore. The CA uses this file to produce a crypto certificate, and a CA certificate that you import into your keystore.

Tip: The examples in this topic use the default password, `NoPassWordSet`. If you change the **Key store password**, and the **Certificate Authority settings** password in IBM Cognos Configuration, ensure you use the password that you set.

Before you begin

On UNIX or Linux operating systems, ensure that you set a JAVA_HOME environment variable before you use the `ThirdPartyCertificateTool`.

On Microsoft Windows installations, you can run the tool with `-java:local` to use the JRE that is provided with the installation. For example,

```
ThirdPartyCertificateTool.bat -java:local -c -d ...
```

Procedure

1. Back up your key data:
   a) Go to the *install_location*`\configuration` directory.
   b) Back up the `cogstartup.xml` file to a secure location.
   c) Back up the contents of the following directory to a secure location: *install_location*`\configuration\certs`
2. Go to the *install_location*`\bin` directory.
3. Create the certificate signing request for the cyrpto key by typing the following command:

   On UNIX or Linux, type

   ```
   ThirdPartyCertificateTool.sh -c -e -d "CN=EncryptCert,O=MyCompany,C=CA" -r
   encryptRequest.csr -p NoPassWordSet
   ```

   On Windows, type

   ```
   ThirdPartyCertificateTool.bat -c -e -d "CN=EncryptCert,O=MyCompany,C=CA" -r
   encryptRequest.csr -p NoPassWordSet
   ```

   The distinguished name (DN) value in the command (`"CN=SignCert,O=MyCompany,C=CA"`) uniquely identifies the IBM Cognos installation. The attributes that are used reflect a hierarchical structure in your organization.

   The password that you enter for this key must be used again when import the certificate and again in IBM Cognos Configuration.

   You can safely ignore any warnings about logging.

   The command creates the `CAMKeystore` file in the `certs` directory, sets the specified password, creates a keypair, stores it in the keystore, and exports the `encryptRequest.csr` file to the *install_location*`\bin` directory.
4. Copy the `encryptRequest.csr` file to a directory that is accessible by your certificate authority.
5. Input the `encryptRequest.csr` file into the certificate authority, and generate the certificate.

   The certificate authority produces a crypto key certificate, and a CA certificate.

   Important: The certificates that are generated by your CA must be PEM (Base-64 encoded ASCII) format.

Results

You can now import the generated certificates into your IBM Cognos components.

Import the CA certificates into IBM Cognos components

After you obtain the certificates from the CA, you must import them to your IBM Cognos components.

You must import the certificates on each computer where you have IBM Cognos components installed; including Content Manager, the Application Tier Components, the gateway, and the modeling components.

Tip: The examples in this topic use the default password, `NoPassWordSet`. If you change the **Key store password**, and the **Certificate Authority settings** password in IBM Cognos Configuration, ensure you use the password that you set.

Before you begin

On UNIX or Linux operating systems, ensure that you set a JAVA_HOME environment variable before you use the `ThirdPartyCertificateTool`.

On Microsoft Windows installations, you can run the tool with `-java:local` to use the JRE that is provided with the installation. For example,

```
ThirdPartyCertificateTool.bat -java:local -c -d ...
```

Procedure

1. Create a copy of the crypto certificate and name it `encryptCertificate.cer`.
2. Create a copy of the root CA certificate and name it `ca.cer`.
3. Copy the `encryptCertificate.cer`, and `ca.cer` files to the *`install_location`*`/bin` directory.
4. Import the crypto certificate into the IBM Cognos encryption key store by typing the following command:

   On UNIX or Linux operating systems, type

   ```
   ThirdPartyCertificateTool.sh -i -e -r encryptCertificate.cer -p
   NoPassWordSet -t ca.cer
   ```

   On Windows operating systems, type

   ```
   ThirdPartyCertificateTool.bat -i -e -r encryptCertificate.cer -p
   NoPassWordSet -t ca.cer
   ```

   Important: Ensure you use the password that you entered when you exported the encryption key in the previous task.

   You can safely ignore any warnings about logging.

   The command reads the `encryptCertificate.cer` and `ca.cer` files in the *`install_location`* `\bin` directory and imports the certificates from both files into the `CAMKeystore` file in the `certs` directory using the specified password.
5. Import the CA certificate into the IBM Cognos trust store by typing the following command:

   On UNIX or Linux operating systems, type

   ```
   ThirdPartyCertificateTool.sh -i -T -r ca.cer -p NoPassWordSet
   ```

   On Windows operating systems, type

   ```
   ThirdPartyCertificateTool.bat -i -T -r ca.cer -p NoPassWordSet
   ```

   The command reads the `ca.cer` file and imports the contents into the `CAMKeystore` file in the `certs` directory using the specified password.

Results

You can now configure your IBM Cognos components to use your CA certificates.

Configure IBM Cognos components to use certificates generated by your CA

After you import the CA certificates, you use IBM Cognos Configuration to configure each computer where an IBM Cognos component is installed to use the certificate.

Note: Ensure that the key store locations and passwords in IBM Cognos Configuration match the ones that you typed in the command-line tool. For example, if you change the **Encryption key store password**, and the **Certificate Authority key store password** in IBM Cognos Configuration, ensure you use the password that you set.

Procedure

1. Start IBM Cognos Configuration.
2. In the **Explorer** window, under **Security** > **Cryptography**, click **Cognos**.
3. Click the **Value** box next to **Use third party CA**, and select **True**.

   When you set this property to true, all properties for the certificate authority and identity name are ignored.
4. Enter the password that you used for the crypto key in **Encryption key store password**, and enter the path for the **Encryption key store location**. If you used the same values in the examples in the previous tasks, you do not have to change the path.
5. Enter the **Certificate Authority key store password**.
6. Click **File** > **Save**.
7. Restart your IBM Cognos services.

Configuring the SSL protocol for IBM Cognos components

You can use the Secure Sockets Layer (SSL) protocol for communication between IBM Cognos components in single server and distributed installations.

IBM WebSphere Liberty Profile connectors

If the internal dispatcher URI is prefixed with http but the external dispatcher URI is prefixed with https, or vice versa, both the non-SSL Liberty HTTP/1.1 and SSL Liberty HTTP/1.1 connectors are enabled in the `server.xml` file.

If the internal and external dispatcher URIs use different protocols or ports, the internal dispatcher port is accessible only to the components on the local computer. The internal dispatcher URI must also specify localhost.

Single computer installations

In a single computer installation, if you are not currently using SSL, you must stop the service before changing the protocol to https. After you save the configuration with SSL settings, you can restart the services.

Distributed installations

In distributed installation, you must first configure the default active Content Manager computer to use the SSL protocol and start the services on that computer before you configure the Application Tier and gateway components to use SSL.

Add a computer to an installation

If you add a computer to an SSL-enabled environment, you will be prompted to temporarily accept trust for a certificate when you save the configuration. Accepting the temporary certificate will allow permanent trust to be established with the existing components.

Add a component to a computer

If you add a component to an installation that has already been configured for SSL, the trust to the SSL certificates is inherited from the existing components. If you add the component to a different location on the same computer but to an environment already configured for SSL, you will be prompted to temporarily accept trust for a certificate when you save the configuration. Accepting the temporary certificate will allow permanent trust to be established with the existing components.

Configuring SSL for IBM Cognos components

For IBM Cognos components, you can use SSL for internal connections, external connections, or both.

If you configure SSL for internal connections only, IBM Cognos components on the local computer communicate using this protocol. The dispatcher listens for secure connections on a different port than for remote, HTTP requests. Therefore, you must configure two dispatcher URIs.

If you configure SSL for external connections only, communications from remote IBM Cognos components to the local computer uses the SSL protocol. You must configure the dispatcher to listen for secure, remote requests on a different port than local, HTTP requests. You must also configure the Content Manager URIs and the dispatcher URI for external applications to use the same protocol and port as the external dispatcher.

If you configure SSL for all connections, the dispatcher can use the same port for internal and external connections. Similarly, if you do not use SSL for local or remote communication, the dispatcher can use the same port for all communications.

By default, IBM Cognos Analytics components use an internal certificate authority (CA) to establish the root of trust in the IBM Cognos security infrastructure. This applies to both SSL and non-SSL connections. If you want to use certificates that are managed by another service, see "Configuring IBM Cognos components to use another certificate authority" on page 117.

In distributed installation, you must first configure the default active Content Manager computer to use the SSL protocol and start the services on that computer before you configure the Application Tier Components computer.

Procedure

1. Start IBM Cognos Configuration.
2. In the **Explorer** window, click **Environment**.
3. In the **Properties** window, type the appropriate values for the URI values:

   Important: For HTTPS/SSL configurations, make sure to use a fully qualified hostname for URIs. Also, in the Explorer window, under **Security** > **Cryptography** > **Cognos** > **Identity name**, change the **Server common name** from CAMUSER to the fully qualified domain name of the server.

   - To configure SSL for internal connections only, enter `https` and a port number for SSL communication in the **Internal dispatcher URI** property.

     For the **External dispatcher URI** and **Dispatcher URI for external applications** properties, leave `http` as the protocol and use the default or another available port number.

     If you use the application server that is provided with IBM Cognos Analytics, the **Internal dispatcher URI** property must specify `localhost`.

     The port number in the two dispatcher URIs must be different.

   - To configure SSL for external connections only, enter `https` and a port number for SSL communication in the **External dispatcher URI** and **Dispatcher URI for external applications** properties.

     For the **Internal dispatcher URI** property, leave `http` as the protocol and use the default or another available port number.

     If you use the application server that is provided with IBM Cognos Analytics, the **Internal dispatcher URI** property must specify `localhost`.

     The port numbers in the two dispatcher URIs must be different.

   - To configure SSL for all connections, enter the same URI for both the **Internal dispatcher URI**, **External dispatcher URI**, and **Dispatcher URI for external applications** properties. Enter `https` and a port number for SSL communication.
   - Additionally, you can enter `https` and a port number for SSL communication in the **Content Manager URI** property.

- If you installed the gateway on a separate computer, and you are using SSL for external connections, in IBM Cognos Configuration on the gateway computer, enter `https` and the port number for SSL communication in the **Dispatcher URIs for gateway** property.

4. From the **File** menu, click **Save**.
5. Restart your services.

   In a distributed environment, start the services on the Content Manager computer first, followed by the services on the Application Tier Components computers.

Set up shared trust between IBM Cognos servers and other servers

If you want to use the default IBM Cognos certificate authority and you want to use SSL for connections from other servers to IBM Cognos servers, you must add the IBM Cognos certificate to the trust store on the other servers.

Note: If you use browsers to connect to IBM Cognos components, the browsers automatically prompt users to update their trust stores.

If you want the connection between IBM Cognos servers and the other server to be mutually authenticated, you must also copy the certificate from your certificate authority to the trust store for IBM Cognos servers.

If you have configured IBM Cognos components to use another certificate authority (CA), you do not have to set up shared trust between IBM Cognos server and other servers.

Copying the IBM Cognos certificate to another server

The first task in adding the IBM Cognos certificate to the trust store on other servers is to copy the certificate to the server.

Procedure

1. Go to the *install_location*/bin directory.
2. Extract the IBM Cognos certificate by typing the following command:
   - On UNIX or Linux operating systems, type

     ```
     ThirdPartyCertificateTool.sh -E -T -r destination_file -p NoPassWordSet
     ```
   - On Microsoft Windows operating systems, type

     ```
     ThirdPartyCertificateTool.bat -E -T -r destination_file -p NoPassWordSet
     ```
3. Import the certificate to the trust store on your server.

   For information on updating the server trust store, see the documentation for your server.

Copying the CA certificate to IBM Cognos servers

After copying the IBM Cognos certificate to the other servers, copy the certificate from the certificate authority to the IBM Cognos server.

Procedure

1. Copy the certificate from your certificate authority to a secure location on the IBM Cognos server.

   Ensure that the CA certificate is in Base-64 encoded X.509 format.
2. Import the CA certificate by typing the following command:
   - On UNIX or Linux operating systems, type the following:

     ```
     ThirdPartyCertificateTool.sh -T -i -r CA_certificate_file -p NoPassWordSet
     ```
   - On Microsoft Windows operating systems, type

     ```
     ThirdPartyCertificateTool.bat -T -i -r CA_certificate_file -p NoPassWordSet
     ```

Select and rank cipher suites for Secure Socket Layer

An SSL connection begins with a negotiation in which the client and server present a list of supported cipher suites in a priority sequence. A cipher suite provides the quality of protection for the connection. It contains cryptographic, authentication, hash, and key exchange algorithms. The SSL protocol selects the highest priority suite that the client and the server both support.

A list of supported cipher suites for SSL is provided. You can eliminate cipher suites that do not meet your requirements and then assign a priority, or preference, to the remaining cipher suites. The selected cipher suites are presented in priority sequence for the client and server sides of the negotiation. At least one of the selected cipher suites between the client and server platforms must match.

The list of supported cipher suites is dynamically generated on each computer, and depends on the Java Runtime Environment (JRE) or whether you have other cryptographic software installed on the computer. If you have made changes to a computer, such as upgraded the JRE or installed software that has upgraded the JRE, this may affect the supported cipher suites available on that computer. If you no longer have a supported cipher suite that matches the other computers in your environment, you may have to change the JRE on the computer to match the other computers in your environment.

Procedure

1. Start IBM Cognos Configuration.
2. In the **Explorer** window, click **Cryptography** > **Cognos**.
3. In the **Properties** window, click the **Value** column for the **Supported ciphersuites** property.
4. Click the edit icon ✏.
   - To move a cipher suite to the **Current values** list, click the check box in the **Available values** list and then click **Add**.
   - To move a cipher suite up or down in the **Current values** list, click the check box and then click the up or down arrows.
   - To remove a cipher suite from the **Current values** list, click the check box and then click **Remove**.
5. Click **OK**.
6. From the **File** menu, click **Save**.

Use secure sockets layer (SSL) protocol for database connections in IBM Cognos Configuration

You can configure IBM Cognos Analytics to use the secure sockets layer (SSL) protocol for communication to databases used by IBM Cognos Analytics, including the content store, notification, and logging databases.

SSL must be enabled on the database server and the database clients must be configured to use SSL connections to the database server before you enable it in IBM Cognos Configuration.

SSL support is available for all supported databases except for IBM Db2 for z/OS.

Db2

You can use SSL for Db2 version 9.1 Fix Pack 2 and later versions.

For information about configuring Db2 for SSL connections, see the documentation for your version of Db2.

For example, for version 10.5, see the IBM Db2 version 10.5 documentation (pic.dhe.ibm.com/infocenter/db2luw/v10r5/index.jsp?topic=%2Fcom.ibm.db2.luw.admin.sec.doc%2Fdoc%2Fc0053514.html).

IBM Informix

For information about configuring IBM Informix for SSL connections, see the documentation for your version of IBM Informix.

For example, for version 12.10, see the IBM Informix version 12.10 documentation (pic.dhe.ibm.com/infocenter/informix/v121/index.jsp?topic=%2Fcom.ibm.sec.doc%2Fids_ssl_001.htm).

Oracle

For information about configuring Oracle for SSL connections, see the documentation for your version of Oracle.

The SSL With Oracle JDBC Thin Driver white paper (www.oracle.com/technetwork/database/enterprise-edition/wp-oracle-jdbc-thin-ssl-130128.pdf) published by Oracle provides information for configuring SSL for the database server and client.

Microsoft SQL Server

For information about configuring Microsoft SQL Server for SSL connections, see the documentation for your version of Microsoft SQL Server.

For example, for version 2012, see the Microsoft SQL Server version 2012 documentation (technet.microsoft.com/en-us/library/bb879949.aspx).

Note: After you enable SSL on the database server, you can set **SSL Encryption Enabled** to **True** in IBM Cognos Configuration.

Using SSL for database connections in IBM Cognos Configuration for Microsoft SQL Server

To use secure sockets layer (SSL) for database connections in IBM Cognos Configuration, you must import the SSL certificate to the Java keystore and then modify some IBM Cognos configuration files. For information about configuring Microsoft SQL Server for SSL connections, see the documentation for your version of Microsoft SQL Server.

You can use SSL for database connections in IBM Cognos Configuration, including the content store, notification, logging databases, Human Task and Annotation Services, and Cognos Mobile.

The Microsoft JDBC driver **replaces** the JSQLConnect driver for SQL Server. From version forward you must download, from Microsoft, and put the new type 4 driver in the `*install_location*/drivers` folder.

Note: There are different driver JAR file names, such as `sqljdbc4.jar`, `sqljdbc41.jar` and `sqljdbc42.jar`. Officially, `sqljdbc42.jar` supports JRE8, which is the version Cognos Analytics ships with.

Before you begin

Ensure that you enable SSL on your database server before you configure IBM Cognos to use SSL for the database connections.

Ensure that you export the SSL certificate from your database server and have it available on the computer where you are configuring the database connection in IBM Cognos Configuration.

Procedure

1. If you are using an SQL server that is configured for SSL as your content store database, follow these steps:

   a) Obtain the root Certificate Authority certificate that issued your SQL Server's certificate (or the self-signed server certificate if it was not issued by a Certificate Authority), and copy to the computer where Cognos Analytics is installed. For example, copy the file `sqlcert.cer` to the root directory, `c:\sqlcert.cer`

   b) Type cd C:\Program Files\ibm\cognos\analytics\jre\lib\security

   c) Type , for example, C:\Progra~1\ibm\cognos\analytics\jre\bin\keytool -import -trustcacerts -file "c:\sqlcert.cer" -keystore cacerts -alias SQLCert

2. Edit *install_location*\bin64\startwlp.bat (Windows) or *install_location*\bin64\startwlp.sh (Linux, UNIX) to add the following lines after the line set JVM_ARGS=-Xmx4096m -XX:MaxNewSize=2048m -XX:NewSize=1024m %DEBUG_OPTS%:

   Windows:

   ```
   set JVM_ARGS="-Dcom.ibm.jsse2.overrideDefaultTLS=true" %JVM_ARGS%
   set JVM_ARGS="-Dcom.ibm.jsse2.sp800-131=strict" %JVM_ARGS%
   ```

   Linux, UNIX:

   ```
   JVM_ARGS=-Dcom.ibm.jsse2.overrideDefaultTLS=true $JVM_ARGS
   JVM_ARGS=-Dcom.ibm.jsse2.sp800-131=strict $JVM_ARGS
   ```

3. Edit *install_location*\bin64\bootstrap_wlp_*os_version*.xml to add the following lines after the line <param condName="${java_vendor}" condValue="IBM">-Xscmaxaot4m</param>:

   Windows:

   ```
   <param>"-Dcom.ibm.jsse2.overrideDefaultTLS=true"</param>
   <param>"-Dcom.ibm.jsse2.sp800-131=strict"</param>
   ```

   Linux, UNIX:

   ```
   <param>-Dcom.ibm.jsse2.overrideDefaultTLS=true</param>
   <param>-Dcom.ibm.jsse2.sp800-131=strict</param>
   ```

4. Edit *install_location*\bin64\cogconfig.bat (Windows) or *install_location*\bin64\cogconfig.sh (Linux, UNIX) to add the following lines after the line set J_OPTS=%DD_OPTS% %J_OPTS%:

   Windows:

   ```
   set J_OPTS="-Dcom.ibm.jsse2.overrideDefaultTLS=true" %J_OPTS%
   set J_OPTS="-Dcom.ibm.jsse2.sp800-131=strict" %J_OPTS%
   ```

   Linux, UNIX:

   ```
   JAVA_OPTS=$JAVA_OPTS -Dcom.ibm.jsse2.overrideDefaultTLS=true
   JAVA_OPTS=$JAVA_OPTS -Dcom.ibm.jsse2.sp800-131=strict
   ```

5. Start Cognos Configuration using cogconfig.bat or cogconfig.sh you modified in the previous step.

   Important: You must start IBM Cognos Configuration using cogconfig.bat (that you modified to include the keystore and password) and not the usual executable (cogconfigw.exe) or start menu shortcut.

6. Under **Data Access**, under the database connection type, select the database connection.
7. Select **True** for **SSL Encryption Enabled**.
8. Test the connection, and save your configuration.
9. Start Cognos Analytics. You will have to match the full server name in SQL Server Configuration Manager to the one in the certificate (for example, mymachine.canlab.ibm.com instead of localhost).

Results

Important: For single sign-on (SSO) and Windows authentication, you need to put `sqljdbc_auth.dll` in the `bin64` directory. Windows authentication is a single sign-on setup. The selection in Configuration Manager for the Content Manager is called **Microsoft SQL Server database (Windows Authentication)**.

Using SSL for database connections in IBM Cognos Configuration for an IBM Db2, Informix database

To use secure sockets layer (SSL) for database connections in IBM Cognos Configuration, you must import the SSL certificate to the Java keystore and then modify some IBM Cognos configuration files.

You can use SSL for database connections in IBM Cognos Configuration, including the content store, notification, and logging databases.

Before you begin

Ensure that you enable SSL on your database server before you configure IBM Cognos to use SSL for the database connections.

Ensure that you export the SSL certificate from your database server and have it available on the computer where you are configuring the database connection in IBM Cognos Configuration.

Procedure

1. Follow the documentation for your database version to enable SSL for the database server and to export the SSL certificate.
2. Download unlimited strength policy jar files.

   For IBM JRE, go to https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=jcesdk (https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=jcesdk) and download `unrestrictedpolicyfiles.zip`. Unzip the policy files to `*install_location*/jre/lib/security`.
3. On the computer where you are configuring the database connection, import the SSL certificate with the keytool for the JRE that you are using for IBM Cognos Analytics.
   For example, if you are using the JRE that is provided with IBM Cognos Analytics installations on Microsoft Windows operating systems, do the following steps:
   a) Go to the `*install_location*/jre/bin` directory.
   b) Run the following command.

   ```
   keytool -import -file path/filename -keystore keystorename -alias aliasname
   ```

   Where *keystorename* is a name for a new keystore, and *aliasname* is an alias that you choose for the certificate.
   c) Enter a password for your keystore. If you are adding the certificate to an existing keystore, enter that keystore's password. If you are creating a new keystore, enter a password for the new keystore.

   Important: The SSL certificate must be imported to the keystore for the JRE that you are using for IBM Cognos Analytics.
4. Edit the `java.security` file to include the SSL provider.
   a) If you are using the JRE that is provided with IBM Cognos Analytics installations on Microsoft Windows operating systems, go to the `*install_location*/jre/lib/security` directory. Otherwise, go to the `lib/security` directory for the JRE you are using for IBM Cognos Analytics.
   b) Open `java.security` in a text editor.
   c) Locate the following lines in the file.

   ```
   ssl.KeyManagerFactory.algorithm=IbmX509
   ssl.TrustManagerFactory.algorithm=PKIX
   ```

   d) Add the following lines after the previous lines.

```
ssl.SocketFactory.provider=com.ibm.jsse2.SSLSocketFactoryImpl
ssl.ServerSocketFactory.provider=com.ibm.jsse2.SSLServerSocketFactoryImpl
```

   e) Save and close the file.

5. Edit the IBM Cognos `startwlp` file. This file is used when you start IBM Cognos Analytics.
   a) Go to the *`install_location`*`/bin64` directory.
   b) Open the `startwlp.bat` file in a text editor. On UNIX or Linux operating systems, open the `startwlp.sh` file.
   c) Locate the following line in the file.

   Windows:

```
set JVM_ARGS=-Dcom.ibm.cognos.disp.useDaemonThreads=true %JVM_ARGS%
```

   Linux, UNIX:

```
DISP_OPTS="-Dcom.ibm.cognos.disp.useDaemonThreads=true"
```

   d) Add the following lines after the previous lines.

   Windows:

```
set JVM_ARGS=-Dcom.ibm.jsse2.usefipsprovider=true %JVM_ARGS%
set JVM_ARGS=-Djavax.net.ssl.trustStore=path/keystorename %JVM_ARGS%
```

   Linux, UNIX:

```
DISP_OPTS="-Dcom.ibm.jsse2.usefipsprovider=true %DISP_OPTS%"
DISP_OPTS="-Djavax.net.ssl.trustStore=path/keystorename"
```

   Where *path* is the path to the keystore, and *keystorename* is the name of the keystore.

   e) Save and close the file.

6. Edit the `bootstrap_wlp_`*`os_version`*`.xml` file. This file is used when you start IBM Cognos Analytics as a service from IBM Cognos Configuration.
   a) Go to the *`install_location`*`/bin64` directory.
   b) Open the `bootstrap_wlp_`*`os_version`*`.xml` file in a text editor.
   c) Add the following lines to the file.

```
<param>"-Dcom.ibm.jsse2.usefipsprovider=true"</param>
<param>"-Djavax.net.ssl.trustStore=path/keystorename"</param>
```

   Where *`path`* is the path to the keystore, and *`keystorename`* is the name of the keystore.

   d) Save and close the file.

7. Edit the IBM Cognos `cogconfig` file.
   a) Go to the *`install_location`*`/bin64` directory.
   b) Open the `cogconfig.bat` file in a text editor. On UNIX or Linux operating systems, open the `cogconfig.sh` file.
   c) Locate the following line in the file.

   Windows:

```
J_OPTS=%DD_OPTS% %J_OPTS% %DEBUG_OPTS%
```

   Linux, UNIX:

```
$JAVA_CMD $JAVA_OPTS CRConfig $*
```

d) Add the following lines after the previous lines.

Windows:

```
set J_OPTS=-Dcom.ibm.jsse2.usefipsprovider=true %J_OPTS%
set J_OPTS=-Djavax.net.ssl.trustStore=path/keystorename %J_OPTS%
```

Linux, UNIX:

```
JAVA_OPTS="$JAVA_OPTS -Dcom.ibm.jsse2.usefipsprovider=true %JAVA_OPTS%"
JAVA_OPTS="$JAVA_OPTS -Djavax.net.ssl.trustStore=path/keystorename"
```

Where *path* is the path to the keystore, and *keystorename* is the name of the keystore.

e) Save and close the file.

8. Start IBM Cognos Configuration by using the `cogconfig` file that you modified.
   - On Microsoft Windows operating systems, double-click the `cogconfig.bat` file that you modified.
   - On UNIX or Linux operating systems, run the `cogconfig.sh` file that you modified.
9. Under **Data Access**, under the database connection type, select the database connection.

   You can use SSL for connections to the content store database, notification database, logging database, and human task and annotation databases.
10. Select **True** for **SSL Encryption Enabled**.
11. Test the connection.
12. Save your configuration, and restart your services.

Using SSL for database connections in IBM Cognos Configuration for an Oracle database

To use secure sockets layer (SSL) for database connections in IBM Cognos Configuration, you must import the SSL certificate to the Java keystore and then modify some IBM Cognos configuration files.

You can use SSL for database connections in IBM Cognos Configuration, including the content store, notification, and logging databases.

Before you begin

Ensure that you enable SSL on your database server before you configure IBM Cognos to use SSL for the database connections.

Procedure

1. Edit the IBM Cognos `startwlp` file.

   a) Go to the *install_location*/bin64 directory.

   b) Open the `startwlp.bat` file in a text editor. On UNIX or Linux operating systems, open the `startwlp.sh` file.

   c) Add the following lines to the file.

   ```
   set JVM_ARGS=-Doracle.net.ssl_version=3 %JVM_ARGS%
   set JVM_ARGS=-Doracle.net.ssl_client_authentication=false %JVM_ARGS%
   set JVM_ARGS=-Doracle.net.wallet_location=(SOURCE=(METHOD=file)
   (METHOD_DATA=(DIRECTORY=path/client_wallet))) %JVM_ARGS%
   ```

   The *path* parameter is the path to the Oracle wallet directory for the client, and the *client_wallet* parameter is the name of the wallet directory for the client.

   d) Save and close the file.
2. Edit the `bootstrap_wlp_os_`*`version`*`.xml` file.

   This file is used when you start IBM Cognos Analytics as a service from IBM Cognos Configuration.

   a) Go to the *install_location*/bin64 directory.

b) Open the `bootstrap_wlp_`*`os_version`*`.xml` file in a text editor.

c) Add the following lines to the file.

```
<param>-Doracle.net.ssl_version=3</param>
<param>-Doracle.net.ssl_client_authentication=false</param>
<param>-Doracle.net.wallet_location=(SOURCE=(METHOD=file)(METHOD_DATA=(DIRECTORY=path/
client_wallet)))</param>
```

Java parameters in this file should be the same as in step 1.

Tip: Using double quotes in the `bootstrap_wlp_linux38664.xml` file prevents IBM Java from starting, and causes Cognos startup to hang and fail.

d) Save and close the file.

3. Edit the IBM Cognos `cogconfig` file.

a) Go to the *`install_location`*`/bin64` directory.

b) Open the `cogconfig.bat` file in a text editor. On UNIX or Linux operating systems, open the `cogconfig.sh` file.

c) Add the following lines to the file.

```
set J_OPTS=-Doracle.net.ssl_version=3 %J_OPTS%
set J_OPTS=-Doracle.net.wallet_location=(SOURCE=(METHOD=file)
(METHOD_DATA=(DIRECTORY=path/client_wallet))) %J_OPTS%
set J_OPTS=-Doracle.net.ssl_client_authentication=false %J_OPTS%
```

d) Save and close the file.

4. Copy the following Oracle driver files to the *`install_location`*`/drivers` directory.

- `jssl-1_1.jar`
- `oraclepki.jar`
- `osdt_cert.jar`
- `osdt_core.jar`

5. Start IBM Cognos Configuration.

6. Under **Data Access**, for the database connection type, select the database connection.

You can use SSL for connections to the content store database, notification database, logging database, and human task and annotation databases.

Tip: Ensure that the connection uses the **Oracle database (Advanced)** type. If you did not select the **Oracle database (Advanced)** type, delete the database connection, and create a new one that uses **Oracle database (Advanced)**.

7. Select **True** for **SSL Encryption Enabled**.

8. Test the connection.

9. Save your configuration, and restart your services.

Configure JDBC data source connections for single sign-on using Kerberos

You can configure single sign-on using the Kerberos protocol for JDBC data source connections that are used for dynamic query mode (DQM).

Except for Microsoft SQL Server, single sign-on data source authentication is supported only for dynamic query mode.

Support for constrained delegation (a Microsoft extension to Kerberos), allows a service to obtain a ticket for another service on behalf of the user by presenting the user's service ticket to itself. The service ticket is either delegated from the user (Service for User to Proxy - S4U2Proxy), or generated by the service itself when user is authenticated by different means.

To configure a data source for single sign-on authentication using Kerberos, you must

- Create a Kerberos initialization file.
- Configure a service principal name (SPN) for the dynamic query mode data source.
- Create a keytab file.
- Configure the Kerberos login module.
- Configure data source connections.

Before you start, you must ensure that the following conditions are met:

1. The IBM Cognos service is configured for single sign-on using a Microsoft Active Directory namespace.
2. The database is configured to use the Kerberos protocol.
3. The Active Directory users are also configured on the database server.
4. If single sign-on is configured with constrained delegation, check the driver documentation to ensure the driver supports constrained delegation. Not all drivers that support Kerberos authentication also support constrained delegation.

   Dynamic query supports Kerberos constrained delegation with the JDBC drivers for Netezza and Cloudera Impala. This capability requires JDBC drivers of the following versions or higher which have been enhanced to receive GSS credentials.: Netezza 7.2.0.9-P3 and 7.2.1.3-P3 (see http://www-01.ibm.com/support/docview.wss?uid=swg21997658 for more information), and Cloudera Impala 2.5.36

   IBM Cognos Analytics can be used with either an ORACLE or IBM JRE. The versions IBM requires are found in the supported environments page. Persons trying to use Cognos Analytics with an IBM JRE and Cloudera Impala JDBC would need to use IBM JRE 8.0.3.12 or above. See https://developer.ibm.com/javasdk/downloads/sdk8/.

Using Kerberos authentication without single sign-on

If you don't configure Active Directory namespace, you still can configure your data source for Kerberos authentication. The dynamic query mode query service interprets the credentials that you provide (user name and password) as the credentials for obtaining a ticket granting ticket (TGT) from the Kerberos Distribution Center (Active Directory or another Kerberos implementation). These credentials can be provided through a signon or entered by the user when prompted for database credentials. In this case, configuration steps change as follows:

- You do not have to register an SPN.
- You do not have to create a keytab file.
- You **do not** have to configure the Kerberos Login Module.
- You have to supply a Kerberos initialization file.

Creating Kerberos initialization files

You must create a Kerberos initialization file and place it in a specific location on all computers with Application Tier Components installed. The Kerberos initialization file, `krb5.conf` is used by the JRE Kerberos protocol implementation.

For more information about Kerberos initialization files, see the MIT Kerberos Documentation (web.mit.edu/kerberos/krb5-devel/doc/admin/conf_files/krb5_conf.html).

Procedure

On all computers where you have Application Tier Components installed, copy the `krb5.conf` file to the `JAVA_HOME/lib/security` directory.

On computers running UNIX, copy the `krb5.conf` file to the `/etc/krb5` directory.

On computers running Linux, copy the `krb5.conf` file to the `/etc` directory.

On computers running Microsoft Windows, copy the `krb5.conf` file to the `C:\winnt` directory, and rename it to `krb5.ini`

Creating an SPN for the query service

You must create a service principal name (SPN) for the query service to use. The SPN must be configured with an Active Directory domain user that is trusted for delegation.

The SPN must be formatted as `spn@REALM`. The spn value is formatted as *`service name/fully qualified domain name`*. And `REALM` is the realm name that is configured in the Kerberos initialization file. For example, if dqm is the service name, `dqm/myserver.mydomain.com@MYWINDOWSDOMAIN.COM`.

If your Active Directory domain user is named dqmuser, you would register the SPN by using the following command:

```
setspn -s dqm/myserver.mydomain.com mywindowsdomain\dqmuser
```

You can use the -L and -Q parameters to verify that the SPN was created correctly. For example:

```
setspn -L mywindowsdomain\dqmuser
```

```
setspn -Q dqm/myserver.mydomain.com
```

Creating a keytab file

After you create the SPN, you must create a keytab file for the service. The keytab file allows the service to log in without a password. The keytab file must be re-created if the service account password changes.

Procedure

Use the following command to create a keytab file:

```
ktpass -out krb5.keytab -princ SPN -mapUser username -mapOp set -pass password
-pType KRB5_NT_PRINCIPAL -crypto RC4-HMAC-NT
```

For example,

```
ktpass -out krb5.keytab -princ dqm/myserver.mydomain.com@mywindowsdomain.com -
mapUser dqmuser@mywindowsdomain -mapOp set -pass password -pType
KRB5_NT_PRINCIPAL -crypto RC4-HMAC-NT
```

Configuring the Kerberos login module

You must configure the Kerberos login module to allow the IBM Cognos query service to log in to the Active Directory domain. To allow the log in the Java Authentication and Authorization Service (JAAS) package requires a configuration file.

There are two possible procedures in configuring the login modules.

To configure the login module for Kerberos with single sign-on (Active Directory):

1. In Cognos Configuration, select the Active Directory namespace in **Security** > **Authentication**.
2. In the **DQM Service Principal Name** property, enter the value exactly as it is listed in the keytab.

   Use the command `klist -k <keytab file>` to find the principal name.
3. Rename the keytab file to `ibmcognosba.keytab`, and place it in the *`install_location`*`/configuration` folder.

Cognos Analytics will dynamically create the necessary login configuration.

A configuration file must be included in the `java.security` file in the *`JRE_HOME`*`/lib/security` directory. You must include a line such as the following in the `java.security` file.

```
login.config.url.1=file:///${java.home}/lib/security/jaas.conf
```

JAAS configuration examples are provided in the IBM Cognos installation. The example files are named `jaas-ibm.config` and `jaas-oracle.config`, and the files are in the *`install_location`* `\configuration` directory.

In the example files, you must replace the following values:

- *`<principal name>`* is the SPN that you created.
- *`<keytab file specification>`* is the path and file name of the keytab file that you created.

If you are not using a database connection that is configured for Kerberos authentication for modeling, then instead of modifying the `java.security` file, you can specify the JAAS login configuration file as an additional startup parameter for query service in IBM Cognos Administration. In IBM Cognos Administration, under **System**, expand your server, select **Query Service** > **Set Properties** > **Settings**, and enter the value in **Additional JVM arguments for the query service** in the form `-Djava.security.auth.login.config=`*<configuration file>*

Verifying the Kerebos configuration

To verify the Java Authentication and Authorization Service (JAAS) configuration and the keytab file, you can run a command using the `java` command from the JRE that Cognos Analytics is using.

Procedure

Run the following command from *`install_location`*`/webapps/p2pd/WEB-INF/lib`

```
java -cp xqeService.jar -Dcom.ibm.security.krb5.Krb5Debug=all -
Dcom.ibm.security.jgss.debug=all com.cognos.xqe.util.KerberosSSOLoginHelper
```

The utility will attempt a login using the keytab file, and in the process will display the Kerberos debug output. At the end, it will display `Helper login successful` or `Helper Login failed <error message>`.

Verifying the JDBC driver capabilities

Regardless of whether single sign-on is configured or not, DQM requires that the database driver can create connections using a pre-authorized subject. There is a utility that comes with the IBM Cognos Analytics installation which can help test the driver.

Before you begin

The utility accepts url, uid and password as parameters. The driver must be installed in the *`install_location`*`/webapps/p2pd/WEB-INF/lib` folder.

Procedure

From the *`install_location`*`/webapps/p2pd/WEB-INF/lib` folder, using the java command from the jre Cognos is using, run the following command:

```
java -cp xqeService.jar;<driver.jar>
com.cognos.xqe.util.KerberosConnectionHelper <driver class name> <jdbc url>
<user> <password>
```

where:

- *<driver.jar>* is the jar file containing the driver. If the driver has too many jar files, you can specify "*" for the classpath parameter.
- *<driver class name>* is the class name used to load the driver.
- *<jdbc url>* is the JDBC connection URL for the data source, including the driver-specific properties for Kerberos authentication.
- *<user>* is the Kerberos principal.
- *<password>* is the Kerberos principal password.

The utility tries to connect to the database using the supplied parameters, and outputs the Kerberos debug trace.

Configuring data source connections when using Kerberos

Use the guidelines in this topic when configuring the connection strings for data source connections using Kerberos single sign-on.

Procedure

1. In the Signon section, select **external namespace** and select the Active Directory namespace from the list. For dual tab (Native and JDBC) connection strings, the Signon section is on the Native tab.
2. In the **Connection properties** field, specify `ibmcognos.authentication=java_krb5`, and then add the properties required by the JDBC driver for Kerberos authentication, if any. For data source connections with dual tab (Native and JDBC), this field is on the **JDBC** tab and is called **JDBC Connection Parameters**.

   If IBM Cognos Analytics is installed on a computer that are running Microsoft Windows operating systems, you do not have to specify `ibmcognos.authentication=java_krb5` for Microsoft SQL Server and Teradata data source connections.
3. Test the data source connection.

Example

The following are examples for data source connection properties for some data sources:

- For Teradata data source connections:

  ```
  ibmcognos.authentication=java_krb5;LOGMECH=KRB5;
  ```
- For SAP-HANA data source connections:

  ```
  ibmcognos.authentication=java_krb5;
  ```
- For Microsoft SQL Server data source connections:

  ```
  ibmcognos.authentication=java_krb5;authenticationScheme=JavaKerberos;
  ```

Configuring a Repository for Log Messages

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

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

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

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

- During planning, determine the logging configuration that is suitable for your environment. For example, evaluate various log message repositories, such as remote log servers and log files, such as the UNIX or Linux syslog or the Windows NT Event log, in addition to the local log file. You can also send only audit logging information to a database. Consider security, such as methods available for protecting log files from system failures and user tampering.

- During configuration, define the startup properties for logging, such as connection settings for databases. You must also create a logging database if you plan to collect audit logs. If communication between a local log server and a remote log server must be secured, make the appropriate configuration changes on both IBM Cognos Analytics computers. You can also enable certain logging features, such as user-specific logging.
- When setting up logging, specify the level of detail to log to focus messages on the information that is relevant in your organization. Audit reports may also be set up to track user and report activity.

  For information about setting up logging, see the *IBM Cognos Analytics Administration and Security Guide*.

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

Guidelines for creating a logging database

You can create a database to store log messages. Creating a logging database involves the following tasks:

- Create a logging database.

  For IBM Db2, Oracle, Microsoft SQL Server, use the same procedure that was used to create the content store database. Use the instructions in Guidelines for creating the content store.

  Note: If you are using Db2, you cannot generate a script to create the notification database in the same way as you can the content store.

  For Db2 on z/OS, use the instructions in “Suggested settings for creating a logging database on Db2 on z/OS” on page 136.
- Set up the database connectivity.

  Use the instructions in “Database connectivity for the logging database” on page 137.
- Specify the log messages repository.

  Use the instructions in “Log message repositories” on page 139.

Suggested settings for creating a logging database on Db2 on z/OS

The database you create must contain the specified configuration settings.

Use the following checklist to help you set up the logging database on Db2 on z/OS.

__ • Log on to the z/OS system as a user with administrator privileges on Db2 on z/OS.

__ • Create a database instance, storage group, and a user account for the content store. IBM Cognos uses the credentials of the user account to communicate with the database server.

__ • Ensure that you allocate a buffer pool with a page size of 8 KB for the database instance.

__ • For a logging database on Db2 on z/OS, administrators must run a tablespace script to create tablespaces to hold large objects and other data for the logging database, and then grant user rights to the table. For information about running the tablespace script, see “Create tablespaces for a logging database on Db2 on z/OS ” on page 136.

Create tablespaces for a logging database on Db2 on z/OS

If you are using IBM Db2 on z/OS, a database administrator must run a script to create a set of tablespaces required for the logging database. The script must be modified to replace the placeholder parameters with ones that are appropriate for your environment.

Ensure that you use the name convention for Db2 on z/OS. For example, all names of parameters must start with a letter and the length must not exceed 6 characters. For more information, see the Db2 Knowledge Center.

Procedure

1. Connect to the database as a user with privileges to create and drop tablespaces and to allow execution of SQL statements.
2. Go to the *install_location*/configuration/schemas/logging/db2zos directory.
3. Open the LS_tablespace_db2zOS.sql script file and use the following table to help you to replace the generic parameters with ones appropriate for your environment.

Table 22: Tablespace parameter names and descriptions for a logging database on Db2 on z/OS

Parameter Name	Description
IPFSCRIPT_DATABASE	The name of the logging database.
IPFSCRIPT_STOGROUP	The name of the storage group.
IPFSCRIPT_TABLESPACE	The name of the tablespace that contains the base tables in the logging database. This tablespace is not for Auxiliary tables.
IPFSCRIPT_LS_ID	The instance identifier for the audit database. This value must not be longer than two characters.
IPFSCRIPT_BP	The name of the 8 k buffer pool that is allocated for regular objects.
IPFSCRIPT_USERNAME	The user account that accesses the logging database.

   Not all of the parameters listed are in the script, but may be added in the future.
4. Save and run the script.
5. Grant the IBM Cognos user rights to the tablespaces that were created when you ran the script file:
   - Open the LS_rightsGrant_db2zOS.sql script file.
   - Replace the parameter values with those that are appropriate for your environment.

     Tip: Ensure you use the same values that you used when you created the buffer pools and user account.
   - Save and run the LS_rightsGrant_db2zOS.sql script.

Results

The logging database is created.

Database connectivity for the logging database

After you create a database for audit logs, additional steps are required to set up the database client if you use Oracle, IBM Db2, Informix Dynamic Server as the database server.

In a distributed environment, the local log server on an Application Tier Component computer may send log messages to a remote log server, which then sends messages to the logging database. For Oracle, and Db2, the appropriate JDBC driver and/or database client software is required only on the Application Tier Components computer with the remote log server that connects to the logging database.

Microsoft SQL Server

If you use a Microsoft SQL Server database, the `JSQLConnect.jar` file is installed to the appropriate location by default. The only additional step is to ensure that the Microsoft SQL Server uses TCP/IP connectivity.

Set up database connectivity for an IBM Db2 logging database

You must set up the database client software and the JDBC driver on all Application Tier Components computers with a connection to the logging database. You must set up the JDBC driver on the Content Manager computer, unless you are using the same type of database for the log messages as you use for the content store.

The driver version must be at least JCC 3.7 for a Linux or UNIX operating system, or for a Microsoft Windows operating system version 9.1 fix pack, or JCC 3.42 for a Linux, UNIX operating system, or for a Microsoft Windows operating system version 9.5 fix pack 2.

Procedure

Copy the following files from *DB2_installation*`\sqllib\java` directory to the *install_location* `\drivers` directory:

- The universal driver file, `db2jcc4.jar`
- The license file:

  For Db2 on Linux, UNIX, or Windows operating systems, use `db2jcc_license_cu.jar`.

  For Db2 on z/OS, use `db2jcc_license_cisuz.jar`.

  If you are connecting to Db2 on z/OS, use the driver version from Linux, UNIX, or Windows version 9.1 fix pack 5 or version 9.5 fix pack 2.

  Tip: To check the driver version, run the following command:

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

Set up database connectivity for an Oracle logging database

You must set up the JDBC driver on all Application Tier Components computers with a connection to the logging database. You must also set up the JDBC driver on the Content Manager computer, unless you are using the same type of database for the log messages as you use for the content store.

Procedure

1. On the computer where the Oracle client is installed, go to the *ORACLE_HOME*`/jdbc/lib` directory.
2. Copy the correct library file for your version of the Oracle client to the *install_location*`\drivers` directory on the computer where Content Manager is installed and where notification is sent to an Oracle database.

   If you are using Oracle 12c, you must have `ojdbc7.jar`.

   If you are using Oracle 11g, you must have `ojdbc5.jar`.

   The files are available from an Oracle client or server install, and can also be downloaded from the Oracle technology Web site.

Set up database connectivity for an Informix logging database

You must set up the JDBC driver on all Application Tier Components computers with a connection to the logging database. You must also set up the JDBC driver on the Content Manager computer, unless you are using the same type of database for the log messages as you use for the content store.

Procedure

1. On the computer where Informix is installed, go to the *Informix_location*`/sqllib/java` directory.

2. Copy the following files to the *install_location*\drivers directory on every computer where Content Manager is installed.
   - the universal driver file, db2jcc4.jar
   - the license file, db2jcc4_license_cisuz.jar

Log message repositories

A local log server is automatically installed when you install Content Manager or the Application Tier Components. You can specify one or more repositories where the local log server sends log messages.

Sending log messages to a remote log server

In a distributed installation, you can configure the log server on each IBM Cognos computer to send log messages to a single remote log server, which acts as a common log server. You can then configure the common log server to send the log messages to a local file or database on the same or different computer.

If the remote log server becomes unavailable, log messages are redirected to recovery files on the local computer in the *install_location*/logs/recovery/remote directory. These recovery files have timestamp information in their file names, and are not readable like regular log files. When the remote log server becomes available, an automatic recovery process moves all log information to the remote log server and deletes the local log files.

Saving log messages to a file

The log server is configured by default to send log messages to the *install_location*/logs/cogaudit.log file. If the default log file does not exist when the IBM Cognos service starts, it is created automatically.

You can configure the log server to send log messages to a different file. If you configure a different log file, IBM Cognos attempts to automatically create this file on startup, in addition to the default log file. If the location for the configured log file is different from the *install_location*/logs directory, you must ensure the path to the log file exists before starting the IBM Cognos service. For example, if you configure the log server to send messages to the /usr/lpp/logfiles/cognos.log file, IBM Cognos attempts to automatically create the cognos.log file in the /usr/lpp/logfiles folder. If this folder does not exist, IBM Cognos does not create the cognos.log file and no log messages can be recorded in it. Note that these log messages are not recorded in the default log file. Although IBM Cognos automatically creates the default log file even when another log file is configured, the default log file is not used as a backup.

Saving log messages to a database

The log server can also send audit logs to a database on the same or another computer. Audit logs provide information about user and report activity.

The logging database has the same configuration and user account requirements as the content store database. After you configure IBM Cognos components to send messages to a logging database, and restart the IBM Cognos service, IBM Cognos components create the required tables and table fields. You can test the connection to the logging database before you restart the IBM Cognos service.

Specify the Log Messages Repository for IBM Db2 on UNIX, Linux, or Windows

You can configure a type of repository for the log messages, and then configure properties for the specific repository. You can also configure more than one repository for log messages.

Before you begin

Before you specify a database as a repository, ensure that you

__ • created the logging database

__ • set up the database client

Procedure

1. On the computer where you installed Content Manager or the Application Tier Components, start IBM Cognos Configuration.
2. In the **Explorer** window, under **Environment**, click **Logging**.
3. In the **Properties** window, use the following table to help set the log server properties.

   Table 23: Log server properties

Task	Action
Use TCP between IBM Cognos components on a computer and its local log server	Set the **Enable TCP** property to **True**. UDP provides faster communication with a lower risk of lost connections than TCP. However, the risk of losing a local TCP connection is low. TCP is always used for communication between a local log server and a remote log server.
Change the number of threads available to the local log server	Type the value in the **Local log server worker threads** property. Keep the default value of 10. The range is between 1 and 20. However, if you have a high number of log messages, you can allocate more threads to improve performance.

4. In the **Explorer** window, under **Environment**, right-click **Logging**, and click **New resource** > **Destination**.
5. In the **Name** box, type the name of the repository.
6. In the **Type** list, click the type of repository and then click **OK**.
7. If the repository is a file, in the **Properties** window, type the appropriate values for the mandatory and optional properties.
8. If the repository is a remote log server, in the **Properties** window, type the appropriate values for the mandatory and optional properties.

   If the **Internal dispatcher URI** of the repository computer is configured to use SSL, in the **Properties** window, set the **Enable SSL** property to **True**.

   You must later specify the log messages repository when you configure the remote log server.
9. If the repository is a database, in the **Explorer** window, under **Logging**, specify the type of database and its properties, as follows:

   - Right-click the database name, and click **New resource** > **Database**.
   - In the **Name** box, type the name of the repository.
   - In the **Type** list, click the type of database and then click **OK**.

- In the **Properties** window, type the appropriate values for the mandatory and optional properties.

  For a Microsoft SQL Server database, you can choose to use a port number, such as 1433, or a named instance as the value for the **Database server with port number or instance name** property. Include the port number if you use nondefault ports. Include the instance name if there are multiple instances of Microsoft SQL Server.

  To connect to a named instance, you must specify the instance name as a JDBC URL property or a data source property. For example, you can type **localhost\instance1**. If no instance name property is specified, a connection to the default instance is created.

  Note that the properties specified for the named instance, along with the user ID and password, and database name, are used to create a JDBC URL. Here is an example:

  jdbc:JSQLConnect://localhost\\instance1/user=sa/*more properties as required*
- Test the connection to the new database. In the **Explorer** window, under **Environment**, right-click **Logging** and click **Test**.

  IBM Cognos components connect to the database. If you configured more than one database for logging messages, IBM Cognos components test all the databases.

10. Repeat steps 5 to 10 for each repository to which you want the log server to send messages.
11. From the **File** menu, click **Save**.
12. In the **Explorer** window, click **IBM Cognos services** > **IBM Cognos**.
13. From the **File** menu, click **Restart**.

    If you selected a database as the repository, IBM Cognos components create the required tables and fields in the database that you created.

Results

If the repository was a remote log server, configure and start the remote log server. Then restart the IBM Cognos service on the local computer.

If the repository was a database, you can use IBM Cognos components to run log reports from the database.

You can also set the logging level, which controls the amount of detail and type of messages that are sent to a log file or database. For instructions, see the *IBM Cognos Analytics Administration and Security Guide*.

Specify the Log Messages Repository for IBM Db2 on z/OS

You can configure a type of repository for the log messages, and then configure properties for the specific repository. You can also configure more than one repository for log messages.

Procedure

1. On the computer where you installed Content Manager or the Application Tier Components, start IBM Cognos Configuration.
2. In the **Explorer** window, under **Environment**, click **Logging**.
3. In the **Properties** window, use the following table to help set the log server properties.

Table 24: Log server properties

Task	Action
Use TCP between IBM Cognos components on a computer and its local log server	Set the **Enable TCP** property to **True**. UDP provides faster communication with a lower risk of lost connections than TCP. TCP is used for communication between a local log server and a remote log server.

Table 24: Log server properties (continued)

Task	Action
Change the number of threads available to the local log server	Type the value in the **Local log server worker threads** property. Keep the default value of 10. The range is between 1 and 20. However, if you have a high number of log messages, you can allocate more threads to improve performance.

4. In the **Explorer** window, under **Environment**, right-click **Logging**, and click **New resource** > **Destination**.
5. In the **Name** box, type the name of the repository.
6. In the **Type** list, click **Database** and then click **OK**.
7. In the **Explorer** window, under **Logging**, right-click the database name, and click **New resource** > **Database**.
8. In the **Name** box, type the name of the repository.
9. In the **Type** list, click **DB2 database** and then click **OK**.
10. In the **Properties** window, type the **Database server and port number**, **User ID and password**, and the z/OS **Database name**.

    Ensure that the User ID is the same as the value you specified for the IPFSCRIPT_USERNAME parameter in the LS_tablespace_db2zOS.sql script file "Create tablespaces for a logging database on Db2 on z/OS " on page 136.
11. In the **Explorer** window, click **Local Configuration**.
12. In the **Properties** window, next to **Advanced properties**, click inside the **Value** box, and then click the edit icon ✎.
13. Click **Add**, and then add the configuration parameter names and values from the following table:

    Table 25: Configuration parameter names and values

Parameter Name	Value
IPFSCRIPT_CREATE_IN	The base tables location. For example, databaseName.baseTablespaceName
IPFSCRIPT_STOGROUP	The name of the storage group.
IPFSCRIPT_DATABASE	The name of logging database.
IPFSCRIPT_LS_ID	The instance identifier for the audit database. This value must not be longer than two characters.

14. From the **File** menu, click **Save**.
15. Test the connection to the new database. In the **Explorer** window, under **Environment**, right-click **Logging** and click **Test**.

    IBM Cognos components connect to the database. If you configured more than one database for logging messages, IBM Cognos components test all the databases.

Specify the Log Messages Repository for Informix

You can configure a type of repository for the log messages, and then configure properties for the specific repository. You can also configure more than one repository for log messages.

Procedure

1. In the **Explorer** window, under **Environment**, click **Logging**.
2. In the **Properties** window, use the following table to help set the log server properties.

Table 26: Log server properties

Task	Action
Use TCP between IBM Cognos components on a computer and its local log server	Set the **Enable TCP** property to **True**. UDP provides faster communication with a lower risk of lost connections than TCP. TCP is used for communication between a local log server and a remote log server.
Change the number of threads available to the local log server	Type the value in the **Local log server worker threads** property. Keep the default value of 10. The range is between 1 and 20. However, if you have a high number of log messages, you can allocate more threads to improve performance.

3. In the **Explorer** window, under **Environment**, right-click **Logging**, and click **New resource** > **Destination**.
4. In the **Name** box, type the name of the repository.
5. In the **Type** list, click **Database** and then click **OK**.
6. In the **Explorer** window, under **Logging**, right-click the database name, and click **New resource** > **Database**.
7. In the **Name** box, type the name of the repository.
8. In the **Type** list, click **Informix Dynamic Server database** and then click **OK**.
9. In the **Properties** window, type the values for **Database server and port number**, **User ID and password**, and **Database name**.
10. If you have multiple instances of an Informix logging database, create the advanced property IPFSCRIPTIDX and specify the account under which the instance runs:
    - In the **Explorer** window, click **Local Configuration**.
    - In the **Properties** window, click the **Value** column for **Advanced properties** and then click the edit icon ✎.
    - In the **Value - Advanced properties** dialog box, click **Add**.
    - In the **Name** column, type **IPFSCRIPTIDX**
    - In the **Value** column, type the user ID of the account under which the instance of the logging database runs.

      Use a different user account for each instance of Informix logging database.
    - Repeat in every instance of IBM Cognos Configuration that uses an instance of an Informix logging database.
11. From the **File** menu, click **Save**.
12. Test the connection to the new database. In the **Explorer** window, under **Environment**, right-click **Logging** and click **Test**.

IBM Cognos components connect to the database. If you configured more than one database for logging messages, IBM Cognos components test all the databases.

Enabling User-specific Logging

When diagnosing problems, you can temporarily set logging to track one or more specific users instead of all users at once. After you complete the diagnosis, you can resume normal logging. To enable user-specific logging, you use IBM Cognos Configuration to configure connection information for Java Management Extensions (JMX) a technology that supplies tools to manage and monitor applications and service-oriented networks. Then you configure JMX connection information in a deployment properties file.

After enabling user-specific logging for IBM Cognos components, enable logging for a specific user by using the Remote Process service for JMX. For information, see the topic about using logging to diagnose a problem for a specific user in the *IBM Cognos Analytics Administration and Security Guide*.

You must install Oracle Java SE Development Kit or Java Software Development Kit for IBM before you can enable user-specific logging.

Configure JMX Connection Information using IBM Cognos Configuration

You configure Java Management Extensions (JMX) connection information in IBM Cognos Configuration by specifying a cookie value and then setting the JMX port and credentials.

Procedure

1. On the computer where Content Manager is installed, start IBM Cognos Configuration.
2. In the **Explorer** window, click **Environment**.
3. In the **Properties** window, configure the JMX properties under **Dispatcher Settings**:
   - For **External JMX port**, type an available port number.
   - For **External JMX credential**, click the edit icon ✎ in the **Value** column, type a user ID and password, and then click **OK**.

     The user ID and password ensure that only an authorized user can connect to the Java environment to specify the user or users to be logged, using the port specified in **External JMX port**.
4. Save the configuration.

Configure JMX Connection Information in a Deployment Properties File

To support the Java Management Extensions (JMX) settings on your application server, specify the JMX port in the p2pd deployment properties file.

Procedure

1. In a text editor, open the `p2pd.deploy_defaults.properties` file located at *`install_location`*`/webapps/p2pd/WEB-INF`.
2. Uncomment the `rmiregistryport` line and set the value to the **External JMX port** that you configured in IBM Cognos Configuration.
3. Save the `p2pd.deploy_defaults.properties` file.
4. Restart the services for IBM Cognos.

Results

IBM Cognos now supports logging for one or more specific users. For more information, see the topic about using logging to diagnose a problem for a specific user in the *IBM Cognos Analytics Administration and Security Guide*.

Changing Global Settings

By default, IBM Cognos components ensure that all locales, which may come from different sources and in various formats, use a normalized form. That means that all expanded locales conform to a language and regional code setting. Each computer has a default system locale and one user locale per user. The user locales may be different from the default system locale. If you change global settings on one Content Manager computer, you must make the same changes on the other Content Manager computers.

You change global settings

- to customize language support for the user interface
- to customize currency support
- to customize content locale support
- to map the language used in the product user interface
- to map content locales
- to add fonts to your IBM Cognos environment
- to customize the default time zone
- to change the encoding for email messages
- to customize cookie settings

Customize Language Support to the User Interface

Use the Product Locales table to add or remove the user interface language support. For example, if you do not require a German user interface, you can remove the language from the list.

If you change the user interface language of the product, data is not affected.

Before you begin

Ensure that you install the appropriate fonts to support the character sets and currency symbols you use. For Japanese and Korean currency symbols to appear correctly, you must install the additional fonts from the Supplementary Language Documentation disk.

Procedure

1. On each Content Manager computer, start IBM Cognos Configuration.
2. From the **Actions** menu, click **Edit Global Configuration**.
3. Click the **Product Locales** tab.

   All supported locales are displayed.
4. Click **Add**.

   Tip: To remove support, select the check box next to the **Supported Locale** and then click **Remove**.
5. In the second column, type the language portion of a locale.
6. Repeat steps 3 to 5 for other language support that you want to add.
7. Click **OK**.
8. From the **File** menu, click **Save**.

Customizing Currency Support

If you require additional currencies or want to remove some from the user interface, you can update the list of supported currencies in the Currencies table. If you use Japanese or Korean currencies, you must configure support so that Japanese Yan and Korean Won characters display correctly.

By default IBM Cognos components show only a subset of supported currencies in the user interface. Currencies are identified by their ISO 4217 currency code. The complete list of supported currencies that can be added are listed in the i18n_res.xml file in the *install_location*/bin directory.

Adding currencies to the IBM Cognos environment does not guarantee that your computer has a font with the required characters to display the currency. Ensure that you install the appropriate fonts to support the currency symbols you use. For example, to display the Indian currency symbol (rupee) correctly, you must install a font that contains that character. In addition, for Japanese and Korean currency symbols to appear correctly, you must install the additional fonts from the Supplementary Language Documentation disk.

Add Currencies to the User Interface
You can add supported or unsupported currencies to the user interface. You add supported currencies in IBM Cognos Configuration. You add unsupported currencies to the i18n_res.xml file that is provided in IBM Cognos.

If you add a currency code that is not supported by IBM Cognos, you must manually add it to the i18n_res.xml file in the *install_location*/bin directory. Copy this file to each IBM Cognos computer in your installation.

Procedure

1. On each Content Manager computer, start IBM Cognos Configuration.
2. From the **Actions** menu, click **Edit Global Configuration**.
3. Click the **Currencies** tab.
4. Click **Add**.

   Tip: To remove support, select the check box next to the supported item and then click **Remove**.
5. In the second column, type an appropriate value.

   The value you add must comply with ISO 4217 codes for the representation of currencies and formats. Usually the value you add is a three-letter alphabetic code. The first two characters are letters representing the ISO 3166 country or region code for the country or region the currency is from. The additional letter represents the first letter of the currency.
6. Repeat steps 3 to 5 for other types of support that you want to add.
7. From the **File** menu, click **Save**.

Customize content locale support

To ensure users see reports, data or metadata in their preferred language, or specific to their region, you can add partial locales (language) or complete locales (language-region) to the Content Locales table. This way, if content is available in different languages, or in different locales, it is rendered to users based on their user locale. By default, content locale overrides product locale in the portal for some content.

If you view reports in Thai language, digits are not supported.

Before you begin

If a locale is not required, you can remove it from the list. You must leave at least one content locale in the list for the Application Tier Components to operate.

Adding incomplete locales (languages) to the IBM Cognos environment does not guarantee that your computer has a font that can display Web pages in your preferred languages. Ensure that you install the appropriate fonts to support the character sets and currency symbols you use. For Japanese and Korean currency symbols to appear correctly, you must install the additional fonts from the Supplementary Language Documentation disk.

Procedure

1. On each Content Manager computer, start IBM Cognos Configuration.
2. From the **Actions** menu, click **Edit Global Configuration**.
3. Click the **Content Locales** tab.

   All supported locales are displayed.

4. Click **Add**.

   Tip: To remove support, select the check box next to the supported item and then click **Remove**.
5. In the second column, type an appropriate value.
   - To add language support for report data and metadata, type a partial local (language) setting.
   - To add support specific to a region, type a complete locale (language-region) setting.
6. Repeat steps 3 to 5 for each additional locale that you want to support.
7. From the **File** menu, click **Save**.

Content Locales

Use the Content Locale Mappings table to map user locales to a complete (language-region) or partial (language) locale. You can also map a user's preferred language to another language if content is not available in the user's preferred language.

For example, if a report or scorecard is not available in a preferred language, for example Vietnamese, but is available in French and German, you can use the Content Mappings table to map the preferred language (Vietnamese) to another language (French or German). This way, you see the report or scorecard in the mapped language.

By default, the Content Locale Mappings table includes locales that do not contain the region. This allows you to use only the language portion of the locale when you specify locale settings and ensures that you always see the correct information. For example, in a multilingual database, data is usually available in different languages, such as French (fr), Spanish (es) and English (en), rather than being available in different locales, such as English Canada (en-ca), English United States (en-us), or French France (fr-fr).

The following examples show the method that IBM Cognos components use to determine which report or scorecard the user sees if the multiple language versions are available.

Example 1

A report is available in Content Manager in two locales, such as en-us (English-United States) and fr-fr (French-France), but the user locale is set to fr-ca (French-Canadian). IBM Cognos uses the locale mapping to determine which report the user sees.

First, IBM Cognos checks to see if the report is available in Content Manager in the user's locale. If it is not available in the user's locale, IBM Cognos maps the user's locale to a normalized locale configured on the Content Locale Mapping tab. Because the user's locale is fr-ca, it is mapped to fr. IBM Cognos uses the mapped value to see if the report is available in fr. In this case, the report is available in en-us and fr-fr, not fr.

Next, IBM Cognos maps each of the available reports to a normalized locale. Therefore, en-us becomes en and fr-fr becomes fr.

Because both report and the user locale maps to fr, the user having the user locale fr-ca will see the report saved with the locale fr-fr.

Example 2

The user's locale and the report locales all map to the same language. IBM Cognos chooses which locale to use. For example, if a user's locale is en-ca (English-Canada) and the reports are available in en-us (English-United States) and en-gb (English-United Kingdom), IBM Cognos maps each locale to en. The user will see the report in the locale setting that IBM Cognos chooses.

Example 3

The report and the user locales do not map to a common language. IBM Cognos chooses the language. In this case, you may want to configure a mapping. For example, if a report is available in en-us (English-United States) and fr-fr (French-France), but the user locale is es-es (Spanish-Spain), IBM Cognos chooses the language.

Map Content Locales
Use the Content Locale Mappings table to map user locales to a complete (language-region) or partial (language) locale. You can also map a user's preferred language to another language if content is not available in the user's preferred language.

Procedure

1. On each Content Manager computer, start IBM Cognos Configuration.
2. From the **Actions** menu, click **Edit Global Configuration**.
3. Click the **Content Locale Mapping** tab.
4. Click **Add**.
5. In the **Key** box, type the user locale:

   - To ensure all regions for a user locale see content in a specific language, type the language portion of the locale, followed by a dash (-) and an asterisk (*).

     For example, type **fr-***
   - To ensure a user locale (language-region) sees content in a specific language, type the complete locale.

     For example, type **fr-ch**
   - To map a preferred language to another language, type the preferred language portion of the locale.

     For example, type **zh**

   Tip: To specify the locale to use for a range of keys, use the wildcard character (*) with the **Key** value and then, in the **Locale Mapping** box, type the locale. For example, if you want all the German keys to use the German locale, type **de*** in the **Key** box and type in the **Locale Mapping** box.
6. In the **Locale Mapping** box, type the language portion of the locale.

   User locales specified in the **Key** box will see content in this language.
7. Repeat steps 3 to 5 for other mappings you want to do.
8. Click **OK**.
9. From the **File** menu, click **Save**.

Map Product Locales

Use the Product Locale Mappings table to specify the language used in the user interface when the language specified in the user's locale is not available.

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

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

Procedure

1. On each Content Manager computer, start IBM Cognos Configuration.
2. From the **Actions** menu, click **Edit Global Configuration**.
3. Click the **Product Locale Mappings** tab.
4. Click **Add**.
5. In the **Key** box, type the user locale:

- To ensure all regions for a locale see the user interface in a specific language, type the language portion of the locale, followed by a dash (-) and an asterisk (*).

  For example, type **es-***
- To ensure a complete locale (language-region) see the user interface in a specific language, type the complete locale.

  For example, type **es-es**
- To map a preferred language to another language, type the preferred language portion of the locale.

  For example, type **zh**

Tip: To specify which locale to use as the default, use the wildcard character (*) for the **Key** value and then, in the **Locale Mapping** box type the locale.

6. In the **Locale Mapping** box, type the language portion of the locale.

   User locales specified in the **Key** box will see content in this language.
7. Repeat steps 3 to 5 for other mappings you want to do.
8. Click **OK**.
9. From the **File** menu, click **Save**.

Customize the Server Time Zone

You can customize the time zone used by Content Manager by selecting a different server time zone in IBM Cognos Configuration.

For UNIX installations that do not support a Java-based graphical user interface, you can view the list of acceptable time zones by opening IBM Cognos Configuration on the Windows computer where Framework Manager is installed.

Content Manager is configured to use the time zone of your operating system by default. All scheduled activities in IBM Cognos are set using this time zone. In addition, users in the portal use this time zone if they set their preferences for the default time zone. For more information about setting user preferences in the portal, see the *IBM Cognos Analytics Administration and Security Guide*.

Procedure

1. Start IBM Cognos Configuration.
2. From the **Actions** menu, click **Edit Global Configuration**.
3. In the **Global Configuration** window, click the **General** tab.
4. Click the **Value** column for **Server time zone** and select another time zone from the list.
5. From the **File** menu, click **Save**.

Encoding for Email Messages

By default, IBM Cognos components use UTF-8 encoding in emails. This value sets the default encoding used by the delivery service in this instance for all email messages. You may have older email clients or send email from IBM Cognos to cell phones and PDAs that do not recognize UTF-8. If so, you can change the email encoding to a value that works on all your email clients (for example, ISO-8859-1, Shift-JIS). Each instance of IBM Cognos that has an available delivery service must be changed.

The specified encoding affects the entire message, including the subject, attachments, attachment names, and plain or HTML body text.

The encoding values are shown in the following table:

Table 27: Supported encoding values

Character set	Supported encoding value
UTF-8	utf-8

Table 27: Supported encoding values (continued)

Character set	Supported encoding value
Western European (ISO 8859-1)	iso-8859-1
Western European (ISO 8859-15)	iso-8859-15
Western European (Windows-1252)	windows-1252
Central and Eastern European(ISO 8859-2)	iso-8859-2
Central and Eastern European (Windows-1250)	windows-1250
Cyrillic (ISO 8859-5)	iso-8859-5
Cyrillic (Windows-1251)	windows-1251
Turkish (ISO 8859-9)	iso-8859-9
Turkish (Windows-1254)	windows-1254
Greek (ISO 8859-7)	iso-8859-7
Greek (Windows-1253)	windows-1253
Japanese (EUC-JP)	euc-jp
Japanese (ISO-2022-JP)	iso-2202-jp
Japanese (Shift-JIS)	shift_jis
Traditional Chinese (Big5)	big5
Simplified Chinese (GB-2312)	gb2312
Korean (EUC-KR)	euc-kr
Korean (ISO 2022-KR)	ISO 2022-KR
Korean (KSC-5601)	ksc_5601
Thai (Windows-874)	windows-874
Thai (TIS-620)	tis-620

Change Encoding for Email Messages

You can change the email encoding to a value that works on all your email clients.

Procedure

1. Start IBM Cognos Configuration.
2. From the **Actions** menu, click **Edit Global Configuration**.
3. In the **Global Configuration** window, click the **General** tab.
4. Click the **Value** column for the **Email Encoding** property.

5. Scroll to the desired setting and click it.
6. From the **File** menu, click **Save**.

Customizing cookie settings

Based on the requirements of your IBM Cognos environment, you may need to modify the settings that IBM Cognos components use to create cookies. You can use IBM Cognos Configuration to customize the cookie domain, path, and secure flag.

IBM Cognos components determine the cookie domain from the HTTP request submitted by the client, which is typically a Web browser. In most network configurations, HTTP requests pass through intermediaries such as proxy servers and firewalls as they travel from the browser to IBM Cognos components. Some intermediaries modify the information that IBM Cognos components use to calculate the cookie domain, and IBM Cognos components then cannot set cookies. The usual symptom of this problem is that users are repeatedly prompted to log on. To avoid this problem, configure the cookie domain.

To set the correct value for the cookie domain, use the format and value that represents the widest coverage for the host as suggested in the following:

- For the Domain value, use the computer or server name alone. Specify this name without any dots. For example, `mycompany`
- The Domain value can also specify a suffix. Suffixes include .com, .edu, .gov, .int, .mil, .net, or .org. Include a prefix dot. For example, `.mycompany.com`
- Other levels can be used in a Domain value. Include a prefix dot. For example `.accounts.mycompany.com`
- A Path value can further restrict cookies. The most general path is `/`. A path of `/payables` restricts the cookie to all paths beginning with "payable" (and all subdirectories). A path of `/payables/` restricts the cookie to the "payables" directory (and all subdirectories).

Additionally, for security, administrators can set the HTTPOnly attribute to block scripts from reading or manipulating the CAM passport cookie during a user's session with their web browser. For more information about this attribute, see the *IBM Cognos Analytics Administration and Security Guide*.

Procedure

1. On each Content Manager computer, start IBM Cognos Configuration.
2. From the **Actions** menu, click **Edit Global Configuration**.
3. Click the **General** tab.
4. Click in the **Value** column under **Cookie Settings** for each property that you want to change and specify the new value.

   If you leave the **Domain** property blank, the dispatcher derives the domain from the host name of the request.
5. Click **OK**.

Change the IP Address Version

IBM Cognos products support two IP address versions: IPv4 and IPv6. IPv4 uses 32-bit IP addresses and IPv6 uses 128-bit IP addresses.

For example:

- IPv4: 192.168.0.1:80
- IPv6: [2001:0db8:0000:0000:0000:148:57ab]:80

In IBM Cognos Configuration, you can select IPv4 or IPv6 for IBM Cognos communication using the **IP Version for Host Name Resolution** property. By default IPv4 is employed.

The setting applies only to the computer where it is set. If you select **Use IPv4 addresses**, all outgoing IBM Cognos connections on that computer are established using IPv4 and the dispatcher accepts only incoming IPv4 connections. If you select **Use IPv6 addresses**, all outgoing IBM Cognos connections on that computer are established using IPv6 and the dispatcher accepts both incoming IPv4 and IPv6 connections.

IPv4 client computers can communicate with dispatcher computers that are configured for IPv6.

Hostnames specified within a URI are resolved based on the value of the **IP Version for Host Name Resolution** property. However, if a URI has been specified with a numeric address, it has precedence over this setting and communication takes place using IPv4.

For IBM Cognos Configuration to accept IPv6 addresses in the local URI properties, you must start IBM Cognos Configuration with the -ipv6 option. You can specify the option each time you open IBM Cognos Configuration from the command line.

On Windows, you can set the option permanently by adding the option to the Start menu shortcut.

Setting the IP version

Use IBM Cognos Configuration to select the IP version.

Procedure

1. Start IBM Cognos Configuration.
2. In the **Explorer** window, click **Environment**.
3. Click the **Value** box for **IP Version for Host Name Resolution** and click **Use IPv4 addresses** or **Use IPv6 addresses**.
4. From the **File** menu, click **Save**.
5. Close IBM Cognos Configuration.

Manually configuring IBM Cognos Configuration to start with the IPv6 option

You can manually configure IBM Cognos Configuration to use the IPv6 option by specifying the option in the start command.

Procedure

1. Go to the *install_location*/bin or the *install_location*/bin64 directory.
2. Start IBM Cognos Configuration by including the IPv6 option in the command, as follows:
   - On Windows, type

     ```
     cogconfig.bat -ipv6
     ```
   - On UNIX or Linux, type

     ```
     ./cogconfig.sh -ipv6
     ```
3. Edit the URI properties that use IPv6 format, specify the values, and then from the **File** menu, click **Save**.

Configuring IBM Cognos Configuration to always start with the IPv6 option on Windows

You can configure IBM Cognos Configuration to always use the IPv6 option on Microsoft Windows operating systems by setting the option in the Start menu shortcut.

Procedure

1. From the **Start** menu, right-click **IBM Cognos Configuration**, and select **Properties**.
2. On the **Shortcut** tab, in the **Target** box, type

   ```
   "install_location\bin\cogconfigw.exe -ipv6"
   ```
3. Click **OK**.

Configuring the Collaboration Discovery URI

You can configure IBM Cognos Analytics and IBM Cognos Workspace to use IBM Connections for collaborative decision-making. Integration with IBM Connections allows business users to collaborate while creating or viewing reports, performing analysis, or monitoring workspaces. Users have access to IBM Connections activities from within IBM Cognos Workspace and to the IBM Connections homepage from within IBM Cognos Analytics and IBM Cognos Workspace.

The Collaboration discovery URI specifies the IBM Connections server to use as the collaboration provider. When a URI is specified, collaboration-related support is added to IBM Cognos Analytics as follows:

- a link is added to the IBM Cognos Analytics portal welcome page. If the user has access to the IBM Connections homepage, the link is named **Access my social network** and links the user to the homepage. If the user has access to IBM Connection activities, but not the homepage, the link is named **My Activities** and links the user to the activities page.
- a link to the IBM Connections homepage is added to the Launch menu in the portal
- a link to the IBM Connections homepage is added to the Actions menu in IBM Cognos Workspace
- the **Collaborate** menu button is added on the workspace application bar in IBM Cognos Workspace. This allows the user to create or view a workspace activity in IBM Connections.

Procedure

1. In **IBM Cognos Administration**, on the **Configuration** tab, click **Dispatchers and Services** to view the list of dispatchers.
2. From the toolbar, click the set properties - configuration button.
3. Click the **Settings** tab.
4. For the **Environment** category, **Collaboration discovery URI**, specify the URI as follows:

   `http://`*`server_name`*`:`*`port_number`*`/activities/serviceconfigs`

   For example, `http://`*`server_name`*`:9080/activities/serviceconfigs`

   where *`server_name`* represents the server name where IBM Connections is installed.
5. Click **OK**.

Configuring IBM Cognos Workspace

IBM Cognos Workspace is included with IBM Cognos Analytics server. It delivers dynamic and customizable features that allow you to quickly and easily assemble interactive workspaces using IBM Cognos content, as well as external data sources. After you test that IBM Cognos Workspace is running, configure access to the secured functions and features.

Complete the following configuration tasks.

__ • Configure access to IBM Cognos Workspace.

__ • Configure Supported MIME Types in Microsoft Internet Information Services.

After the configuration tasks are completed, you can perform the following tasks as required:

__ • Set up a database for annotations.

__ • Configure IBM Cognos Workspace to use content from a TM1 Data Server.

__ • Configure IBM Cognos Workspace to access IBM Cognos TM1 Applications.

__ • Change styles in your reports.

__ • Use the samples.

Configuring access to IBM Cognos Workspace or its functions

Configure access to IBM Cognos Workspace by granting required permissions for the Executive Dashboard capability to specified namespaces, users, groups, or roles.

You can grant full access to IBM Cognos Workspace or you can grant access only to the publishing function.

IBM Cognos Analytics must be configured and operating before you can configure access for IBM Cognos Workspace.

Granting full access to IBM Cognos Workspace

To grant access to IBM Cognos Workspace and all its functionality, grant execute and traverse permissions for the Executive Dashboard capability.

Additional information about configuring permission for users can be found in a technote (www.ibm.com/support/docview.wss?uid=swg21498402) on the IBM Web site.

Procedure

1. From the IBM Cognos Analytics portal, launch **IBM Cognos Administration**.
2. On the **Security** tab, click **Capabilities**.
3. Find the **Executive Dashboard** capability, click the actions button ▼ next to the capability name, and then select **Set properties**.
4. Select the **Permissions** tab.
5. Grant Execute permission to all user groups that should have access to IBM Cognos Workspace, and then click **OK**.

Granting access to the publishing function for IBM Cognos Workspace

To grant access only to the publishing function within IBM Cognos Workspace, grant traverse permissions for the Executive Dashboard capability and execute permissions for the Publish Dashboards to Collaboration Spaces secured function.

Procedure

1. From the IBM Cognos Analytics portal, launch **IBM Cognos Administration**.
2. On the **Security** tab, click **Capabilities**.
3. Find and select the **Executive Dashboard** capability.
4. Click the actions button ▼ next to **Publish Dashboards to Collaboration Spaces**, and click **Set properties**.
5. Select the **Permissions** tab.
6. To set access permissions explicitly for each entry, select the **Override the access permissions acquired from the parent entry**.
7. For each user group, select the check box for the entry, and in the box next to the list, select the check boxes to grant permissions for the entry.
8. To add new entries to the list, click **Add** and choose how to select entries:

    - To choose from available entries, click the appropriate namespace, and then select the check boxes next to the users, groups, or roles.
    - To search for entries, click **Search** and in the Search string box, type the phrase you want to search for. For search options, click **Edit**. Find and click the entry that you want.
    - To type the name of entries that you want to add, click **Type** and type the names of groups, roles, or users using the following format, where a semicolon (;) separates each entry: `namespace/group_name;namespace/role_name;namespace/user_name;`

    You can then grant the appropriate permissions for each new entry.

9. Click **OK**.

Configuring Supported MIME Types in Microsoft Internet Information Services

If you use Microsoft Internet Information Services (IIS) 6.0, then for IBM Cognos Workspace to load successfully, you must define the MIME type that IBM Cognos Workspace uses.

Procedure

1. Open the Microsoft IIS management console.
2. Right-click the local computer name, and click **Properties**.
3. Click **MIME Types**.
4. Click **New**.
5. In the **Extension** box, type **.cfg**.
6. In the **MIME Type** box, type **text/plain**.
7. Apply the new settings.

   The changes will take effect when the worker process recycles. To avoid waiting, you can restart the World Wide Web Publishing Service. For more information, search the Microsoft online library for *Handling MIME Types in Internet Explorer*.

Creating tablespaces for the human task and annotation database on IBM Db2 on z/OS

If you are using Db2 on z/OS, a database administrator must run scripts to create the tablespaces required for the human task and annotation database. The script must be modified to replace the placeholder parameters with ones that are appropriate for your environment.

Ensure that you use the name convention for Db2 on z/OS. For example, all names of parameters must start with a letter and the length must not exceed six characters. For more information, see the Db2 Knowledge Center.

You can use your content store database or a separate database for the human task and annotation database. In either case, you must run the scripts to create the tablespaces.

Procedure

1. Connect to the database as a user with privileges to create and drop tablespaces and to allow execution of SQL statements.
2. To create the human tasks tablespaces, go to the *`install_location`*`/configuration/schemas/hts/zosdb2` directory.
   a) Make a backup copy of the `HTS_tablespaces.sql` script file and save the file to another location.
   b) Open the original `HTS_TABLESPACES.sql` script file and use the following table to help you to replace the generic parameters with ones appropriate for your environment.

      Table 28: Tablespace parameter names and descriptions for human tasks on Db2 for z/OS

Parameter Name	Description
NCCOG	Specifies the name of the database.
DSN8G810	Specifies the name of the storage group.
BP32K	Specifies name of the 32 k buffer pool.

      See the script for a complete list of the parameters required.
   c) Save and run the script.

d) Open the `HTS2_CREATE_Db2zos.sql` script file and use the following table to help you to replace the generic parameters with ones appropriate for your environment.

Table 29: Tablespace parameter names and descriptions for human tasks on Db2 for z/OS

Parameter Name	**Description**
NCCOG	The name of the database.

See the script for a complete list of the parameters required.

e) Save and run the script.

3. To create the annotations tablespaces, go to the *`install_location`*`/configuration/schemas/ans/zosdb2` directory.

   a) Make a backup copy of the `ANN_TABLESPACES.sql` script file and save the file to another location.

   b) Open the original `ANN_TABLESPACES.sql` script file and use the following table to help you to replace the generic parameters with ones appropriate for your environment.

Table 30: Tablespace parameter names and descriptions for annotations on Db2 for z/OS

Parameter Name	**Description**
NCCOG	The name of the database.
DSN8G810	The name of the storage group.
BP32K	The name of the 32 k buffer pool.

See the script for a complete list of the parameters required.

   c) Save and run the script.

   d) Open the `ANS2_CREATE_Db2zos.sql` script file and use the following table to help you to replace the generic parameters with ones appropriate for your environment.

Table 31: Tablespace parameter names and descriptions for annotations on Db2 for z/OS

Parameter Name	**Description**
NCCOG	The name of the database.

See the script for a complete list of the parameters required.

   e) Save and run the script.

Setting up a database for Human Tasks and Annotations

By default, the data used for the Human Tasks and Annotations feature in IBM Cognos Workspace is stored in the same database as the content store. You can configure a separate database for Human Tasks and Annotations.

To set up the database, you must first create the database, create a user account under which the database will operate, and then configure the Human Tasks and Annotations feature to use the new database.

Procedure

1. Create a database using the same instructions as Guidelines for creating the content store.

If you are using IBM Db2 on z/OS for your database, you must create the required tablespaces by running two scripts. For more information, see "Creating tablespaces for the human task and annotation database on IBM Db2 on z/OS" on page 155.

2. Create a user account that will be used to operate the database.
3. For the instance where the Application Tier Components are installed, start IBM Cognos Configuration.
4. In the **Explorer**, right-click **Human Task and Annotation Services** and select **New resource** > **Database**.
5. In the **New Resource - Database** dialog box, type a name for the database, select the type, and then click **OK**.
6. In the database resource properties window, configure the following:
   - Specify the mandatory values for all properties that are marked with an asterisk.
   - Specify the **User ID and password** for the account that operates the database.
7. From the **File** menu, click **Save**.

   The logon credentials are immediately encrypted.
8. To test the connection to the new database, from the **Actions** menu, click **Test**.
9. Repeat these steps on each Application Tier Components and Content Manager instance.

Configuring IBM Cognos Workspace to use IBM Cognos TM1 data

To be able to use IBM Cognos TM1 data in IBM Cognos Workspace, you must modify configuration files in your IBM Cognos Analytics installation.

To configure the TM1 data server for IBM Cognos Workspace, you must perform the following tasks:

__ • Set connection information for your TM1 Server.

__ • Set the names of your IBM Cognos TM1 server as they would appear in IBM Cognos Workspace.

__ • Optionally, change the name for the Views folder.

Set connection information for your TM1 Server

You must modify a configuration file to set the connection information for your TM1 Servers.

A sample contribution file is provided with in your IBM Cognos Analytics installation. If you are using a distributed installation, the configuration file is available on the computers where you installed the Application Tier Components.

If the IBM Cognos Analytics gateway is running on a different computer than TM1 Web, ensure that you use the fully qualified domain names for server name values, such as the `TM1WebHost`. For example, use `http://`*`mycomputer.mydomain`*`.com/ibmcognos` rather than `http://`*`mycomputer`*`/ibmcognos`. Also, you must use the fully qualified domain names for the server name values in the **Environment** section of IBM Cognos Configuration.

Procedure

1. On the computer where you installed the IBM Cognos Analytics Application Tier Components, go to the *`install_location`*`\configuration\icd\contributions\contrib` directory, and rename the `tm1_contribution.atom.sample` file as `tm1_contribution.atom`.
2. Open the `tm1_contribution.atom` file in a text editor.

   The file contains three `<atom:entry>` sections. You must change the values in one `<atom:entry>` section for each TM1 server you want to access in IBM Cognos Workspace. If you have more TM1 servers you want to add, you must add `<atom:entry>` sections as required. You must also comment out any extra `<atom:entry>` sections. The third `<atom:entry>` section in the sample file is already commented out.

   The first `<atom:entry>` section is for a TM1 server that does not use Cognos authentication.

   The second `<atom:entry>` section is for a TM1 server that uses Cognos authentication.

3. In the appropriate `<atom:entry>` section for the authentication required, replace TM1WebHostName and TM1HostName values with the name or IP address of the TM1 Web server and TM1 data server.

   For example, change the highlighted sections of the sample.

   ```
   TM1WebHost=TM1WebHostName&amp;
   TM1WebVirtualDirectory=tm1web&amp;
   TM1Host=TM1HostName&amp;
   ```

4. For a TM1 server that does not use IBM Cognos authentication, change the highlighted sections shown for the `TM1DataServer` value:

   ```
   TM1DataServer=TM1ServerHostWithoutCAM&amp;
   TM1username=admin&amp;TM1pass=apple
   ```

   Replace admin and apple with the user ID and password of the administrator account that is used for the TM1 server.

5. For a TM1 server that uses IBM Cognos authentication, change the highlighted sections shown for the `TM1DataServer` value:

   ```
   TM1DataServer=CamAuthenticatedTM1ServerHost
   ```

6. If you are not using the default values, change the following properties:

   - `https`

     This property describes the protocol used for the TM1 Web server. If the TM1 Web is running with HTTP secure, replace 0 with 1.

   - `TM1WebVirtualDirectory`

     This property is the name of the virtual directory for the TM1 Web. If the TM1 Web directory name is not `tm1web`, replace the value of the `TM1WebVirtualDirectory` property with the correct name.

     For example,

     ```
     TM1WebVirtualDirectory=planningweb&amp;
     ```

   - `TM1Toolbar`

     This property determines whether the internal toolbar is visible. Versions of TM1Web older than version 9.5.2 do not allow for an external toolbar. The default value of `TM1Toolbar` is 0. To display the internal toolbar, set the value to 1.

7. If you are defining multiple TM1 server connections, create a `<atom:entry>` section for each TM1 server.

   All `atom:id` values in all `.atom` entries must be unique. For example,

   ```
   <atom:entry>
           <atom:id>tag:ibm.cognos.icd.com,2010-01-01:/tm1_rootfeed_2
   </atom:id>
   ```

   ```
   <atom:entry>
           <atom:id>tag:ibm.cognos.icd.com,2010-01-01:/tm1_rootfeed_2b
   </atom:id>
   ```

   The samples are unique because of `tm1_rootfeed_2` and `tm1_rootfeed_2b`.

   Ensure that you use unique names for values such as tm1_rootfeed_1, rootfeed_title_1, and rootfeed_summary_1.

8. Ensure that you comment out or delete any unused `<atom:entry>` sections.
9. Save and close the file.

10. Restart the IBM Cognos services. If you want to change the names of the TM1 servers as they would appear in IBM Cognos Workspace, you can restart the services after the next task.

Set the names of your IBM Cognos TM1 server

You can define the names of your TM1 servers as they would appear in IBM Cognos Workspace.

If you use languages other than English, you can create additional language files to display the names in IBM Cognos Workspace.

Procedure

1. On the computer where you installed the IBM Cognos Analytics Application Tier Components, go to the *install_location*\configuration\icd\contributions\contrib directory.
2. Open the file named tm1_en.properties in a text editor.
3. Change the text that appears after the equal (=) sign to provide a meaningful name for the TM1 server defined for the title.

   For example, if you defined a TM1 server connection using the rootfeed_title_1 section in the tm1_contribution.atom file in the previous task, change the name to appear as:

   ```
   rootfeed_title_1 = MyTM1Server
   ```
4. Change the description in the rootfeed_summary_1 property to give a meaningful description for the TM1 server.

   For example, if you defined a name for your TM1 server connection using rootfeed_title_1, change the rootfeed_summary_1 value such as:

   ```
   rootfeed_summary_1 = Detail about MyTM1Server
   ```
5. Add new values for each TM1 server you added in the tm1_contribution.atom file in the previous task. Ensure that you match the rootfeed_title and rootfeed_summary sections with the values you defined in the tm1_contribution.atom file.
6. If your environment supports multiple languages:
   - Make a copy of the tm1_en.properties file.
   - Rename the file as tm1_*language_code*.properties, where *language_code* is the two-character code for the language that you are using such as ja or es.

     A sample French properties file is provided: tm1_fr.properties.
7. Restart the IBM Cognos services for the changed to take effect.

Change the name for the Views folder

Optionally, you can change the name that is displayed in IBM Cognos Workspace for the **Views** folder.

By default, IBM Cognos Workspace displays an Applications folder and a Views folder for each TM1 server that is identified in the tm1_contribution.atom file. The name of the Applications folder is returned by the TM1 server. The name of the Views folder is determined by a messages file that is provided with IBM Cognos Workspace.

Procedure

1. Go to the *install_location*\templates\ps\messages directory.
2. Create a copy of the tm1buxmsgs_en.xml file and name it using the appropriate language code.

   A sample French translation file is provided: tm1buxmsgs_fr.xml.
3. Open the new translation file in an XML editor.
4. Replace the word Views in the following section with an appropriate value:

   ```
   <string id="TM1_VIEWS" type="String" usage="TM1 views">Views</string>
   ```

5. Save and close the new file.
6. Repeat the steps for each supported language.

Configuring IBM Cognos Workspace to access IBM Cognos TM1 Applications

IBM Cognos Analytics server can access the Web client for IBM Cognos TM1 Applications through an external iwidget that displays in the content pane of IBM Cognos Workspace. Before the iwidget can display, use the TM1 Applications documentation to perform the following tasks.

Procedure

1. Install IBM Cognos TM1 Applications.
2. Configure IBM Cognos TM1 Applications for interoperability with the IBM Cognos Analytics server.

   When copying the `icon_active_application.gif` file to the Cognos Analytics server portal images folder, also copy this file to the *`install_location`*`/webcontent/icd/feeds/images` folder.
3. Deploy your applications.

   IBM Cognos TM1 Applications generates a URL, which the IBM Cognos Analytics server detects.

Results

The TM1 Contributor URL displays under **Public Folders** in the content pane of IBM Cognos Workspace.

Changing the style of report objects in IBM Cognos Workspace

When you drag a report object onto a workspace, it appears in the silver and blue gradient style of your product. You can configure the report object appear in the original authored style by changing a global property in the IBM Cognos Viewer configuration file.

Report objects that are affected by the global setting include queries, analyses, reports, and report parts that were authored using IBM Cognos Version 1.x style, Version 8.x style, and financial (balance sheet) style. These objects pick up the global setting even if you saved them before changing the global setting. Workspace thumbnails are affected by the global setting only if you rerun the thumbnail.

Some report objects are not affected by the global setting and will always render in the authored style, such as PowerPlay reports and report object thumbnails.

Procedure

1. For each Content Manager and Application Tier Components instance, go to the *`install_location`*`/webapps/p2pd/WEB-INF/classes directory`.
2. Open the `viewerconfig.properties` file in a text editor.
3. To make report objects appear in the original authored style, change the value for useAuthoredReportStyles to `true`.
4. Save the file and then restart the services.

Accessing the IBM Cognos Workspace samples

IBM Cognos Workspace samples are included with the IBM Cognos Analytics samples.

Business users can access the samples for IBM Cognos Workspace by selecting the option to open existing workspaces and then selecting **Samples** > **Models** > **Cognos Workspace Samples**.

For more information about installing and setting up the samples, see *IBM Cognos Analytics Samples Guide*. For more information about using the samples, see the *IBM Cognos Workspace User Guide*.

Configure the Router to Test Dispatcher Availability

If you use a router to distribute requests to IBM Cognos dispatchers, and the router can test the availability of a server using a test URL, you can configure the router to test the availability of an IBM Cognos dispatcher.

Procedure

Configure the router to use a URL with the path `/p2pd/servlet/ping`.

If the dispatcher is not ready, the following response is returned:

```
503 Service Unavailable
```

If the dispatcher is ready, the following response is returned:

```
200 OK
```

Configuring IBM Cognos Analytics to Work with Other IBM Cognos Products

Some IBM Cognos products provide functionality that is not available in IBM Cognos Analytics.

You can continue to use these products in the same environment. Additional configuration tasks may be required to ensure that IBM Cognos Analytics can access objects that were created using other IBM Cognos products. Additional requirements for access depend on how you choose to run the two products.

Enable Scheduled Reports and Agents for IBM Cognos Planning Contributor Data Sources

To run scheduled reports and agents, which are based on IBM Cognos Planning Contributor data sources, you must specify a shared, secret password. This helps to ensure secure communication between IBM Cognos Analytics servers and Contributor Data Server.

Procedure

1. On the Application Tier Components computer, start IBM Cognos Configuration.
2. In the **Explorer** window, click **Data Access**, **IBM Cognos Planning**, **Contributor Data Server**.
3. In the **Properties** window, click the **Value** box next to the **Signature password** property and then click the edit button ✎ when it appears.
4. In the **Value - Signature Password** dialog box, type the password that will be digitally signed.

   The password is case-sensitive and must match the **Signature password** property that you configure in IBM Cognos Series 7, Configuration Manager, **Cognos Planning/Cognos BI - Contributor Data Server/General** properties.
5. From the **File** menu, click **Save**.

Results

A digital signature, based on the password, is created. The digital signature is encoded by IBM Cognos Analytics and decoded by Contributor Data Server.

Configuring the Software Development Kit

To use the IBM Cognos Software Development Kit, you must perform some configuration and set-up tasks.

To configure the Software Development Kit, follow this process:

- If you want to run the Framework Manager script player from outside the bin directory, configure the FM_INI_FILE_PATH environment variable as a system variable on a Microsoft Windows operating system. The environment variable must point to the *`Framework_Manager_location`* `\configuration\fm.ini` directory.
- To allow the browsing or import of system objects such as tables, views, synonyms, stored procedures, or functions from a relational database in Framework Manager, edit the entry for ImportDatabaseSystemObjects in your `fm.ini` file.

  By default, ImportDatabaseSystemObjects is set to FALSE. Users can see only the user tables in the import and expression editor dialog boxes. To allow browsing or import of system objects, set the preference to TRUE.
- Set up the samples for IBM Cognos Analytics and Framework Manager.

  For more information, see the Installation and Configuration Guide for your IBM Cognos product.
- Set up the IBM Cognos software to use the Software Development Kit code samples.

  For more information, see the *IBM Cognos Software Development Kit Developer Guide.*
- Set up the IBM Cognos software to use the Mashup Service samples.

  For more information, see the *IBM Cognos Mashup Service Developer Guide.*

Chapter 7. Configuring authentication providers

IBM Cognos components run with two levels of access: anonymous and authenticated. By default, anonymous access is enabled.

You can use both types of logon with your installation. If you choose to use authenticated logon only, you must disable anonymous access. For more information, see Disable anonymous access.

For authenticated logon, you must configure IBM Cognos Analytics components with an appropriate namespace for the type of authentication provider in your environment. You can configure multiple namespaces for authentication and then choose, at run time, which namespace you want to use. For more information, see the *Administration and Security Guide*.

If you upgraded from ReportNet and IBM Cognos detects a previously configured namespace that is no longer configured, the unconfigured namespace appears in the list of authentication providers in the Administration portal. You can configure the namespace if you still require the user account information. Otherwise, you can delete the namespace. Also, when upgrading from one version to another, you must use the same authentication namespace for both versions. Otherwise, the old secured content will not be available because the new version might not contain the same policies, users, roles, and groups.

IBM Cognos components support the following types of servers as authentication sources:

- Active Directory Server
- Custom Authentication Provider
- IBM Cognos Series 7 namespace
- LDAP
- OpenID connect
- CA SiteMinder
- RACF®
- SAP

If you use more than one Content Manager, you must configure identical authentication providers in each Content Manager location. This means that the type of authentication provider you select and the way you configure it must be identical in all locations for all platforms. The configuration must contain information that is accessible by all Content Managers.

When IBM Cognos is installed in a single Linux-based computer, or when Content Manager is installed on a Linux-based computer, IBM Cognos can be configured to use only LDAP V3-compliant directory servers and custom providers as authentication sources.

Some authentication providers require libraries external to the IBM Cognos environment to be available. If these libraries are not available on Linux, the authentication provider cannot be initialized.

If you want to configure one of the following as your authentication source, you must install Content Manager on an operating system it supports:

- IBM Cognos Series 7 namespace (Windows, Solaris, AIX)
- Active Directory Server (Windows only)
- SAP BW (All except Power PC, z/OS, z/Linux)

If you enable security, you must configure security settings immediately after you complete the installation and configuration process. For more information, see the *Administration and Security Guide*.

Important: Do not disable security after you enable it. Existing permission settings will refer to users, groups, or roles that no longer exist. While this does not affect how the permissions work, a user administering the permission settings may see "unknown" entries. Because these entries refer to users, groups, and roles which no longer exist, you can safely delete them. However, "unknown" entries can also show up if you are not authenticated into all namespaces. In this scenario, do not delete "unknown" entries.

After you configure an authentication provider for IBM Cognos components, you can enable single signon between your authentication provider environment and IBM Cognos components. This means that a user logs on once and can then switch to another application without being asked to log on again.

Users can select namespaces when they log in to the IBM Cognos Analytics portal. You can hide Custom Java namespaces and CA SiteMinder namespaces from users. For more information, see “Hide the Namespace from Users During Login” on page 181.

Disabling anonymous access

If you want to configure IBM Cognos Analytics for authenticated logon only, you need to disable anonymous access to the application.

By default, IBM Cognos components do not require user authentication. Users can log on anonymously.

Procedure

1. On each computer where Content Manager is installed, start IBM Cognos Configuration.
2. In the **Explorer** window, under **Security** > **Authentication**, click **Cognos**.

   The Cognos namespace stores information about IBM Cognos groups and roles, contacts, and distribution lists, and so on, and references to objects in other security namespaces.
3. In the **Properties** window, click the box next to the **Allow anonymous access** property and then select **False**.
4. From the **File** menu, click **Save**.

Results

Now, you must configure a namespace so that users are required to provide logon credentials when they access IBM Cognos Analytics.

Restricting user access to the Cognos namespace

You can configure access to IBM Cognos Analytics so that only users who are members of any group or role in the **Cognos** namespace can access the application.

Ensure that you are a member of the built-in **System administrator** role in the **Cognos** namespace before you enable this configuration.

Procedure

1. On each Content Manager computer, start IBM Cognos Configuration.
2. In the **Explorer** window, under **Security**, click **Authentication**.
3. In the **Properties** window, change the value of **Restrict access to members of the built-in namespace** to **True**.
4. From the **File** menu, click **Save**.

What to do next

You must now remove the **Everyone** group from certain Cognos built-in groups and roles, and ensure that authorized users belong to at least one Cognos group or role. These tasks are performed by administrators in the Cognos Analytics administration interfaces. For more information, see the *IBM Cognos Analytics Managing Guide* or the *IBM Cognos Analytics Administration and Security Guide*.

Configuring Lightweight Third-Party Authentication

You can configure IBM Cognos Analytics components to use IBM Lightweight Third-Party Authentication (LTPA). The practices described in this topic are based on Cognos Analytics 11.0.7 distributed environment with IBM Tivoli Directory Server LDAP or Microsoft Active Directory as authentication sources.

To implement LTPA, Cognos Analytics must be configured to use an authentication source configured in the WebSphere Liberty container that it runs in. You can configure single sign-on between Cognos Analytics and WebSphere Liberty using the identity mapping configuration in the Cognos namespace. For example, you can configure WebSphere Liberty to use an LDAP or Active Directory server for authentication, then configure Cognos Analytics to use the same LDAP or Active Directory, and set the identity mapping to use REMOTE_USER.

For Cognos Analytics, this means that a user must be authenticated to an identity assigned to the HTTP session prior to accessing Cognos Analytics within that very same session. Authentication is completed by presenting credentials to an external-to-Cognos security system. The security system might provide the identity and some sort of credential information suitable for achieving single sign-on to other systems, usually in the form of an SSO token. Typical candidates for such security systems are authentication proxies, such as IBM Tivoli WebSEAL, Oracle Oblix, Computer Associates SiteMinder or any other software or hardware solutions that can authenticate an HTTP session and persist that authentication in a token.

WebSphere Liberty has many different options for authenticating users. For more information, see the WebSphere Liberty documentation: https://www.ibm.com/support/knowledgecenter/en/SSD28V_8.5.5/com.ibm.websphere.wlp.nd.iseries.doc/ae/twlp_sec.html

Configuring LTPA using an LDAP namespace

The following procedure describes how to set up LTPA for Cognos Analytics when using IBM Tivoli Directory Server LDAP as the authentication source.

For details about configuring LDAP, see "Configuring IBM Cognos components to use LDAP" on page 181

Procedure

1. In every location where you installed Content Manager, open IBM Cognos Configuration.
2. In the **Explorer** window, under **Security,** right-click **Authentication**, and then click **New resource** > **Namespace**.
3. In the **Name** box, type a name for your authentication namespace.
4. In the **Type** list, select **LDAP – General default values**.
5. In the **Properties** window, for the **Namespace ID** property, specify a unique identifier for the namespace.
6. Specify the following properties:

   Host and port
   The fully qualified host and port of the LDAP server.

   Base distinguished name
   For example, `o=`*`organization_name`*`.com`

   User lookup
   For example, `uid=${userID},ou=people`

   Use External Identity
   `True`

   External identity mapping
   For example, `uid=${environment("REMOTE_USER")},ou=people`
7. If you want the LDAP authentication provider to bind to the directory server by using a specific **Bind user DN and password** when you perform searches, then specify these values.

   If no values are specified, the LDAP authentication provider binds as anonymous.

If external identity mapping is enabled, **Bind user DN and password** are used for all LDAP access. If external identity mapping is not enabled, **Bind user DN and password** are used only when a search filter is specified for the **User lookup** property. In that case, when the user DN is established, subsequent requests to the LDAP server are run under the authentication context of the user.

8. If you do not use external identity mapping, use bind credentials for searching the LDAP directory server using the following steps:

   - Ensure that **Use external identity** is set to **False**.
   - Set **Use bind credentials for search** to **True**.
   - Specify the user ID and password for **Bind user DN and password**.

   If you do not specify a user ID and password, and anonymous access is enabled, the search is done by using anonymous.
9. Check the mapping settings for the required objects and attributes.

   Depending on the LDAP configuration, you may have to change some default values to ensure successful communication between IBM Cognos components and the LDAP server.

   LDAP attributes that are mapped to the **Name** property in **Folder mappings**, **Group mappings**, and **Account mappings** must be accessible to all authenticated users. In addition, the **Name** property must not be blank.
10. From the **File** menu, click **Save**.
11. Create an XML file named `local-server.xml` and place it in the *`install_location`*`/configuration` directory.
12. In the `local-server.xml` file, enter values that are appropriate for your environment:

```
<?xml version="1.0" encoding="UTF-8"?>
<server>
    <featureManager>
        <feature>ldapRegistry-3.0</feature>
        <feature>appSecurity-2.0</feature>
    </featureManager>
    <ldapRegistry id="id" realm="realm"
        host="host" port="port" ignoreCase="true"
        baseDN="o=basedn" ldapType="Custom" sslEnabled="false">
        <idsFilters
            userFilter="(uid=%v,ou=people)"
            userIdMap="*:uid"
            groupFilter='(objectclass=groupofnames)'
            groupIdMap="*:cn" />
    </ldapRegistry>
      <webAppSecurity allowFailOverToBasicAuth="true" displayAuthenticationRealm="true"/>
</server>
```

13. If Cognos Analytics is configured to use SSL, see "Configuring the SSL protocol for IBM Cognos components" on page 122 for more information.
14. To verify the configuration, log on to `http://`*`host`*`:`*`port`*`/bi` or `https://`*`host`*`:`*`port`*`/bi` for SSL enabled systems, where host is the fully qualified Cognos Analytics host domain.

    You should not see the Cognos Analytics logon page. Instead, you should be prompted by the browser to log on.

What to do next

If you want to configure single sign-on (SSO) between the Cognos Analytics application that was set up with LTPA authentication, and the application is deployed into a WebSphere instance, install the WebSphere key on each Cognos Analytics dispatcher where LTPA was set up, and update the `local-server.xml` file with the following `<ltpa>` element:

```
<ltpa keysFileName="yourLTPAKeysFileName.keys"
keysPassword="keysPassword" expiration="120" />
```

For more information, see the WebSphere Liberty documentation.

Configuring LTPA using an Active Directory namespace

The following procedure describes how to set up LTPA for Cognos Analytics with Microsoft Active Directory as the authentication source.

Procedure

1. In every location where you installed Content Manager, open IBM Cognos Configuration.
2. In the **Explorer** window, under **Security,** right-click **Authentication**, and then click **New resource** > **Namespace**.
3. In the **Name** box, type a name for your authentication namespace.
4. In the **Type** list, select **LDAP - Default values for Active Directory** and then click **OK**.

   The new authentication provider resource appears in the **Explorer** window, under the **Authentication** component. Default values are generated for you. Check them and make changes as needed.
5. In the **Properties** window, for the **NamespaceID** property, specify a unique identifier for the namespace.

   Tip: Do not use colons (:) in the Namespace ID property.
6. Specify the values for all other required properties to ensure that IBM Cognos components can locate and use your existing authentication provider.

   - For **User lookup**, enter `(sAMAccountName=${userID})`
   - If you use single sign-on, for **Use external identity**, set the value to **True**.
   - If you use single sign-on, for **External identity mapping**, enter `(sAMAccountName=${environment("REMOTE_USER")})`

     If you want to remove the domain name from the REMOTE_USER variable, enter `(sAMAccountName=${replace(${environment("REMOTE_USER")}, "domain\\","")})`.

     Important: Ensure that you use only the variable REMOTE_USER. Using another variable can cause a security vulnerability.
   - For **Bind user DN and password**, enter `user@domain`.
   - For **Unique identifier**, enter `objectGUID`
7. Create an XML file named `local-server.xml` and place it in the *`install_location`*`/configuration` directory.
8. In the `local-server.xml` file, enter values that are appropriate for your environment:

```
<?xml version="1.0" encoding="UTF-8"?>
<server>
    <featureManager>
        <feature>ldapRegistry-3.0</feature>
        <feature>appSecurity-2.0</feature>
    </featureManager>
    <ldapRegistry id="id" realm="realm"
    host="host" port="port" ignoreCase="true"
    baseDN="DC=dc,DC=dc,DC=dc" bindDN="CN=doejohn,
               OU=Users,DC=dc,DC=dc,DC=dc"
    bindPassword="password" ldapType="Microsoft Active Directory" sslEnabled="false">
        <activedFilters
            userFilter="(&amp;(sAMAccountName=%v)(objectcategory=user))"
            groupFilter="(&amp;(cn=%v)(objectcategory=group))"
            userIdMap="user:sAMAccountName"
            groupIdMap="*:cn"
            groupMemberIdMap="memberOf:member">
        </activedFilters>
    </ldapRegistry>
    <webAppSecurity allowFailOverToBasicAuth="true" displayAuthenticationRealm="true"/>
</server>
```

9. If Cognos Analytics is configured to use SSL, see "Configuring the SSL protocol for IBM Cognos components" on page 122 for more information.
10. To verify the configuration, log on to `http://`*`host`*`:`*`port`*`/bi` or `https://`*`host`*`:`*`port`*`/bi` for SSL enabled systems, where host is the fully qualified Cognos Analytics host domain.

You should not see the Cognos Analytics logon page. Instead, you should be prompted by the browser to log on.

What to do next

If you want to configure single sign-on (SSO) between the Cognos Analytics application that was set up with LTPA authentication, and the application is deployed into a WebSphere instance, install the WebSphere key on each Cognos Analytics dispatcher where LTPA was set up, and update the `local-server.xml` file with the following `<ltpa>` element:

```
<ltpa keysFileName="yourLTPAKeysFileName.keys"
keysPassword="keysPassword" expiration="120" />
```

For more information, see the WebSphere Liberty documentation.

OpenID Connect authentication provider

OpenID Connect is a simple identity layer on top of the OAuth 2.0 protocol. It is used for federated identity and authentication with multiple applications that use the same identity provider. OpenID Connect is the preferred web-based authentication provider if you want to federate IBM Cognos Analytics with other applications.

OpenID Connect is a modern standard that incorporates the OpenID and OAuth 2.0 standards. It is supported for both on-premises and Cloud installations of Cognos Analytics.

Cognos Analytics supports the following types of OpenID Connect identity providers:

- ADFS (Active Directory Federation Services)
- Azure AD (Active Directory)
- Generic
- Google
- IBMid (IBM identity provider)
- OKTA
- Ping
- SalesForce
- SiteMinder

Tip: Contact the identity provider administrator in your organization, or the sales and support organization, to find out which product version you should use.

OpenID Connect Authentication Proxy

Cognos Analytics now provides another provider type, 'OpenID Connect Authentication Proxy' in Cognos Configuration. This menu offers the option to have Trusted Signon Provider (TSP) for OpenID connect. Similar to OpenID Connect entries, you will see the list of Identity Providers currently supported.

Additional configuration setting entries under Advanced Properties are now visible. You will need to configure the claim you want passed to the real provider as well as the namespace ID of the real provider.

- Identity claim name: Specifies the name of the claim that will be provided to the target namespace (for example. John Doe)
- Trusted environment name: Specifies the environment variable name that will be used to transfer the claim to the target namespace (for example. REMOTE_USER)
- Redirect namespace ID: Specifies the namespace ID that will be invoked with the claim obtained from the OpenID identity provider (for example. LDAP)

Leveraging the identity provider single sign-on

If your OpenID Connect identity provider supports single sign-on and two-factor authentication, Cognos Analytics can leverage this functionality.

If the identity provider does not support single sign-on, when a user makes an authentication request to Cognos Analytics, the user is redirected to the OpenID Connect identity provider logon page. After providing the required information, the user is redirected back to Cognos Analytics with an authorization code that is redeemed for an ID token that contains the identity of the user. The user can then access Cognos Analytics.

If the identity provider supports single sign-on, the user receives the ID token when making the authentication request to Cognos Analytics, and can immediately access the application.

Federating IBMid with SAML 2.0 identity providers

IBMid is the IBM OpenID Connect identity provider. If your identity provider (IdP) does not support OpenID Connect, but supports SAML 2.0, you can use IBMid to configure an OpenID Connect namespace as your authentication provider in Cognos Analytics. Simply, choose IBMid as your identity provider when configuring the OpenID Connect namespace.

With this namespace configuration, you can federate Cognos Analytics with most SAML 2.0 identity providers. As a result, when users log on to Cognos Analytics, they are redirected to the IBMid sign-on page where they type their email address. If the email address is recognized by IBMid, the users are redirected to their organization SAML 2.0 identity provider logon page. In this page, the users complete the authentication process by providing their credentials. Then, they can access Cognos Analytics.

Configuring an OpenID Connect namespace

To use an OpenID Connect identity provider with IBM Cognos Analytics, you must configure an OpenID Connect namespace.

If you use IBMid as your OpenID Connect identity provider, see Managing OpenID connect namespaces for more information.

If users have authentication problems after you successfully configured your OpenID Connect namespace, use diagnostic logging in the **Manage** component of Cognos Analytics to troubleshoot issues. You need to create a new logging topic that is based on the predefined **AAA** topic. Modify the **AAA** logging topic by adding the following code to it:

```
{
"loggerDefinitions": [
{
"loggerName": "com.ibm.cognos.camaaa.internal.OIDC",
"level": "DEBUG",
"additivity": true
}
],
"topicName": "OIDC"
}
```

For more information on diagnostic logging, see Logging types and files.

Procedure

1. Open IBM Cognos Configuration on your Content Manager computer.
2. Under **Security** > **Authentication**, right-click and select **New resource** > **Namespace**.
3. For **Type (Group)**, select **OpenID connect**.
4. For **Type**, select one of the identity providers from the drop-down list that includes the supported identity providers.
5. Type the namespace name in the **Name** field, and then click **OK**.

   The new namespace is added in the **Explorer** pane under **Security** > **Authentication**, and its properties are displayed in the properties pane.

6. Specify values for the namespace properties.

   Tip: Information about each property is displayed in the user interface when you click the property.

   - The **Namespace ID** is used in the CAMID.
   - Specify values for **Discovery Endpoint**, **Client Identifier**, and **OpenID Connect client secret**, as suggested by your OpenID Connect administrator.
   - Update the **Return URL** with your gateway or dispatcher URL, as shown in the following example:

     `http://`*`mycompany`*`:9300/bi/completeAuth.jsp`

     If you use a load balancer in your environment, include the load balancer DNS entry in the **Return URL** in front of the gateway or dispatcher nodes, as shown in the following example:

     `https://`*`MyLoadbalancerDNS`*`.`*`mycompany`*`.com:443/ibmcognos/bi/completeAuth.jsp`

     In this example, the Cognos Analytics gateway is installed on the web server.

     If you are using a set of dispatcher nodes behind the load balancer where the Cognos Analytics gateway is not installed on the web server, the **Return URL** might look as follows:

     `https://`*`MyLoadbalancerDNS`*`.`*`mycompany`*`.com:9300/bi/completeAuth.jsp`

   Tip: The **Multitenancy** properties do not need to be specified now.
7. Import the OpenID Connect root certificate authority certificate into the Cognos Analytics keystore by using the Third-Party Certificate Tool.

   - On UNIX or Linux operating systems, type `ThirdPartyCertificateTool.sh -i -T -r` *`cert`*`.cer -p NoPassWordSet`
   - On Windows operating systems, type `ThirdPartyCertificateTool.bat -i -T -r` *`cert`*`.cer -p NoPassWordSet`

   Tip: Replace the *cert* variable with the name of the certificate file that is used by your OpenID Connect identity provider. For IBMid, the file name is `blueid.cer`.

   The command imports the contents into the `CAMKeystore` file in the `certs` directory by using the specified password.
8. Perform the same configuration steps on your backup Content Manager computer.
9. Restart the IBM Cognos service on the Content Manager and the backup Content Manager computers.

Results

All users who are registered with your OpenID Connect identity provider should now have access to Cognos Analytics.

Configuring IBM Cognos Components to Use Active Directory Server

If you install Content Manager on a Microsoft Windows operating system computer, you can configure an Active Directory namespace as your authentication source.

If you install Content Manager on a UNIX-based computer, you must instead use an LDAP namespace to configure Active Directory as your authentication source. If you install Content Manager on a mix of Windows and UNIX computers, you must use an LDAP namespace to configure Active Directory for all Content Managers. When you use an LDAP namespace to authenticate against Active Directory Server, you are limited to LDAP features only. You do not have access to Active Directory features such as advanced properties for domains and single signon with Kerberos delegation.

If you install Content Manager on a Linux-based computer, the same restrictions apply as for UNIX. You must use an LDAP namespace to configure Active Directory as your authentication source.

If you want to use Microsoft SQL Server or Microsoft Analysis Server as a data source and use single signon for authentication, you must use Active Directory as your authentication source.

You cannot connect to the Active Directory Global Catalog, which is a caching server for Active Directory Server. If the connection uses port 3268, you must change it. By default, Active Directory Server uses port 389.

Procedure

1. Configure IBM Cognos components to use an Active Directory Server namespace
2. Enable secure communication to the Active Directory Server, if required
3. Enable single signon between Active Directory and IBM Cognos components

Configuring an Active Directory Namespace

You can use Active Directory Server as your authentication provider.

You also have the option of making custom user properties from the Active Directory Server available to IBM Cognos components.

Before you begin

For IBM Cognos to work properly with Active Directory Server, ensure that the Authenticated users group has Read privileges for the Active Directory folder where users are stored.

If you are configuring an Active Directory namespace to support single signon with a Microsoft SQL Server or Microsoft Analysis Server data source, ensure the following configuration:

- The IBM Cognos gateway is installed on an IIS web server that is configured for Integrated Authentication on Microsoft Windows operating system.
- The gateway is assigned to the local intranet website in your web browser.
- Content Manager is installed on a Windows 2008 or Windows 2012 server.
- Content Manager, Application Tier Components, IIS web server, and the data source server (Microsoft SQL Server or Microsoft Analysis Server) belong to the Active Directory domain.
- The data source connection for Microsoft SQL Server or Microsoft Analysis Server is configured for **External Namespace** and that namespace must be the Active Directory namespace.

For more information about data sources, see the *IBM Cognos Analytics Administration and Security Guide*.

Procedure

1. In every location where you installed Content Manager, open IBM Cognos Configuration.
2. In the **Explorer** window, under **Security,** right-click **Authentication**, and then click **New resource** > **Namespace**.
3. In the **Name** box, type a name for your authentication namespace.
4. In the **Type** list, click the appropriate namespace and then click **OK**.

   The new authentication provider resource appears in the **Explorer** window, under the Authentication component.
5. In the **Properties** window, for the **Namespace ID** property, specify a unique identifier for the namespace.
6. Specify the values for all other required properties to ensure that IBM Cognos components can locate and use your existing authentication provider.
7. Specify the values for the **Host and port** property.

   To support Active Directory Server failover, you can specify the domain name instead of a specific domain controller.

   For example, use *mydomain*.com:389 instead of dc1.*mydomain*.com:389.
8. If you want to search for details when authentication fails, specify the user ID and password for the **Binding credentials** property.

Use the credentials of an Active Directory Server user who has search and read privileges for that server.

9. From the **File** menu, click **Save**.
10. Test the connection to a new namespace. In the **Explorer** window, under **Authentication**, right-click the new authentication resource and click **Test**.

    You are prompted to enter credentials for a user in the namespace to complete the test.

    Depending on how your namespace is configured, you can enter either a valid user ID and password for a user in the namespace or the bind user DN and password.

Results

IBM Cognos loads, initializes, and configures the provider libraries for the namespace.

Make Custom User Properties for Active Directory Available to IBM Cognos Components

You can use arbitrary user attributes from your Active Directory Server in IBM Cognos components. To configure this, you must add these attributes as custom properties for the Active Directory namespace.

The custom properties are available as session parameters through Framework Manager. For more information about session parameters, see the *Framework Manager User Guide*

You can also use the custom properties inside command blocks to configure Oracle sessions and connections. You can use the command blocks can be used with Oracle light-weight connections and virtual private databases. For more information, see the *IBM Cognos Analytics Administration and Security Guide*.

Procedure

1. In every location where you installed Content Manager, open IBM Cognos Configuration.
2. In the **Explorer** window, under **Security** > **Authentication**, click the Active Directory namespace.
3. In the **Properties** window, click in the **Value** column for **Custom properties** and click the edit icon.
4. In the **Value - Custom properties** window, click **Add**.
5. Click the **Name** column and type the name you want IBM Cognos components to use for the session parameter.
6. Click the **Value** column and type the name of the account parameter in your Active Directory Server.
7. Repeat steps 4 to 6 for each custom parameter.
8. Click **OK**.
9. From the **File** menu, click **Save**.

Enabling Secure Communication to the Active Directory Server

If you are using an SSL connection to the Active Directory Server, you must copy the certificate from the Active Directory Server to the Content Manager location.

Procedure

1. In every Content Manager location, use your Web browser to connect to the Active Directory Server and copy the CA root certificate to the Content Manager location.
2. Add the CA root certificate to the certificate store of the account that you are using for the current IBM Cognos session:

    - If you are running the IBM Cognos session under a user account, use the same Web browser as in step 1 to import the CA root certificate to the certificate store for your user account.

      For information, see the documentation for your Web browser.
    - If you are running the IBM Cognos session under the local account, use Microsoft Management Console (MMC) to import the CA root certificate to the certificate store for the local computer.

For information, see the documentation for MMC.

3. In IBM Cognos Configuration, restart the service:
   - In the **Explorer** window, click **IBM Cognos services**, **IBM Cognos**.
   - From the **Actions** menu, click **Restart**.

Include or Exclude Domains Using Advanced Properties

When you configure an authentication namespace for IBM Cognos, users from only one domain can log in. By using the Advanced properties for Active Directory Server, users from related (parent-child) domains and unrelated domain trees within the same forest can also log in. There is no cross-forest support; there must be a namespace for each forest.

If you set a parameter named chaseReferrals to true, users in the original authenticated domain and all child domains of the domain tree can log in to IBM Cognos. Users from a parent domain of the original authenticated domain or in a different domain tree cannot log in.

If you set a parameter named MultiDomainTrees to true, users in all domain trees in the forest can log in to IBM Cognos.

Procedure

1. In every location where you installed Content Manager, open IBM Cognos Configuration.
2. In the **Explorer** window, under **Security** > **Authentication**, click the Active Directory namespace.
3. In the **Properties** window, specify the **Host and port** property:
   - For users in one domain, specify the host and port of a domain controller for the single domain.
   - For users in one domain tree, specify the host and port of the top-level controller for the domain tree.
   - For users in all domain trees in the forest, specify the host and port of any domain controller in the forest.
4. Click in the Value column for **Advanced properties** and click the edit icon.
5. In the **Value - Advanced properties** window, click **Add**.
6. Specify two new properties, **chaseReferrals** and **MultiDomainTrees**, with the values from the following table:

Table 32: Advanced properties settings

Authentication for	chaseReferrals	MultiDomainTrees
One domain	False	False
One domain tree	True	False
All domain trees in the forest	True	True

7. Click **OK**.
8. From the **File** menu, click **Save**.

Enable single signon between Active Directory Server and IBM Cognos components

By default, the Active Directory provider uses Kerberos authentication. It integrates with the Microsoft Internet Information Services (IIS) web server for single signon if Windows authentication (formerly named NT Challenge Response) is enabled on the IIS web server.

If Windows authentication is enabled, you are not prompted to reenter authentication information when you access IBM Cognos content that is secured by the Active Directory namespace.

If you use Kerberos authentication, you can choose to use Service for User (S4U). S4U allows users to access IBM Cognos Analytics from computers not on the Active Directory domain. To enable S4U, you must use enable constrained delegation.

For example, you have users whose computers do not belong to the domain, but they do have the domain account. When they open their web browsers, they are prompted for their domain account. However, they get the Kerberos ticket with Identity privilege only, which prevents them from getting authenticated to IBM Cognos Analytics. To resolve this issue, you can use S4U.

If you do not want Kerberos authentication, you can configure the provider to access the environment variable REMOTE_USER to achieve single signon.

Important: Ensure that you use only the variable REMOTE_USER. Using another variable can cause a security vulnerability.

To enable single signon to use Kerberos authentication, you must ensure that you complete the following tasks:

1. Configure Windows authentication on your Microsoft IIS web server for the ibmcognos/cgi-bin application.
2. Install Content Manager on a computer that is part of the Active Directory domain, for the active and standby Content Managers.
3. Set up the computers, or the user account under which Content Manager runs, to be trusted.

For more information, see the following technote documents:

- Enabling single sign-on to CRN or Cognos secured against Active Directory technote (www.ibm.com/support/docview.wss?uid=swg21341889)
- When using Kerberos Single Sign-on (SSO) with Active Directory in Cognos, user is prompted for credentials technote (www.ibm.com/support/docview.wss?uid=swg21659267)

Enabling single signon between Active Directory Server and IBM Cognos Components to use REMOTE_USER

If you do not want Kerberos authentication, you can configure the provider to access the environment variable REMOTE_USER to achieve single signon.

You must set the advanced property singleSignonOption to the value IdentityMapping. You must also specify bind credentials for the Active Directory namespace.

Microsoft IIS sets REMOTE_USER by default when you enable Windows authentication. If Kerberos authentication is not used, single signon to Microsoft OLAP (MSAS) data sources is not possible.

When you define the REMOTE_USER, you can also choose to save the REMOTE_USER as a trusted credential. Saving as a trusted credential means that scheduled jobs authenticate the REMOTE_USER with the **Binding Credential** privileges.

Important: Ensure that you use only the variable REMOTE_USER. Using another variable can cause a security vulnerability.

Procedure

1. On the computer where you installed Content Manager, open IBM Cognos Configuration.
2. In the **Explorer** window, under **Security** > **Authentication**, and select the Active Directory namespace.
3. Click in the **Value** column for **Advanced properties** and then click the edit icon.
4. In the **Value - Advanced properties** dialog box, click **Add**.
5. In the **Name** column, type `singleSignonOption`
6. In the **Value** column, type `IdentityMapping`.
7. If you want to save the REMOTE_USER as a trusted credential, in the **Value - Advanced properties** dialog box, click **Add**.
8. In the **Name** column, type `trustedCredentialType`.
9. In the **Value** column, type `IdentityMappingForTC`.
10. Click **OK**.

11. Click in the **Value** column for **Binding credentials**, and then click the edit icon.
12. In the **Value - Binding credentials** dialog box, specify a user ID and password and then click **OK**.

Enabling single signon to use Kerberos authentication
If your IIS web server is configured for Windows authentication, you do not have to add any additional settings. Kerberos authentication is used as the default.

Enabling single signon to use Kerberos authentication with constrained delegation
To be able to use constrained delegation, you must define the service principal names (SPN) for the users that are configured to run the IBM Cognos components and your Microsoft Internet Information Services (IIS) web server's application pool in your Active Directory domain.

If you use Kerberos with constrained delegation, you must add an sAMAccountName user for Content Manager when you configure your gateway. All active and stand by Content Managers must be configured to run under the same account.

If you are configuring single signon to your database servers, you must configure the sAMAccountName for the user who runs the Application Tier Components when you add the Active Directory namespace. All Application Tier Components must be configured to run under the same account.

The SPNs are the users that you enter in the sAMAccountName fields in IBM Cognos Configuration.

For example, assume that you have one user who runs the Content Manager component, another who runs the Application Tier Components, and another who runs your web server's application pool. The Content Manager user is `CognosCMUser`. The Application Tier Components user is `CognosATCUser`. The application pool user is `IISUser`. Each user is in the `MyDomain` domain.

1. You must set up IIS so that your `MyDomain\IISUser` is the application pool identity
2. Run the `setspn` command for the computer where IIS is running.

   For example:

   ```
   setspn -A http/IISServerName MyDomain\IISUser
   setspn -A http/IISServerName.MyDomain.com MyDomain\IISUser
   ```

3. Run the `setspn` command for your IBM Cognos users.

   For example:

   ```
   setspn -A ibmcognosba/CognosCMUser MyDomain\CognosCMUser
   setspn -A ibmcognosba/CognosATCUser MyDomain\CognosATCUser
   ```

   In these commands, you must use `ibmcognosba` as shown in the examples. The user names and domains must match your environment.

   Note: In this example, the sAMAccountName users you must enter are `CognosCMUser` and `CognosATCUser`.

4. If you are configuring single signon to your Microsoft SQL Server or Microsoft SQL Server Analysis Services database server, you must set up the SPN for the database server. For more information, see you database server documentation.
5. Finally, you must configure the constrained delegation in the Active Directory Users and Computers administration tool. On the **Delegation** tab for all users (`IISUser`, `CognosCMUser`, and `CognosATCUser`), you must select **Trust this user for delegation to specified services only** and **Use Kerberos only** to use Kerberos with constrained delegation. Select **Trust this user for delegation to specified services only** and **Use any authentication protocol** if you are using the S4U Kerberos extension.

   And then you must add the required SPNs. For example, add `ibmcognosba` as a service type. And add `DomainController1` and `DomainController2` as service type `ldap`.

   If you are configuring single signon for the datasource, add the MSOLAPSvc3 or MSQLSVC service.

Procedure

1. On the computer where you installed Content Manager, open IBM Cognos Configuration.
2. In the **Explorer** window, under **Security** > **Authentication**, and select the Active Directory namespace.
3. Click in the **Value** column for **Advanced properties** and then click the edit icon.
4. In the **Value - Advanced properties** dialog box, click **Add**.
5. In the **Name** column, type `singleSignonOption`.
6. In the **Value** column, enter one of the following values:

    - Enter `KerberosS4UAuthentication` if you want to use Kerberos authentication first. If Kerberos fails, Service For User (S4U) authentication is attempted. If S4U fails, the user is prompted for credentials.
    - Enter `S4UAuthentication` if you want to use S4U authentication first. If S4U fails, the user is prompted for credentials.
7. In the **Value - Advanced properties** dialog box, click **Add**.
8. In the **Name** column, type `trustedCredentialType`.
9. In the **Value** column, enter one of the following values:

    - Enter `CredentialForTC` if you want to save the user's credentials as a trusted credential. For example, if you want to use the credentials to run scheduled jobs.
    - Enter `S4UForTC` if you want to save only the authenticated user name as a trusted credential. The user name is saved in UPN format, and scheduled jobs can be run with the UPN without requiring the user's password.
10. Click **OK**.
11. Click in the **Value** column for **Application Tier Components sAMAccountName**, and enter the sAMAccountName of the user who runs the Application Tier Components.

    Important: This value is required only if you are configuring single signon to your Microsoft SQL Server or Microsoft SQL Server Analysis Services database server. If you are not configuring single signon to the database server, do not change this value.
12. Click **File** > **Save**.
13. Restart the IBM Cognos service.
14. On the computer where you installed the Gateway components, open IBM Cognos Configuration.
15. In the **Explorer** window, click **Environment**.
16. Click in the **Value** column for **Content Manager sAMAccountName**, and enter the sAMAccountName of the user who runs Content Manager.
17. Click **File** > **Save**.

Configuring IBM Cognos to Use IBM Cognos Series 7 Namespace

You can configure IBM Cognos components to use an IBM Cognos Series 7 namespace as the authentication provider. Users are authenticated based on the authentication and signon configuration of the IBM Cognos Series 7 namespace.

An IBM Cognos Series 7 namespace is required if you want to use IBM Cognos Series 7 PowerCubes and Transformer models in IBM Cognos Analytics. You must configure the namespace before you load the Transformer models.

Note: You cannot use an IBM Cognos Series 7 Local Authentication Export (LAE) file for authentication with IBM Cognos components.

You can configure IBM Cognos components to use multiple IBM Cognos Series 7 authentication providers. All IBM Cognos Series 7 namespaces must use the same primary IBM Cognos Series 7 Ticket Server.

Otherwise, you can receive errors or be prompted for authentication more than one time. To maintain performance, also ensure that the ticket server is running.

If you change the configuration information that is stored in the directory server that is used for IBM Cognos Series 7, you must restart the IBM Cognos service before the changes take effect in the IBM Cognos installation.

A user must be in at least one Access Manager user class to log on to IBM Cognos components.

Procedure

1. Configure a Series 7 namespace
2. Enable secure communication to the directory server used by the IBM Cognos Series 7 namespace, if required
3. Enable single signon between IBM Cognos Series 7 and IBM Cognos

Configuring an IBM Cognos Series 7 Namespace

You can configure IBM Cognos to use one or more IBM Cognos Series 7 namespaces for authentication.

Procedure

1. In every location where you installed Content Manager, open IBM Cognos Configuration.
2. In the **Explorer** window, under **Security,** right-click **Authentication**, and then click **New resource** > **Namespace**.
3. In the **Name** box, type a name for your authentication namespace.
4. In the **Type** list, click the appropriate namespace and then click **OK**.

   The new authentication provider resource appears in the **Explorer** window, under the Authentication component.
5. In the **Properties** window, for the **Namespace ID** property, specify a unique identifier for the namespace.
6. Specify the values for all other required properties to ensure that IBM Cognos components can locate and use your existing authentication provider.

   If your IBM Cognos Series 7 namespace version is 16.0, ensure that the **Data encoding** property is set to **UTF-8**. In addition, the locations where Content Manager is installed must use the same locale as the data in the IBM Cognos Series 7 namespace.

   The host value can be a server name or an IP address. If you are publishing from PowerPlay Enterprise Server to IBM Cognos Analytics, you must use the same value format that is used in IBM Cognos Series 7 Configuration Manager for the location of the directory server.

   For example, if the server name is used in IBM Cognos Series 7 Configuration Manager, you must also use the server name in IBM Cognos Configuration for IBM Cognos Analytics.
7. If your namespace environment includes version 15.2 of the IBM Cognos Series 7 namespace, you must disable the **Series7NamespacesAreUnicode** setting.
   - In the **Properties** window, in the **Advanced Properties** value, click the edit icon.
   - In the **Value - Advanced properties** window, click **Add**.
   - In the **Name** box, type **Series7NamespacesAreUnicode**.
   - In the **Value** box, type **False**, and then click **OK**.
8. In the **Properties** window, under **Cookie settings**, ensure that the **Path**, **Domain**, and **Secure flag enabled** properties match the settings that are configured for IBM Cognos Series 7.
9. From the **File** menu, click **Save**.
10. Test the connection to a new namespace. In the **Explorer** window, under **Authentication**, right-click the new authentication resource and click **Test**.

    You are prompted to enter credentials for a user in the namespace to complete the test.

Depending on how your namespace is configured, you can enter either a valid user ID and password for a user in the namespace or the bind user DN and password.

Enabling Secure Communication to the Directory Server Used by the IBM Cognos Series 7 Namespace

If you are using an SSL connection to the Directory Server used by the IBM Cognos Series 7 namespace, you must copy the certificate from the Directory Server to each Content Manager location.

For more information, see the IBM Cognos Access Manager *Administrator Guide* and the documentation for your Directory Server.

Enabling Single Signon Between IBM Cognos Series 7 and IBM Cognos

If your IBM Cognos Series 7 namespace has been configured for integration with your external authentication mechanisms for single signon, the IBM Cognos Series 7 provider will automatically use this configuration.

By configuring single signon, you are not prompted to reenter authentication information when accessing IBM Cognos content that is secured by the IBM Cognos Series 7 namespace.

Procedure

1. Ensure that you configured IBM Cognos components to use an IBM Cognos Series 7 namespace as an authentication provider.
2. For IBM Cognos Series 7, start Configuration Manager.
3. Click **Open the current configuration**.
4. On the **Components** tab, in the **Explorer** window, expand **Services**, **Access Manager - Web Authentication** and click **Cookie Settings**.
5. In the **Properties** window, ensure that the **Path**, **Domain**, and **Secure Flag Enabled** properties match the settings configured for IBM Cognos Analytics.
6. Save and close Configuration Manager.
7. If the IBM Cognos Series 7 namespace uses the Trusted Signon plug-in for single signon, you must now define the SaferAPIGetTrustedSignonWithEnv function.

Results

You can now add IBM Cognos Upfront Series 7 NewsBoxes to IBM Cognos Analytics.

IBM Cognos Series 7 Namespaces and the IBM Cognos Series 7 Trusted Signon Plug-in

If the IBM Cognos Series 7 namespace uses the Trusted Signon plug-in for single signon, you must define the SaferAPIGetTrustedSignonWithEnv function in your plug-in. Then you must recompile and redeploy the library for single signon to be achieved between IBM Cognos components and your authentication mechanism.

The SaferAPIGetTrustedSignonWithEnv function is an updated version of the SaferAPIGetTrustedSignon function. This update is required because IBM Cognos logon is not performed at the Web server as is the case for IBM Cognos Series 7 applications. Therefore, it is not possible for the plug-in to perform a getenv() API call to retrieve Web server environment variables. The plug-in can request that specific environment variables be removed from the Web server using the SaferAPIGetTrustedSignonWithEnv function.

If you are running both IBM Cognos Series 7 and IBM Cognos products using the same plug-in, both the SaferAPIGetTrustedSignonWithEnv and SaferAPIGetTrustedSignon functions are required. For information about the SaferAPIGetTrustedSignon function, see the IBM Cognos Series 7 documentation.

SaferAPIGetTrustedSignonWithEnv Function

For users to be successfully authenticated by Access Manager, OS signons must exist and be enabled in the current namespace.

The memory for the returned trustedSignonName and trustedDomainName is allocated internally in this API. If the function returns SAFER_SUCCESS, Access Manager calls SaferAPIFreeTrustedSignon to free the memory allocated.

The memory for the returned reqEnvVarList is allocated internally in this API. If the function returns SAFER_INFO_REQUIRED, Access Manager calls SaferAPIFreeBuffer() to free the memory allocated.

You must implement both the SaferAPIGetTrustedSignon and SaferAPIFreeBuffer functions to successfully register the library when SaferAPIGetTrustedSignonWithEnv is implemented. The function SaferAPIGetError is required only if you want specific error messages returned from your plug-in.

Syntax

```
SaferAPIGetTrustedSignonWithEnv(

   EnvVar             envVar[],                  /*[IN]*/

   char               **reqEnvVarList,           /*[OUT]*/

   void               **trustedSignonName,       /*[OUT]*/

   unsigned long      *trustedSignonNameLength,  /*[OUT]*/

   void               **trustedDomainName,       /*[OUT]*/

   unsigned long      *trustedDomainNameLength,  /*[OUT]*/

   SAFER_USER_TYPE    *userType,                 /*[OUT]*/

   void               **implementerData);        /*[IN/OUT]*/
```

Parameters for the SaferAPIGetTrustedSignonWithEnv Function

Table 33: Parameters and description for the SaferAPIGetTrustedSignonWithEnv Function

Parameter	Description
[in] envVar	An array of environment variable names and values that were retrieved from the Web server. The end of the array is represented by an entry with a null envVarName and a null envVarValue. Note that the first time this API is called, the envVar array contains only the end of array marker.
[in] reqEnvVarList	A string that contains a comma-separated list of environment variable names that are requested by the Safer implementation. The end of the list must be null-terminated.
[out] trustedSignonName	A sequence of bytes that identifies the currently authenticated user. This value does not need to be null-terminated. This value is mandatory.
[out] trustedSignonNameLength	An integer value that indicates the length of the trustedSignonName. This length should exclude the null terminator, if there is one. This value is mandatory.

Table 33: Parameters and description for the SaferAPIGetTrustedSignonWithEnv Function (continued)

Parameter	Description
[out] trustedDomainName	A sequence of bytes that identifies the domain of the currently authenticated user. You do not need to null-terminate this value. If there is no trustedDomainName, the return is null. This value is optional.
[out] trustedDomainNameLength	An integer value that indicates the length of the trustedDomainName. This length should exclude the null terminator, if there is one. This value is mandatory and must be set to zero if there is no trustedDomainName.
[out] userType	A value that indicates the type of user that Access Manager will authenticate. This value is mandatory. The following return values are required for Access Manager to successfully authenticate users: **SAFER_NORMAL_USER** A named user. OS signons must exist and be enabled in the current namespace. **SAFER_GUEST_USER** A guest user. A guest user account must exist and be enabled in the current namespace. **SAFER_ANONYMOUS_USER** An anonymous user. An anonymous user account must exist and be enabled in the current namespace.
[in/out] implementerData	A pointer used to preserve implementation-specific data between invocations. An invocation occurs every time Access Manager calls the trusted signon plug-in. This value is valid only if the trusted signon plug-in was invoked and you set a value for it.

Configuring IBM Cognos to Use a Custom Authentication Provider

If you implemented a custom Java authentication provider with your existing security infrastructure, you can configure IBM Cognos components to use it.

You can use a custom authentication provider to access and authenticate users to an authentication source. You can also use it as a single signon mechanism to integrate IBM Cognos components with your security infrastructure. You can hide the namespace from users during logon.

For more information, see the Custom Authentication Provider *Developer Guide*.

Configure a Custom Authentication Namespace

You can configure IBM Cognos components to use a custom authentication namespace. Any additional configuration for authentication source access, single signon, or custom attributes are dependent on the custom authentication provider implementation.

Ensure that the versions of Java runtime environment (JRE) and Java Software Development Kit that you use are compatible with each other. If you use supported versions of the JRE and Java Software Development Kit that are not compatible with each other, then the custom Java authentication provider that you configure will not appear in the list of namespaces in IBM Cognos Configuration.

Procedure

1. In every location where Content Manager is installed, open IBM Cognos Configuration.
2. In the **Explorer** window, under **Security,** right-click **Authentication**, and click **New resource** > **Namespace**.
3. In the **Name** box, type a name for your authentication namespace.
4. In the **Type** list, select **Custom Java Provider** and then click **OK**.

   The new authentication provider resource appears in the **Explorer** window, under the **Authentication** component.
5. In the **Properties** window, for the **NamespaceID** property, specify a unique identifier for the namespace.

   Tip: Do not use colons (:) in the Namespace ID property.
6. Specify the values for all other required properties to ensure that IBM Cognos can locate and use your existing authentication provider.
7. From the **File** menu, click **Save**.
8. Test the connection to a new namespace. In the **Explorer** window, under **Authentication**, right-click the new authentication resource and click **Test**.

   You are prompted to enter credentials for a user in the namespace to complete the test.

   Depending on how your namespace is configured, you can enter either a valid user ID and password for a user in the namespace or the bind user DN and password.

Results

IBM Cognos loads, initializes, and configures the provider libraries for the namespace.

Hide the Namespace from Users During Login

You can hide namespaces from users during login. You can have trusted signon namespaces without showing them on the namespace selection list that is presented when users log in.

For example, you may want to integrate single signon across systems but maintain the ability for customers to authenticate directly to IBM Cognos without being prompted to choose a namespace.

Procedure

1. In each location where you configured a custom Java authentication provider, open IBM Cognos Configuration.
2. In the **Explorer** window, under **Security** > **Authentication**, click the custom Java authentication provider.
3. In the **Properties** window, click the box next to **Selectable for authentication** and select **False**.
4. From the **File** menu, click **Save**.

Results

The namespace is not shown on the selection list that is presented at login.

Configuring IBM Cognos components to use LDAP

You can configure IBM Cognos components to use an LDAP namespace as the authentication provider. You can use an LDAP namespace for users that are stored in an LDAP user directory, Active Directory Server, IBM Directory Server, Novell Directory Server, or Oracle Directory Server.

You can also use LDAP authentication with IBM Db2 and Essbase OLAP data sources by specifying the LDAP namespace when you set up the data source connection. For more information, see the *IBM Cognos Analytics Administration and Security Guide*.

You also have the option of making custom user properties from the LDAP namespace available to IBM Cognos components.

If you want to bind users to the LDAP server, see "LDAP mapping" on page 182.

Procedure

1. "Configuring an LDAP namespace" on page 182
2. Make custom user properties available to IBM Cognos components, if required
3. Enable secure communication to the LDAP server, if required
4. Enable single signon between LDAP and IBM Cognos components, if required

LDAP mapping

To bind a user to the LDAP server, the LDAP authentication provider must construct the distinguished name (DN). If the Use external identity property is set to True, it uses the External identity mapping property to try to resolve the user's DN. If it cannot find the environment variable or the DN in the LDAP server, it attempts to use the User lookup property to construct the DN.

If users are stored hierarchically within the directory server, you can configure the User lookup and External identity mapping properties to use search filters. When the LDAP authentication provider performs these searches, it uses the filters that you specify for the User lookup and External identity mapping properties. It also binds to the directory server by using the value you specify for the Bind user DN and password property or by using anonymous if no value is specified.

When an LDAP namespace is configured to use the External identity mapping property for authentication, the LDAP provider binds to the directory server by using the Bind user DN and password or by using anonymous if no value is specified. All users who log on to IBM Cognos by using external identity mapping see the same users, groups, and folders as the Bind user.

If you do not use external identity mapping, you can specify whether to use bind credentials to search the LDAP directory server by configuring the **Use bind credentials for search** property. When the property is enabled, searches are performed by using the bind user credentials or by using anonymous if no value is specified. When the property is disabled, which is the default setting, searches are performed by using the credentials of the logged-on user. The benefit of using bind credentials is that instead of changing administrative rights for multiple users, you can change the administrative rights for the bind user only.

Note: If you use a DN syntax, such as `uid=${userID}, ou=mycompany.com`, for the properties **User lookup**, **External identity mapping**, or **Bind user DN and password,** you must escape all special characters that are used in the DN. If you use a search syntax, such as `(uid=${userID})`, for the properties **User lookup** or **External identity mapping**, you must not escape special characters that are used in the DN.

Configuring an LDAP namespace

You can configure IBM Cognos components to use an LDAP namespace when the users are stored in an LDAP user directory. The LDAP user directory may be accessed from within another server environment, such as Active Directory Server or CA SiteMinder.

If you are configuring an LDAP namespace for a directory server other than LDAP, see the appropriate section:

- For Active Directory Server, see Configure an LDAP Namespace for Active Directory Server.
- For IBM Directory Server, see Configure an LDAP Namespace for IBM Directory Server.
- For Novell Directory Server, see Configure an LDAP Namespace for Novell Directory Server.
- For Oracle Directory Server, see Configure an LDAP Namespace for Oracle Directory Server.

You can also use LDAP authentication with IBM Db2 and Essbase OLAP data sources by specifying the LDAP namespace when you set up the data source connection. For more information, see the *IBM Cognos Analytics Administration and Security Guide*.

Procedure

1. In every location where you installed Content Manager, open IBM Cognos Configuration.
2. In the **Explorer** window, under **Security,** right-click **Authentication**, and then click **New resource** > **Namespace**.
3. In the **Name** box, type a name for your authentication namespace.
4. In the **Type** list, click the appropriate namespace and then click **OK**.

   The new authentication provider resource appears in the **Explorer** window, under the Authentication component.
5. In the **Properties** window, for the **Namespace ID** property, specify a unique identifier for the namespace.
6. Specify the values for all other required properties to ensure that IBM Cognos components can locate and use your existing authentication provider.
7. If you want the LDAP authentication provider to bind to the directory server by using a specific **Bind user DN and password** when you perform searches, then specify these values.

   If no values are specified, the LDAP authentication provider binds as anonymous.

   If external identity mapping is enabled, **Bind user DN and password** are used for all LDAP access. If external identity mapping is not enabled, **Bind user DN and password** are used only when a search filter is specified for the **User lookup** property. In that case, when the user DN is established, subsequent requests to the LDAP server are run under the authentication context of the user.
8. If you do not use external identity mapping, use bind credentials for searching the LDAP directory server by doing the following step:

   - Ensure that **Use external identity** is set to **False**.
   - Set **Use bind credentials for search** to **True**.
   - Specify the user ID and password for **Bind user DN and password**.

   If you do not specify a user ID and password, and anonymous access is enabled, the search is done by using anonymous.
9. Check the mapping settings for the required objects and attributes.

   Depending on the LDAP configuration, you may have to change some default values to ensure successful communication between IBM Cognos components and the LDAP server.

   LDAP attributes that are mapped to the **Name** property in **Folder mappings**, **Group mappings**, and **Account mappings** must be accessible to all authenticated users. In addition, the **Name** property must not be blank.
10. From the **File** menu, click **Save**.
11. Test the connection to a new namespace. In the **Explorer** window, under **Authentication**, right-click the new authentication resource and click **Test**.

    You are prompted to enter credentials for a user in the namespace to complete the test.

    Depending on how your namespace is configured, you can enter either a valid user ID and password for a user in the namespace or the bind user DN and password.

Results

IBM Cognos loads, initializes, and configures the provider libraries for the namespace.

Configuring an LDAP namespace for Active Directory Server

If you configure a new LDAP namespace for use with an Active Directory Server, default values are generated for you.

Procedure

1. In every location where you installed Content Manager, open IBM Cognos Configuration.
2. In the **Explorer** window, under **Security,** right-click **Authentication**, and then click **New resource** > **Namespace**.
3. In the **Name** box, type a name for your authentication namespace.
4. In the **Type** list, select **LDAP - Default values for Active Directory** and then click **OK**.

   The new authentication provider resource appears in the **Explorer** window, under the **Authentication** component. Default values are generated for you. Check them and make changes as needed.
5. In the **Properties** window, for the **NamespaceID** property, specify a unique identifier for the namespace.

   Tip: Do not use colons (:) in the Namespace ID property.
6. Specify the values for all other required properties to ensure that IBM Cognos components can locate and use your existing authentication provider.

   The following settings are examples:

   - For **User lookup**, enter `(sAMAccountName=${userID})`
   - If you use single signon, for **Use external identity**, set the value to **True**.
   - If you use single signon, for **External identity mapping**, enter `(sAMAccountName=${environment("REMOTE_USER")})`

     If you want to remove the domain name from the REMOTE_USER variable, enter `(sAMAccountName=${replace(${environment("REMOTE_USER")}, "domain\\","")})`.

     Important: Ensure that you use only the variable REMOTE_USER. Using another variable can cause a security vulnerability.
   - For **Bind user DN and password**, enter `user@domain`.
   - For **Unique identifier**, enter `objectGUID`
7. If you want the LDAP authentication provider to bind to the directory server by using a specific **Bind user DN and password** when you perform searches, then specify these values.

   If no values are specified, the LDAP authentication provider binds as anonymous.
8. If you do not use external identity mapping, use bind credentials for searching the LDAP directory server by doing the following steps:

   - Ensure that **Use external identity** is set to **False**.
   - Set **Use bind credentials for search** to **True**.
   - Specify the user ID and password for **Bind user DN and password**.
9. From the **File** menu, click **Save**.
10. Test the connection to a new namespace. In the **Explorer** window, under **Authentication**, right-click the new authentication resource and click **Test**.

    You are prompted to enter credentials for a user in the namespace to complete the test.

    Depending on how your namespace is configured, you can enter either a valid user ID and password for a user in the namespace or the bind user DN and password.

Results

IBM Cognos loads, initializes, and configures the provider libraries for the namespace.

Configuring an LDAP namespace for IBM Directory Server

If you configure a new LDAP namespace for use with an IBM Directory Server, default values are generated for you.

Procedure

1. In every location where you installed Content Manager, open IBM Cognos Configuration.
2. In the **Explorer** window, under **Security,** right-click **Authentication**, and then click **New resource** > **Namespace**.
3. In the **Name** box, type a name for your authentication namespace.
4. In the **Type** list, click **LDAP - Default values for IBM Tivoli**, and then click **OK**.

   The new authentication namespace resource appears in the **Explorer** window, under the **Authentication** component. Check them and make changes as needed.
5. In the **Properties** window, for the **NamespaceID** property, specify a unique identifier for the namespace.

   Tip: Do not use colons (:) in the Namespace ID property.
6. Specify the values for all other required properties to ensure that IBM Cognos can locate and use your existing authentication namespace.
   - For **User lookup**, specify `(cn=${userID})`
   - For **Bind user DN and password**, specify *`cn=root`*
7. If you want the LDAP authentication provider to bind to the directory server by using a specific **Bind user DN and password** when you perform searches, then specify these values.

   If no values are specified, the LDAP authentication provider binds as anonymous.
8. If you do not use external identity mapping, use bind credentials for searching the LDAP directory server by doing the following steps:
   - Ensure that **Use external identity** is set to **False**.
   - Set **Use bind credentials for search** to **True**.
   - Specify the user ID and password for **Bind user DN and password**.
9. From the **File** menu, click **Save**.

Configuring an LDAP namespace for Novell Directory Server

If you configure a new LDAP namespace for use with a Novell Directory Server, you must modify the necessary settings and change the values for all properties of the Novell Directory objects.

Procedure

1. In every location where you installed Content Manager, open IBM Cognos Configuration.
2. In the **Explorer** window, under **Security,** right-click **Authentication**, and then click **New resource** > **Namespace**.
3. In the **Name** box, type a name for your authentication namespace.
4. In the **Type(Group)** list, click **LDAP**, then in the **Type** list, choose **LDAP - General default values**, and then click **OK**.

   The new authentication namespace resource appears in the **Explorer** window, under the **Authentication** component.
5. In the **Properties** window, for the **Namespace ID** property, specify a unique identifier for the namespace.

   Tip: Do not use colons (:) in the Namespace ID property.
6. Specify the values for all other required properties to ensure that IBM Cognos can locate and use your existing authentication namespace.
   - For **User lookup**, specify `(cn=${userID})`
   - For **Bind user DN and password**, specify the base DN for an administration user, such as `cn=`*`Admin`*`,o=`*`COGNOS`*

7. If you want the LDAP authentication provider to bind to the directory server by using a specific **Bind user DN and password** when you perform searches, then specify these values.

   If no values are specified, the LDAP authentication provider binds as anonymous.
8. If you do not use external identity mapping, use bind credentials for searching the LDAP directory server by doing the following steps:
   - Ensure that **Use external identity** is set to **False**.
   - Set **Use bind credentials for search** to **True**.
   - Specify the user ID and password for **Bind user DN and password**.
9. To configure the LDAP advanced mapping properties for use with Novell Directory Server objects, use the values specified in the following table.

Table 34: LDAP advanced mapping values for use with Novell Directory Server objects

Mappings	LDAP property	LDAP value
Folder	Object class	organizationalunit,organization,container
	Description	description
	Name	ou,o,cn
Group	Object class	groupofnames
	Description	description
	Member	member
	Name	cn
Account	Object class	inetOrgPerson
	Business phone	telephonenumber
	Content locale	Language
	Description	description
	Email	mail
	Fax/Phone	facsimiletelephonenumber
	Given name	givenname
	Home phone	homephone
	Mobile phone	mobile
	Name	cn
	Pager phone	pager
	Password	(leave blank)
	Postal address	postaladdress

Table 34: LDAP advanced mapping values for use with Novell Directory Server objects (continued)

Mappings	LDAP property	LDAP value
	Product locale	Language
	Surname	sn
	Username	uid

These mapping properties represent changes that are based on a default Novell Directory Server installation. If you modify the schema, you might have to make more mapping changes.

LDAP attributes that are mapped to the **Name** property in **Folder mappings**, **Group mappings**, and **Account mappings** must be accessible to all authenticated users. In addition, the **Name** property must not be blank.

For users to successfully log in to the portal, they must have permission to read the ou and o attributes.

10. From the **File** menu, click **Save**.

Configuring an LDAP namespace for Oracle Directory Server

If you configure a new LDAP namespace for use with an Oracle Directory Server, default values are generated for you.

Procedure

1. In every location where you installed Content Manager, open IBM Cognos Configuration.
2. In the **Explorer** window, under **Security,** right-click **Authentication**, and then click **New resource** > **Namespace**.
3. In the **Name** box, type a name for your authentication namespace.
4. In the **Type** list, click **LDAP - Default values for Oracle Directory Server** and then click **OK**.

   The new authentication namespace resource appears in the **Explorer** window, under the **Authentication** component. Check them and make changes as needed.
5. In the **Properties** window, for the **Namespace ID** property, specify a unique identifier for the namespace.

   Tip: Do not use colons (:) in the Namespace ID property.
6. Specify the values for all other required properties to ensure that IBM Cognos can locate and use your existing authentication namespace.

   The following settings are examples:

   - For **User lookup**, enter `(uid=${userID})`
   - If you use single signon, for **Use external identity**, set the value to **True**.
   - If you use single signon, for **External identity mapping**, specify any attribute, such as the NT user domain ID or the user ID:

     `(ntuserdomainid=$environment("REMOTE_USER")})`

     `(uid=${environment("REMOTE_USER")})`

     Important: Ensure that you use only the variable REMOTE_USER. Using another variable can cause a security vulnerability.
   - For **Unique identifier**, type `nsuniqueid`
7. If you want the LDAP authentication provider to bind to the directory server by using a specific **Bind user DN and password** when you perform searches, then specify these values.

If no values are specified, the LDAP authentication provider binds as anonymous.

8. If you do not use external identity mapping, use bind credentials for searching the LDAP directory server by doing the following steps:
   - Ensure that **Use external identity** is set to **False**.
   - Set **Use bind credentials for search** to **True**.
   - Specify the user ID and password for **Bind user DN and password**.
9. From the **File** menu, click **Save**.

Making custom user properties for LDAP available to IBM Cognos components

You can use arbitrary user attributes from your LDAP authentication provider in IBM Cognos components. To configure this, you must add these attributes as custom properties for the LDAP namespace. The custom properties are available as session parameters through Framework Manager.

You can also use the custom properties inside command blocks to configure Oracle sessions and connections. You can use the command blocks with Oracle lightweight connections and virtual private databases. For more information, see the *IBM Cognos Analytics Administration and Security Guide*.

For more information about session parameters, see the *Framework Manager User Guide*.

Procedure

1. In each location where you installed Content Manager, open Cognos Configuration.
2. In the **Explorer** window, under **Security** > **Authentication**, and select the LDAP namespace.
3. In the **Properties** window, click in the **Value** column for **Custom properties**, and click the edit icon.
4. In the **Value - Custom properties** window, click **Add**.
5. Click the **Name** column, and type the name that you want IBM Cognos components to use for the session parameter.
6. Click the **Value** column, and type the name of the account parameter in your LDAP authentication provider.
7. Repeat the preceding two steps for each custom parameter.
8. Click **OK**.
9. From the **File** menu, click **Save**.

Enabling secure communication to the LDAP server

Secure LDAP protocol (LDAPS) encrypts the communication between the Access Manager component of Content Manager and the directory server. LDAPS prevents sensitive information in the directory server and the LDAP credentials from being sent as clear text.

To enable LDAPS, install a server certificate that is signed by a certificate authority in the directory server. Next, create a certificate database to contain the certificates. Finally, configure the directory server and the IBM Cognos LDAP namespace to use LDAPS.

The server certificate must be a copy of either

- The trusted root certificate and all other certificates that make up the chain of trust for the directory server certificate

  The trusted root certificate is the certificate of the root certificate authority that signed the directory server certificate.
- The directory server certificate only

The certificates must be Base64 encoded in ASCII (PEM) format. All certificates except the trusted root certificate must not be self-signed.

Before you begin

IBM Cognos works with both the `cert8.db` and `cert7.db` versions of the client certificate database. You must use the `certutil` tool from Netscape Security Services (NSS) to create the certificate databases. IBM Cognos does not accept other versions of `cert8.db` files, including those files from the `certutil` tool that is provided with Microsoft Active Directory. IBM Cognos now includes the `certutil` tool on platforms where Netscape Security Services (NSS) is not listed as a system requirement. For platforms where NSS is listed as a system requirement, please use that version of the `certutil` tool.

Procedure

1. Create a directory for the certificate database.
2. Create the certificate database by typing the following command:

   ```
   certutil -N -d certificate_directory
   ```

   Where *certificate_directory* is the directory that you created in step 1.

   This command creates a `cert8.db` file and a `key3.db` file in the new directory.
3. Add the certificate authority (CA) certificate or the directory server certificate to the certificate database by typing the appropriate command for the type of certificate:
   - For a CA certificate:

     ```
     certutil -A -n certificate_name -d certificate_directory -i CA.cert -t
     C,C,C
     ```
   - For a directory server certificate:

     ```
     certutil -A -n certificate_name -d certificate_directory -i
     server_certificate.cert -t P
     ```

   Where *certificate_name* is an alias that you assign, such as the CA name or host name; and *server_certificate* is the prefix of the directory server certificate file.
4. Copy the certificate database directory to the *install_location*/`configuration` directory on every location where Content Manager is installed.
5. Configure the directory server to use LDAPS and restart the directory server.

   For more information, see the documentation for the directory server.
6. In each Content Manager location where you configured the LDAP namespace to use the directory server, start IBM Cognos Configuration.
7. In the **Explorer** window, under **Security** > **Authentication**, click the LDAP namespace.
8. In the **Properties** window, for the **Host and port** property, change the port to the secure LDAPS port.

   For the **SSL certificate database** property, specify the path to the `cert7.db` file.
9. In the **Explorer** window, right-click the LDAP namespace and click **Test**.

   If the test fails, revise the properties, ensuring that the correct certificate is used.
10. From the **File** menu, click **Save**.
11. From the **Actions** menu, click **Restart**.
12. Repeat steps 6 - 11 on every other location where Content Manager is installed.

Enable single signon between LDAP and IBM Cognos components

You achieve single signon to IBM Cognos components by configuring the External Identity mapping property.

The External Identity mapping can refer to a CGI environment variable or an HTTP header variable. For an application server gateway or dispatcher entry that is pointing to IBM Cognos components, the External Identity mapping can refer to the `userPrincipalName` session variable. The resolved value of the External Identity mapping property at run time must be a valid user DN.

When an LDAP namespace is configured to use the External Identity mapping property for authentication, the LDAP provider binds to the directory server by using the Bind user DN and password or by using anonymous if no value is specified. All users who log on to IBM Cognos by using external identity mapping see the same users, groups, and folders as the Bind user.

If you want IBM Cognos components to work with applications that use Java or application server security, you can configure the External identity mapping property to obtain the user ID from the Java user principal. Include the token `${environment("USER_PRINCIPAL")}` in the value for the property. For more information, see the online help for IBM Cognos Configuration.

You can apply limited expression editing to the External Identity mapping property by using the replace operation.

Replace operation

The replace operation returns a copy of the string with all occurrences of the old substring that is replaced by the new substring.

The following rules apply:

- The character \ escapes the characters in the function parameters. Characters such as \ and " need escaping.
- Nested function calls are not supported.
- Special characters are not supported.

Syntax

```
${replace(str , old , new)}
```

Parameters for the Replace Operation

Table 35: Parameters and description for the Replace Operation

Parameter	Description
`str`	The string to search.
`old`	The substring to be replaced by the new substring.
`new`	The substring that replaces the old substring.

Examples

```
${replace(${environment("REMOTE_USER")},"NAMERICA\\",)}
```

```
${replace(${environment("REMOTE_USER")},"NAMERICA\\","")}
```

CA SiteMinder authentication provider

You can configure IBM Cognos Analytics to use a CA SiteMinder namespace as an authentication source.

The authentication provider uses the CA SiteMinder Software Development Kit to implement a custom agent. The custom agent deployment requires that you set the Agent Properties in the CA SiteMinder Policy server administration console to support 4.x agents.

CA SiteMinder configuration requirements

Configure the following items in the CA SiteMinder Policy Server:

- Cognos Analytics must allow certain special characters and character sequences in the Cognos Analytics Server 11.1.x URL. To avoid errors, remove the following character sequences from the list in the BadURLChars parameter of the Agent Configuration Object in CA SiteMinder Policy Server:
  - a tilde (~)
  - a period (.)
  - period and a forward slash (./)
  - forward slash and a period (/.)
  - greater-than sign (>)

  Tip: Customers who embed URLs in their reports should verify the characters passed in the URL parameters and ensure that CA SiteMinder does not treat these characters as BadURLChars or BadCSSChars. For more information, see the CA SiteMinder documentation.
- Cognos Analytics requires 4 verbs for its functionality. Enable the following values in the CA SiteMinder Policy Server: GET, POST, PUT, and DELETE.

CA SiteMinder configured for more than one user directory

If your CA SiteMinder environment is configured for more than one user directory, you must use the **SiteMinder** namespace type in IBM Cognos Configuration.

After you configure the SiteMinder namespace in IBM Cognos Configuration, you must also add a corresponding LDAP or Active Directory Server namespace to IBM Cognos Configuration for each user directory that is defined in CA SiteMinder.

When you configure a corresponding LDAP namespace, ensure that the **External identity mapping** property is enabled and that you include the REMOTE_USER token in property value. This does not mean that you must configure CA SiteMinder to set REMOTE_USER.

When you configure a corresponding Active Directory namespace, ensure that the singleSignonOption property is set to IdentityMapping.

The **SiteMinder** namespace passes user information internally to the corresponding LDAP namespace using the REMOTE_USER environment variable when it receives successful user identification from the CA SiteMinder environment.

For more information, see "Enabling single signon between Active Directory Server and IBM Cognos Components to use REMOTE_USER" on page 174.

Important: Ensure that you use only the variable REMOTE_USER. Using another variable can cause a security vulnerability.

CA SiteMinder configured with only one user directory

If your CA SiteMinder environment is configured with only one user directory, you do not have to use the **SiteMinder** namespace type in IBM Cognos Configuration.

In this case, you can use the user directory as your authentication source by configuring the appropriate namespace, or you can configure the **SiteMinder** with one user directory. For example, if the CA SiteMinder user directory is LDAP, you can configure IBM Cognos components with an LDAP namespace or with one **SiteMinder** namespace, referring to one user directory that is an LDAP namespace.

If the CA SiteMinder user directory is Active Directory, you can use an Active Directory namespace or an LDAP namespace that is configured for use with Active Directory.

If you want to use the user directory as your authentication source directly instead of configuring a **SiteMinder** namespace, you can configure the appropriate LDAP or Active Directory namespace. In this case, verify the Agent Configuration Object properties in CA SiteMinder Policy Server. Ensure that SetRemoteUser is activated.

When you configure the Active Directory namespace, ensure that the singleSignonOption property is set to IdentityMapping.

When you configure a corresponding LDAP namespace, ensure that the **External identity mapping** property is enabled and that you include the REMOTE_USER token in property value.

For more information, see "Enabling single signon between Active Directory Server and IBM Cognos Components to use REMOTE_USER" on page 174.

Important: Ensure that you use only the variable REMOTE_USER. Using another variable can cause a security vulnerability.

Configuring a SiteMinder namespace

If you configured CA SiteMinder for more than one user directory, you must use the **SiteMinder** namespace type in IBM Cognos Configuration. After you add the SiteMinder namespace, you must also add a corresponding LDAP namespace for each user directory in your CA SiteMinder environment.

You can also use the **SiteMinder** namespace type if users are stored in an LDAP server or an Active Directory server.

You can hide namespaces from users during login. You can have trusted signon namespaces without showing them on the namespace selection list that is presented when users login. For example, you want to integrate single sign-on across systems but maintain the ability for customers to authenticate directly to IBM Cognos without being prompted to choose a namespace.

Before you begin

To use the **SiteMinder** namespace, you must obtain the required CA SiteMinder library files, which are shown in the following table, and add the files to the appropriate library path for your operating system.

Table 36: CA SiteMinder library files

Operating system	CA SiteMinder library file
AIX	`libsmagentapi.so`
Microsoft Windows 64-bit	`smagentapi.dll` `smerrlog.dll`

Procedure

1. On the computer where you installed Content Manager, append the directory that contains the CA SiteMinder library file to the appropriate library path environment variable.
   - For AIX operating systems, LIBPATH
   - For Microsoft Windows operating systems, PATH
2. Open IBM Cognos Configuration.
3. In the **Explorer** window, under **Security,** right-click **Authentication**, and click **New resource** > **Namespace**.
4. In the **Name** box, type a name for your authentication namespace.
5. In the **Type** list, select the **SiteMinder** and then click **OK**.
6. Select the namespace that you added.
7. In the **Namespace ID** property, specify a unique identifier for the namespace.

   Tip: Do not use a colon (:) in the identifier.
8. Specify values for the other required properties.

   Tip: If you do not want the users to see the namespace name when they log in, set the **Selectable for authentication** property to **False**.
9. In the **Explorer** window, under **Security** > **Authentication**, right-click the namespace that you added, and click **New resource** > **SiteMinder Policy Server**.

10. In the **Name** box, type a name for the policy server and click **OK**.
11. In the **Properties** window, specify the **Host** property and any other property values you want to change.
12. In the **Explorer** window, right-click the new SiteMinder policy server that you added and click **New resource** > **User directory**.
13. In the **Name** box, type a name for the user directory and click **OK**.

    Important: The name must match the name of the user directory that is found in the policy server.
14. In the **Properties** window, type a value for the **Namespace ID reference** property.
15. Configure a user directory for each user directory in the SiteMinder policy server.
16. Click **File** > **Save**.
17. Test the connection to a new namespace. In the **Explorer** window, under **Authentication**, right-click the new authentication resource and click **Test**.

    You are prompted to enter credentials for a user in the namespace to complete the test.

    Depending on how your namespace is configured, you can enter either a valid user ID and password for a user in the namespace or the bind user DN and password.
18. Configure a corresponding LDAP or Active Directory namespace for each user directory.

    Ensure that you use the same value for the **Namespace ID** property that you use for the **Namespace ID** property for the SiteMinder namespace.

Configure IBM Cognos to use SAP

To use an SAP server as your authentication provider, you must use a supported version of SAP BW.

In SAP BW, you can assign users to user groups or roles or both. The SAP authentication provider uses only the roles.

The authorization rights required by the SAP user depend on who uses IBM Cognos components: users or administrators.

SAP Authorization Settings for IBM Cognos Users

The authorization objects in the following table are required for any IBM Cognos user.

Table 37: SAP authorization settings for IBM Cognos users

Authorization object	**Field**	**Value**
S_RFC Authorization check for RFC access	Activity	
	Name of RFC to be protected	RFC1 RS_UNIFICATION, SDTX, SH3A, SU_USER, SYST, SUSO
	Type of RFC to be protected	FUGR
S_USER_GRP User Master Maintenance: User Groups	Activity	03
	Name of user group	*

Some of the values shown, such as *, are default values that you may want to modify for your environment.

SAP Authorization Settings for IBM Cognos Administrators

If users perform administrative tasks and searches for users and roles, the values from the following table must be added to the S_RFC authorization object in addition to the values for IBM Cognos users.

Table 38: SAP authorization settings for IBM Cognos administrators

Authorization object	Field	Value
S_RFC Authorization check for RFC access	Activity	16
	RFC_NAME	PRGN_J2EE, SHSS, SOA3
	Type of RFC object to be protected	FUGR

Some of the values shown, such as *, are default values that you might want to modify for your environment.

Connectivity Between SAP BW and IBM Cognos on UNIX

To configure connectivity between SAP BW and IBM Cognos components on a UNIX operating system, ensure that you install the SAP shared library file (provided by SAP) and add it to the library path environment variable as follows:

- AIX

  ```
  LIBPATH=$LIBPATH:<librfc.a_directory>
  ```

Configure an SAP Namespace

You can configure IBM Cognos components to use an SAP server as the authentication source.

Before you begin

If you installed your IBM Cognos product on a 64-bit server, you must also manually copy the SAP RFC library files to the IBM Cognos installation directory.

Procedure

1. If running on a 64-bit server, do the following:
   - Go to the SAP installation directory on the 64-bit server.
   - Copy all 64-bit SAP RFC library files to `install_location\bin64`.
   - Copy all 32-bit SAP RFC library files to `install_location\bin`.
2. If running on a 32-bit server, copy all 32-bit SAP library files from the SAP installation directory to the `install_location\bin64` directory.
3. In the location where you installed Content Manager, open IBM Cognos Configuration.
4. In the **Explorer** window, under **Security**, right-click **Authentication**, and click **New resource** > **Namespace**.
5. In the **Name** box, type a name for your authentication namespace.
6. In the **Type** list, click **SAP** and then click **OK**.

The new authentication provider resource appears in the **Explorer** window, under the Authentication component.

7. In the **Properties** window, for the **Namespace ID** property, specify a unique identifier for the namespace.

   Important: Do not use colons (:) in the Namespace ID property.
8. Specify the values for all required properties to ensure that IBM Cognos components can locate and use your existing authentication provider.

   Depending on your environment, for the **Host** property, you may have to add the SAP router string to the SAP host name.
9. If the SAP system encodes the contents of cookies, enable the decode tickets feature:

   - In the **Properties** window, for **Advanced properties**, click the Value and then click the edit icon.
   - Click **Add**.
   - Enter the name `URLDecodeTickets` and enter the value `true`
   - Click **OK**.

   All SAP logon tickets will be decoded by the SAP namespace before establishing a connection.
10. From the **File** menu, click **Save**.
11. Test the connection to a new namespace. In the **Explorer** window, under **Authentication**, right-click the new authentication resource and click **Test**.

    You are prompted to enter credentials for a user in the namespace to complete the test.

    Depending on how your namespace is configured, you can enter either a valid user ID and password for a user in the namespace or the bind user DN and password.

Enable Single Signon Between SAP and IBM Cognos

You can enable single signon between SAP Enterprise Portal and IBM Cognos components as well as when using the external namespace function of the SAP BW data source connections.

To do so, ensure that you set the following system parameters on the SAP BW server:

- login/accept_sso2_ticket = 1
- login/create_sso2_ticket = 1
- login/ticket_expiration_time = 200

Delete an Authentication Provider

If they are no longer required, you can delete namespaces that you added, or unconfigure namespaces that IBM Cognos components detected.

You must not delete the Cognos namespace. It contains authentication data that pertains to all users and is required to save the configuration.

When you delete a namespace, you can no longer log on to the namespace. Security data for the namespace remains in Content Manager until you permanently delete it in the portal. For more information, see the *IBM Cognos Analytics Administration and Security Guide*.

Procedure

1. In each location where you installed Content Manager, open Cognos Configuration.
2. In the **Explorer** window, under **Security** > **Authentication**, right-click the namespace and click **Delete**.
3. Click **Yes** to confirm.

   The namespace disappears from the **Explorer** window and you can no longer log on to the namespace in that location.

4. From the **File** menu, click **Save**.
5. Repeat steps 1 to 4 for each location where you installed Content Manager.

   You must now log on to the portal and permanently delete the data for the namespace. For more information, see the *IBM Cognos Analytics Administration and Security Guide*.

Results

After you delete a namespace, it appears as Inactive in the portal.

Chapter 8. Performance Maintenance

This section includes topics about using IBM Cognos Analytics and other tools and metrics to maintain the performance of your IBM Cognos Analytics environment.

System Performance Metrics

IBM Cognos Analytics provides system metrics that you can use to monitor the health of the entire system and of each server, dispatcher, and service. You can also set the thresholds for the metric scores. Some examples of system performance metrics are the number of sessions in your system, how long a report is in a queue, how long a Java Virtual Machine (JVM) has been running, and the number of requests and processes in the system.

System performance metrics reside in the Java environment, but can be monitored in IBM Cognos Administration through the portal. For more information about monitoring system performance metrics, see the *IBM Cognos Analytics Administration and Security Guide*.

You can take a snapshot of the current system metrics so that you can track trends over time or review details about the state of the system at a particular time. For more information, see the topic about the metric dump file in the *IBM Cognos Analytics Troubleshooting Guide*.

You can also monitor system metrics externally to IBM Cognos Administration by using Java Management Extensions (JMX), a technology that supplies tools to manage and monitor applications and service-oriented networks.

Monitoring System Metrics Externally

You can monitor system metrics outside of IBM Cognos Administration by using industry standard Java Management Extensions (JMX). First, you configure two JMX properties in IBM Cognos Configuration to enable secure access to the metrics in the Java environment. Then you use a secure user ID and password to connect to the metrics through a JMX connection tool.

Before you begin

You must install Oracle Java SE Development Kit or the Java Software Development Kit from IBM before you can use the external monitoring feature.

Procedure

1. In the location where Content Manager is installed, start IBM Cognos Configuration.
2. In the **Explorer** window, click **Environment**.
3. In the **Properties** window, under **Dispatcher Settings**, click **External JMX port**.
4. In the **Value** column, type an available port number.
5. Click **External JMX credential**.
6. In the **Value** column, click the edit icon, type a user ID and password, and then click **OK**.

   The user ID and password ensure that only an authorized user can connect to the system metrics data in the Java environment, using the port specified in **External JMX port**.
7. Save the changes and restart the service.
8. To access the system metrics data, specify the following information in the JMX connection tool:
   - the URL to connect to the system metrics data

     For example,

     ```
     service:jmx:rmi://Content_Manager_server/jndi/rmi://
     monitoring_server:<JMXport>/proxyserver
     ```

where *JMXport* is the value that you typed for **External JMX port**, and *Content_Manager_server* and *monitoring_server* are machine names. Do not use localhost, even if connecting locally.

- the user ID and password to secure the connection

  Use the same values that you configured for **External JMX credential**.

Enabling Only Services That are Required

If some IBM Cognos Analytics services are not required in your environment, you can disable them to improve the performance of other services.

For example, to dedicate a computer to running and distributing reports, you can disable the presentation service on an Application Tier Components computer. When you disable the presentation service, the performance of the Application Tier Components will improve.

Note:

- The Presentation service must remain enabled on at least one computer in your IBM Cognos Analytics environment.
- If you want to use Query Studio, you must enable the Presentation service.
- If you want to use Analysis Studio, you must enable the Report service.
- If some IBM Cognos Analytics components are not installed on a computer, you should disable the services associated with the missing components. Otherwise the IBM Cognos Analytics components will randomly fail.

IBM Cognos services

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

Table 39: IBM Cognos services

Service	Purpose
Agent service	Runs agents. If the conditions for an agent are met when the agent runs, the agent service asks the monitor service to run the tasks.
Annotation service	Enables the addition of commentary to reports via the IBM Cognos Workspace. These comments persist across versions of the report.
Batch report service	Manages background requests to run reports and provides output on behalf of the monitor service.
Content Manager cache service	Enhances the overall system performance and Content Manager scalability by caching frequent query results in each dispatcher.
Content Manager service	• Performs object manipulation functions in the content store, such as add, query, update, delete, move, and copy • Performs content store management functions, such as import and export

Table 39: IBM Cognos services (continued)

Service	**Purpose**
Delivery service	Sends emails to an external SMTP server on behalf of other services, such as the report service, job service, or agent service
Event management service	Creates, schedules, and manages event objects that represent reports, jobs, agents, content store maintenance, and deployment imports and exports.
Graphics service	Produces graphics on behalf of the Report service. Graphics can be generated in 4 different formats: Raster, Vector, Microsoft Excel XML or PDF.
Human task service	Enables the creation and management of human tasks. A human task such as report approval can be assigned to individuals or groups on an ad hoc basis or by any of the other services.
Interactive Discovery Visualization service	Used by Cognos Workspace to provide visualization recommendations.
Job service	Runs jobs by signaling the monitor service to run job steps in the background. Steps include reports, other jobs, import, exports, and so on.
Log service	Records log messages generated by the dispatcher and other services. The log service can be configured to record log information in a file, a database, a remote log server, Windows Event Viewer, or a UNIX system log. The log information can then be analyzed by customers or by Cognos Software Services, including: • security events • system and application error information • selected diagnostic information
Metadata service	Provides support for data lineage information displayed in Cognos Viewer, Reporting, Query Studio, and Analysis Studio. Lineage information includes information such as data source and calculation expressions.
Migration service	Manages the migration from IBM Cognos Series 7 to IBM Cognos Analytics.

Table 39: IBM Cognos services (continued)

Service	Purpose
Mobile service	Manages activities related to IBM Cognos Mobile client: • Transforms reports and analyses for mobile consumption. • Compresses report and analysis content for fast distribution over-the-air to the mobile devices and access from those devices. • Pushes report and analysis content to the mobile devices. • Facilitates incoming and outgoing report-related and analysis-related requests between the mobile device and the environment to search, browse, or run reports. • Synchronizes the mobile content store on the server with the mobile database on the mobile device. • Translates Simple Object Access Protocol (SOAP) messages into wireless-friendly messages. • Communicates with the mobile device.
Monitor service	• Manages the monitoring and execution of tasks that are scheduled, submitted for execution at a later time, or run as a background task • Assigns a target service to handle a scheduled task. For example, the monitor service may ask the batch report service to run a report, the job service to run a job, or the agent service to run an agent. • Creates history objects within the content manager and manages failover and recovery for executing entries
PowerPlay service	Manages requests to run PowerPlay reports.
Presentation service	• Transforms generic XML responses from another service into output format, such as HTML or PDF • Provides display, navigation, and administration capabilities
Query service	Manages Dynamic Query requests and returns the result to the requesting batch or report service.
Relational metadata service	Used by Framework Manager and CubeDesigner to import metadata from relational databases. It may also be used by Dynamic Query Analyzer at runtime.

Table 39: IBM Cognos services (continued)

Service	**Purpose**
Report data service	Manages the transfer of report data between IBM Cognos Analytics and applications that consume the data, such as IBM Cognos for Microsoft Office and IBM Cognos Mobile.
Report service	Manages interactive requests to run reports and provides output for a user.
Repository service	Manages requests to retrieve archived report output from an archive repository or object store.

Tuning a IBM Db2 Content Store

If you use a 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 changing a Db2 content store, allocate sufficient log space to restructure the database.

To reconfigure 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.

Adjusting the memory resources for the IBM Cognos service

To improve performance in a distributed environment, you can change the amount of resources that the IBM Cognos service uses.

By default, the IBM Cognos service is configured to use minimal memory resources to optimize startup time.

The configuration settings for the IBM Cognos service apply only to the application server that IBM Cognos Analytics uses by default. If you want to configure IBM Cognos Analytics to run on another application server, do not use IBM Cognos Configuration to configure the resources. Instead, configure the resources within that application server environment.

The IBM Cognos service is available only on the computers where you installed Content Manager or the Application Tier Components.

Procedure

1. Start IBM Cognos Configuration.
2. In the **Explorer** window, expand **Environment** > **IBM Cognos services**, and then click **IBM Cognos**.
3. In the **Properties** window, change the value for **Maximum memory in MB**.
   - To reduce the startup time, memory footprint, and resources that are used, use the default setting of 4096.

- This value can be adjusted based on available system resources.

4. From the **File** menu, click **Save**.

Cognos Mobile performance

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

Estimate the bandwidth required by IBM Cognos Mobile

IBM Cognos Mobile sends compressed versions of reports from the server to the mobile device.

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

Other operations, such as browsing the content store and answering prompts in Cognos Workspace dashboards, also consume bandwidth. The bandwidth consumed is proportional to that used by a desktop browser performing the same action.

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

```
(number of users) x (average size of a report) x (number of number of scheduled reports sent to
each user per day)
```

Estimate the required number of servers

The load generated by one user using IBM Cognos Mobile on a server (dispatcher) is minimal if the users only consumes Active Reports. For users of Cognos Workspace dashboards, the app does not add any additional load to the servers compared to a desktop user.

Reduce Delivery Time for Reports in a Network

Reports that are distributed globally take longer to open in remote locations than to open locally. In addition, HTML reports take longer than PDF reports to open because more requests are processed for HTML reports.

You can reduce the amount of time for reports to open in remote locations in two ways. You can reduce the number of requests between the browser and the server by running the report in PDF format. If HTML reports are required, you can speed up the delivery of the report by configuring additional gateways in some of the remote locations. Static content, such as graphics and style sheets, will be delivered faster.

Increase Asynchronous Timeout in High User Load Environments

If you have a high user load (over 165 users) and interactive reports are running continuously in a distributed installation, you may want to increase the asynchronous timeout setting to avoid getting error messages. The default is 30000.

You may also want to set the Queue Time Limit setting to 360. For information, see the *IBM Cognos Analytics Administration and Security Guide*.

To resolve this problem, increase the wait timeout.

Procedure

1. Go to the following directory:

   *install_location*webapps/p2pd/WEB-INF/services/.
2. Open the reportservice.xml file in a text editor.

3. Change the async_wait_timeout_ms parameter to 120000.
4. Save the file.
5. Restart the service.

Chapter 9. Manually configuring IBM Cognos Analytics on UNIX and Linux operating systems

The console attached to the UNIX or Linux operating system computer on which you are installing IBM Cognos Analytics may not support a Java-based graphical user interface.

You must perform the following tasks manually:

__ • Change default configuration settings by editing the `cogstartup.xml` file, located in the *install_location*/`configuration` directory.

__ • Change language or currency support, or locale mapping by editing the `coglocale.xml` file, located in the *install_location*/`configuration` directory.

__ • Apply the configuration and the locale settings to your computer by running IBM Cognos Configuration in silent mode.

For all installations, some configuration tasks are required so that IBM Cognos Analytics works in your environment. If you distribute IBM Cognos Analytics components across several computers, the order in which you configure and start the computers is important.

Other configuration tasks are optional and depend on your reporting environment. You can change the default behavior of IBM Cognos Analytics by editing the `cogstartup.xml` file to change property values. You can also use sample files that enable IBM Cognos Analytics to use resources that already exist in your environment.

Manually change default configuration settings

If the console attached to your UNIX or Linux operating system computer does not support a Java-based graphical user interface, you must edit the `cogstartup.xml` to configure IBM Cognos Analytics to work in your environment.

Important: Some configuration settings are not saved in the `cogstartup.xml` file unless you use the graphical user interface. For example, the server time zone is not set for your IBM Cognos components when you modify the `cogstartup.xml` file directly and then run IBM Cognos Configuration in silent mode. In this case, other user settings that rely on the server time zone may not operate as expected.

If you want IBM Cognos Analytics to use a resource, such as an authentication provider that already exists in your environment, you can add a component to your configuration. You do this by copying the required XML code from the sample files into the `cogstartup.xml` file and then edit the values to suit your environment.

By default, the `cogstartup.xml` file is encoded using UTF-8. When you save the `cogstartup.xml` file, ensure that you change the encoding of your user locale to match the encoding used. The encoding of your user locale is set by your environment variables.

When you edit the `cogstartup.xml` file, remember that XML is case-sensitive. Case is important in all uses of text, including element and attribute labels, elements and values.

Before you edit the `cogstartup.xml` file, ensure that you

- make a backup copy
- create the content store on an available computer in your network
- review the configuration requirements for your installation type

Procedure

1. Go to the *install_location*/`configuration` directory.
2. Open the `cogstartup.xml` file in an editor.

3. Find the configuration setting you want to change by looking at the help and description comments that appear before the start tag of the `<crn:parameter>` elements.
4. Change the value of the `<crn:value>` element to suit your environment.

   Tip: Use the `type` attribute to help you determine the data type for the configuration property.
5. Repeat steps 3 to 4 until the configuration values are appropriate your environment.
6. Save and close the file.

Results

You should now use a validating XML editor to validate your changes against the rules in the `cogstartup.xsd` file, located in the *install_location*/`configuration`.

Adding a component to your configuration

The `cogstartup.xml` file contains configuration settings used by IBM Cognos Analytics and by default components. You can change the components that IBM Cognos Analytics uses by copying XML elements from sample files into the `cogstartup.xml` file. You can then edit the configuration values to suit your environment.

For example, to use an Oracle database for the content store, you can use the `ContentManager_`*language code*`.xml` sample file to replace the default database connection information.

IBM Cognos Analytics can use only one instance at a time of the following elements:

- The database for the content store
- A cryptographic provider
- A configuration template for the IBM Cognos service

You should be familiar with the structure of XML files before you start editing them.

Procedure

1. Go to the *install_location*/`configuration/samples` directory.
2. Choose a sample file to open in an editor:
   - To use Oracle, or IBM Db2 for the content store, open the `ContentManager_`*language_code*`.xml` file.
   - To use an authentication provider, open the `Authentication_`*language_code*`.xml` file.
   - To use a cryptographic provider, open the `Cryptography_`*language_code*`.xml` file.
   - To send log messages somewhere other than a file, open the `Logging_`*language_code*`.xml` file.
   - To use a medium or large template for the amount of resources the IBM Cognos Analytics process uses, open the `CognosService_`*language_code*`.xml` file.
3. Copy the elements that you need.

   Tip: Ensure that you copy the code including the start and end tags for the `<crn:instance>`element.

   For example, look for the `(Begin of)` and `(End of)` comments:

   ```
   <!--
   (Begin of) Db2 template
   -->
   <crn:instance ...>
   ...
   </crn:instance>
   <!--
   End of) Db2 template
   -->
   ```
4. Go to the *install_location*/`configuration` directory.

5. Open the `cogstartup.xml` file in an editor.
6. Paste the code from the sample file to the `cogstartup.xml` file and replace the appropriate `<crn:instance>` element.
7. Change the values of these new elements to suit your environment.

   For the `<crn:instance>` element, do not change the class attribute. You can change the name attribute to suit your environment.

   For example, if you use an Oracle database for the content store, change only the name attribute to suit your environment.

   ```
   <crn:instance class="Oracle" name="MyContentStore">
   ```
8. Save and close the file.
9. Run IBM Cognos Configuration in silent mode by typing the following command:

   ```
   ./cogconfig.sh -s
   ```

   This ensures that the file is valid and that passwords are encrypted.

Changing manually encrypted settings

You can manually change encrypted settings, such as passwords and user credentials, in the `cogstartup.xml` file.

To prompt IBM Cognos Configuration to save an encrypted setting, you change the value and then set the encryption flag to false.

Procedure

1. Go to the *`install_location`*`/configuration` directory.
2. Open the `cogstartup.xml` file in an editor.
3. Find the encrypted setting you want to change by looking at the help and description comments that appear before the start tag of the `<crn:parameter>` elements.
4. Change the value of the `<crn:value>` element to suit your environment.

   Tip: Use the type attribute to help you determine the data type for the configuration property.
5. Change the encryption value to false.

   For example,

   ```
   <crn:value encrypted="false">
   ```
6. Repeat steps 3 to 5 until the configuration values are appropriate for your environment.
7. Save and close the file.
8. Type the following configuration command:

   ```
   ./cogconfig.sh -s
   ```

Results

The new settings are saved and encrypted.

Global settings on UNIX and Linux operating systems

If the console attached to your UNIX or Linux operating system computer does not support a Java-based graphical user interface, you must manually edit the `coglocale.xml` file.

You can change global settings

- to specify the language used in the user interface when the language in the user's locale is not available
- to specify the locale used in reports when the user's locale is not available

- to add currency or locale support to report data and metadata
- to add language support to the user interface

By default, IBM Cognos Analytics components ensure that all locales, which may come from different sources and in various formats, use a normalized form. That means that all expanded locales conform to a language and regional code setting.

Before you can add language support to the user interface, you must install the language files on all computers in your distributed installation. For more information, contact your support representative.

Example 1

A report is available in Content Manager in two locales, such as en-us (English-United States) and fr-fr (French-France), but the user locale is set to fr-ca (French-Canadian). IBM Cognos uses the locale mapping to determine which report the user sees.

First, IBM Cognos checks to see if the report is available in Content Manager in the user's locale. If it is not available in the user's locale, IBM Cognos maps the user's locale to a normalized locale configured on the Content Locale Mapping tab. Because the user's locale is fr-ca, it is mapped to fr. IBM Cognos uses the mapped value to see if the report is available in fr. In this case, the report is available in en-us and fr-fr, not fr.

Next, IBM Cognos maps each of the available reports to a normalized locale. Therefore, en-us becomes en and fr-fr becomes fr.

Because both report and the user locale maps to fr, the user having the user locale fr-ca will see the report saved with the locale fr-fr.

Example 2

The user's locale and the report locales all map to the same language. IBM Cognos chooses which locale to use. For example, if a user's locale is en-ca (English-Canada) and the reports are available in en-us (English-United States) and en-gb (English-United Kingdom), IBM Cognos maps each locale to en. The user will see the report in the locale setting that IBM Cognos chooses.

Example 3

The report and the user locales do not map to a common language. IBM Cognos chooses the language. In this case, you may want to configure a mapping. For example, if a report is available in en-us (English-United States) and fr-fr (French-France), but the user locale is es-es (Spanish-Spain), IBM Cognos chooses the language.

Changing manually the global settings on UNIX and Linux operating systems

Use the following steps to change global settings on UNIX and Linux operating systems using the `coglocale` file.

Procedure

1. On every computer where you installed Content Manager, go to the *`install_location`*`/configuration` directory.
2. Open the `coglocale.xml` file in an editor.
3. Add or modify the required element and attribute between the appropriate start and end tags.

   The elements, attributes, and start and end tags are listed in the following table.

Table 40: Tags for global settings

Type of element	Start tag	End tag
Language	<supportedProductLocales>	</supportedProductLocales>

Table 40: Tags for global settings (continued)

Type of element	Start tag	End tag
Content Locales	<supportedContentLocales>	</supportedContentLocales>
Currency	<supportedCurrencies>	</supportedCurrencies>
Product Locale Mapping	<productLocaleMap>	</productLocaleMap>
Content Locale Mapping	<contentLocaleMap>	</contentLocaleMap>
Fonts	<supportedFonts>	</supportedFonts>
Cookie settings, archive location for reports	<parameter name="*setting*">	</parameter>

Tip: To remove support, delete the element.

4. Save and close the file.

Results

Tip: Use a validating XML editor to validate your changes against the rules in the `cogstartup.xsd` file, located in the *install_location*/`configuration`.

If you add a currency code that is not supported, you must manually add it to the `i18n_res.xml` file in the *install_location*/`bin/` directory. Copy this file to each IBM Cognos computer in your installation.

Starting and stopping Cognos Analytics in silent mode on UNIX and Linux operating systems

You run IBM Cognos Configuration in silent mode to apply the configuration settings and start the services on UNIX or Linux operating system computers that do not support a Java-based graphical user interface.

Before you run the configuration tool in silent mode, you should ensure the `cogstartup.xml` file is valid according to the rules defined in the `cogstartup.xsd` file. The `cogstartup.xsd` file is located in the *install_location*/`configuration` directory.

Starting Cognos Analytics in silent mode on UNIX and Linux operating systems

Use the following steps to start the IBM Cognos Analytics software in silent mode.

Procedure

1. Ensure that the `cogstartup.xml` file, located in the *install_location*/`configuration` directory, has been modified for your environment.

   For more information, see "Manually change default configuration settings" on page 205.
2. Go to the *install_location*/`bin64` directory.
3. Type the following command

   ```
   ./cogconfig.sh -s
   ```

   Tip: To view log messages that were generated during an unattended configuration, see the `cogconfig_response.csv` file in the *install_location*/`logs` directory.

Results

IBM Cognos Configuration applies the configuration settings specified in the `cogstartup.xml` file, encrypts credentials, generates digital certificates, and if applicable, starts the Cognos service or process.

Stopping Cognos Analytics in silent mode on UNIX and Linux operating systems

Use the following steps to stop the IBM Cognos Analytics software in silent mode.

Procedure

1. Go to the *`install_location`*`/bin64` directory.
2. Type the following command

   ```
   ./cogconfig.sh -stop
   ```

Chapter 10. Uninstalling IBM Cognos Analytics

It is important to use uninstall programs to completely remove all files and modifications to system files. To uninstall IBM Cognos Analytics, you uninstall server components and modeling tools.

If you are running IBM Cognos Analytics in an application server environment, use the administration tool provided with the application server to stop the application if it is running and undeploy the Java portion of IBM Cognos Analytics components. Many application servers do not completely remove all deployed application files or directories during an undeployment; therefore, you may have to perform this action manually. After you have undeployed IBM Cognos Analytics components, complete the steps in this section to uninstall on UNIX and Microsoft Windows operating systems.

Tip: If monitoring tools such as Process explorer, MMC (Microsoft Management Console) are running during the uninstall, they will interfere with the deletion of the services. This applies to all services in general. For example, after uninstalling Cognos Analytics, product services such as ApacheDS, IBM Cognos, and Informix will not be fully removed, but instead they will show in the services panel as stopped and disabled. To avoid this, do not have any monitoring tools running while running the uninstall. Shutting down these monitoring tools after the uninstall will also complete the removal of the services.

Important: Do not delete the configuration and data files if you are upgrading to a new version of IBM Cognos Analytics and you want to use the configuration data with the new version.

Important: The Application and associated services must be stopped for the uninstall process to complete. Note that stopping of the services can take up to 15 minutes to complete.

Uninstall IBM Cognos Analytics on UNIX or Linux operating systems

If you no longer require IBM Cognos Analytics or if you are upgrading on your UNIX or Linux operating system, uninstall IBM Cognos Analytics.

Uninstalling does not remove any files that changed since the installation, such as configuration and user data files. Your installation location remains on your computer, and you retain these files until you delete them manually.

Procedure

1. If the console attached to your computer does not support a Java-based graphical user interface, determine the process identification (pid) of the IBM Cognos Analytics process by typing the following command:

   ```
   ps -ef | grep cogbootstrapservice
   ```

2. Stop the IBM Cognos Analytics process:

   - If you run XWindows, start IBM Cognos Configuration, and from the **Actions** menu, click **Stop**.
   - If you do not run XWindows, type:

     ```
     kill -TERM pid
     ```

3. To uninstall IBM Cognos Analytics, go to the *install_location* directory and type the appropriate command:

   - If you use XWindows, type

     ```
     ./uninst -u
     ```

   - If you do not use XWindows, do an unattended uninstallation (see Use an unattended installation).

4. Follow the prompts to complete the uninstallation.
5. Delete all temporary Internet files from the Web browser computers.

Uninstall IBM Cognos Analytics on Microsoft Windows operating systems

If you no longer require IBM Cognos Analytics or if you are upgrading, uninstall all IBM Cognos Analytics components and the IBM Cognos service.

If you installed more than one component in the same location, you can choose the packages to uninstall using the uninstall wizard. All components of the package will be uninstalled. You must repeat the uninstallation process on each computer that contains IBM Cognos Analytics components.

It is not necessary to back up the configuration and data files on a Microsoft Windows operating system. These files are preserved during the uninstallation.

Close all programs before you uninstall IBM Cognos Analytics. Otherwise, some files may not be removed.

Uninstalling does not remove any files that changed since the installation, such as configuration and user data files. Your installation location remains on your computer, and you retain these files until you delete them. Do not delete the configuration and data files if you are upgrading to a new version of IBM Cognos Analytics and you want to use the configuration data with the new version.

Procedure

1. From the **Start** menu, click **All Programs** > **IBM Cognos Analytics** > **Uninstall IBM Cognos Analytics**.

   The **Uninstall** wizard appears.

   Tip: IBM Cognos Analytics is the default name of the Program Folder that is created during the installation. If you chose another name, go to that folder to find the program.
2. Follow the instructions to uninstall the components.

   The `cognos_uninst_log.htm` file records the activities that the Uninstall wizard performs while uninstalling files.

   Tip: To find the log file, look in the Temp directory.
3. Delete all temporary Internet files from the Web browser computers.

   For more information, see your Web browser documentation.

Recovering from an unsuccessful uninstall

If an uninstall is unsuccessful, files, registry entries, and services may remain that should have been deleted. This topic provides guidelines for both Easy and Custom installations.

Procedure

1. For an Easy, first install:

   a) Remove Informix by executing the Informix uninstall command:

   ```
   install_location\informix\bin\ifxdeploy.exe -u install_location\informix -delifx
   ```

   a) Remove the following registry key: `HKEY_LOCAL_MACHINE\SOFTWARE\Informix\Online\ol_cognoscm`

   b) Remove the installation folder *`install_location`*

   c) If this is the only InstallAnywhere-based install on your machine, you can remove the InstallAnywhere registry file: `%PROGRAM FILES%\Zero G Registry\.com.zerog.registry.xml`
2. For all other installations:

   a) Remove the installation folder *`install_location`*

   b) If this is the only InstallAnywhere-based install on your machine, you can remove the InstallAnywhere registry file :

On Windows (hidden directory): `%PROGRAM FILES%\Zero G Registry\.com.zerog.registry.xml`

On UNIX: registry file: `.com.zerog.registry.xml` located:

- If logged in as root, the global registry is located in `/var`
- If logged in as a user, it is located in the user's home directory.

If you are not sure about the status of InstallAnywhere installations, you can simply rename this file in order to keep a copy of it.

Chapter 11. IBM Cognos content archival

Storing archived content in your external repository provides you with the ability to adhere to regulatory compliance requirements, and can enhance the scalability and performance of IBM Cognos products by reducing the size of content in the content store.

The software supports an IBM FileNet® Content Manager with IBM FileNet CMIS external repository. If you already have IBM Filenet CMIS version 1 of the software installed, you must upgrade this software with fix pack, version 2. Content archival can also be configured to use your file system.

Administrators create a data source connection to an external repository to allow content to move from the content store to the repository. Users can then view the archived content in the external repository. By providing search results for recent and archived content, users can make critical comparisons between current data and historical data. This efficient mechanism allows your company to meet corporate and government requirements while providing a seamless user experience.

The content archived in the external repository is not managed in IBM Cognos environment. For example, if you delete reports in IBM Cognos Analytics, the archived outputs are not deleted in your external repository.

For information about administering your archives, see the *IBM Cognos Analytics Administration and Security Guide*.

There are two workflow scenarios for archiving your content. The first workflow allows administrators archive packages and folders after installing IBM Cognos Content Archival software. The second workflow allows administrators to create repository connections for new packages and folders.

Workflow 1: Archiving content after installing connectivity software

Administrators can archive saved report output for specific packages and folders or all packages and folders after installing or upgrading IBM Cognos Analytics. This workflow only needs to be completed once since all of your content is currently located in your content store.

- Create a data source connection to the external repository.
- Select repository connections for the packages and folders that need to be archived.
- Create and run a content archival maintenance task to select folders and packages to archive in the external repository.

Once you set a repository connection for packages and folders, any new report output is automatically archived, which means that there is no need to run the content archival maintenance task again.

Workflow 2: Creating repository connections for new packages and folders

Administrators can create repository connections for new packages and folders by completing these tasks:

- Create a data source connection to the external repository.
- Select repository connections for the packages and folders that need to be archived.

Using content archival content maintenance tasks

The content archival content maintenance task creates a reference to the report versions in the folders and packages that you select and configure. Selecting folders and packages marks the content within and allows it to remain in the content store until it is archived in your external repository.

It is important to note that this task does not move your content from the content store to the external repository. You must select repository connections for your packages and folders first. Report versions in folders and packages that are not marked for archiving are available for deletion from the content store.

Once the content is marked, the content archival task is complete. A background task in Content Manager finds the marked items and then copies and saves them in the external repository.

Importing content into a folder or package that is configured for archiving to an external repository does not automatically move and archive the imported content into the repository. An administrator must run a content archival content maintenance task for this folder or package to archive the imported content.

Background tasks

The background XML tasks used to move content from the content store to the external repository are archiveTask.xml and deleteTask.xml. The archiveTask.xml file moves marked content to an external repository. You can also use this file to set thread execution times and archive outputs of selected formats. The deleteTask.xml file is a configuration file that retrieves and deletes marked version objects from the queue. You should not modify this file.

Preserve content IDs before you archive

If required, you can preserve content IDs before report output is archived.

Objects in the content store have content IDs that are deleted and replaced with new IDs by default when you run an import deployment and move content to a target environment. However, there may be situations when you must preserve content IDs, for example, when moving report output to a external report repository.

Configure content archival

You must configure your environment for content archival. For the configuration changes to take effect you must stop and start your IBM Cognos services.

Creating a file location for a file system repository

To archive reports or report specifications to an IBM Cognos content archival file system repository, you must create an alias root that points to a file location on a local drive or network share.

Before you begin

You must be an administrator and have access to the file location. Content Manager and Application Tier Components must be able to access this location by using a file URI.

Procedure

1. If running, stop the IBM Cognos service.
2. Start IBM Cognos Configuration.
3. Click **Actions** > **Edit Global Configuration.**
4. On the **General** tab, select **Alias Roots**, click inside the value field, click the edit button, and when the **Value - Alias Roots** dialog box appears, click **Add**.
5. In the **Alias root name** column, type a unique name for your file system repository.

   Note: There is no limit to the number of aliases you can create.
6. Type the path to your file system location, where file-system-path is the full path to an existing file location:

   - On Windows, in the **windowsURI** column, type `file:///` followed by the local path, for example, `file:///c:/file-system-path` or type `file://` followed by the server name and share path, for example `file://server/share`.
   - On UNIX or Linux, in the **unixURI** column, type `file:///` followed by the local path, for example, `file:///file-system-path`.

   Note: Relative paths, such as `file:///../file-system-path`, are not supported.

In a distributed installation, both the Content Manager and Application Tier Components computers must have access to the file location. Use both URIs only in a distributed installation. The UNIX URI and the Windows URI in an alias root must point to the same location on the file system.

7. Click **OK**.
8. Restart the IBM Cognos service. This might take a few minutes.

Results

Use this file system repository name to create a data source connection to use with the Cognos content archival software. For more information, see the *IBM Cognos Administration and Security Guide.*

Importing custom classes definitions and properties into IBM FileNet Content Manager

To use IBM Cognos content archival, you must import a set of custom classes and properties files into IBM FileNet Content Manager.

Custom classes definitions and properties include FileNet specific metadata. You can install custom classes and properties files at any time.

Procedure

1. If you have FileNet archiving set up, go to `*install_location*/configuration/repository/filenet/upgrade/`directory.
2. If FileNet archiving is not already set up, go to `*install_location*/configuration/repository/filenet/new/` directory.
3. Copy the `CMECMIntegrationObjects_CEExport._xxx.xml` files to a local folder on the FileNet server.
4. Open the FileNet Enterprise Manager Administration tool and connect to the domain for the FileNet external repository.
5. Select a target Object Store, and click **Import All Items** to import the definitions into the object store.
6. In the Import Options pane, click **Import Manifest File** and browse to where the `CMECMIntegrationObjects_CEExport._xxx.xml` files are located.
7. Select the `CMECMIntegrationObjects_CEExport_Manifest.xml` file and click **Import**.
8. Restart the FileNet Content Engine and FileNet CMIS application to apply the changes to your environment.

   Note: It might take a long time for changes to be updated across all FileNet nodes.

Importing custom classes definitions and properties into IBM Content Manager 8

To use IBM Cognos content archival with IBM Content Manager 8, you must import a set of custom classes and properties files. You must also update the CMIS configuration file with the IBM Cognos folder types.

Custom classes definitions and properties include IBM Content Manager 8 specific metadata. You can install custom classes and properties files at any time.

As there is no Resource Manager that is defined during the installation process, there are conflict error messages during the import process.

Before you begin

You must have IBM Content Manager 8 installed with an IBM Content Manager 8 CMIS version 1.1 external repository.

Procedure

1. Open the Content Manager 8 **System Administration Client**.
2. From the main menu, click **Tools** > **Import XML**.

3. From the **Import XML Options** window, **File to import** section:

   - In the **Data model file** field, click **Browse**, and select the `CMECMIntegrationTypes_RMImport_Manifest.xsd` file from which you want to import the objects.
   - In the **Administrative objects file** field, click **Browse**, and select the `CMECMIntegrationTypes_RMImport_MimeTypes.xml` file to import the Administrative objects file.

   The default location is `*install_location*/configuration/repository/contentManager8/New` directory.
4. To view conflicts, from the **Import XML Options** window, under **Processing options**, select **Process interactively**.
5. Click **Import** to begin the import process.

   a) From the **Import Preprocessor Results** window, expand **Item Types**, and double-click an item type that indicates a conflict.

   b) From the **Details of Import Definition and Target Definition** window, in the **Resulting Target** column, select the names for the **Resource Manager** and **Collection** created when you installed Content Manager 8, and click **Accept**.

   c) Repeat steps a and b for each item type that indicates a conflict.
6. After you resolve all the conflicts, from the **Import Preprocessor Results** window, click **Continue**.
7. From the **Confirm Import Selection** window, click **Import**.
8. After the import is complete, click **OK**.
9. To update the CMIS configuration file to detect the IBM Cognos folder types, run the CMIS for Content Manager 8 configuration program to create a profile.
10. Open the `cmpathservice.properties` file in the IBM CMIS for Content Manager configuration profiles folder.

    For UNIX, the default file path is: `/opt/IBM/CM_CMIS/profiles/profile1`

    For Windows, the default file path is: `C:\Program Files\IBM\CM_CMIS\profiles\profile1`

    a) Locate the `folderTypes` line.

    b) Add the IBM Cognos folders types COGNOSREPORT and REPORTVERSION in uppercase. Separate each folder type by a comma.

    ```
    For example,
    folderTypes = ClbFolder,COGNOSSREPORT,REPORTVERSION
    ```

    c) Save and close the file.
11. Run the CMIS for Content Manager 8 configuration program and select the option to redeploy the CMIS configuration file automatically.

    Note: For more information about manually deploying CMIS, see Manually deploying IBM CMIS for Content Manager (http://pic.dhe.ibm.com/infocenter/cmgmt/v8r4m0/topic/com.ibm.installingcmcmis.doc/cmsde001.htm).
12. From the WebSphere Application Server Liberty Profile administrative console, restart the **CMIS for Content Manager Application**.

Specifying an available time to run the archival process

To maintain high system performance during peak hours, you can configure a blackout period to specify when the archive or delete tasks run.

A blackout period is a temporary period in which the movement of data is denied. By default, a blackout period is not defined when the software is installed.

Procedure

1. Go to the *install_location*/webapps/p2pd/WEB-INF/cm/tasks/manager directory.
2. Using an XML text editor, open the tasksManager.xml file.
3. For example, to specify a weekly blackout period from 8.00 a.m. to 5 p.m., Tuesday through Friday, add the following <blackoutPeriods> element as a child element of the backgroundTasksManager element.

   - start time = <hour>08</hour>
   - stop time = <hour>17</hour>
   - days =

   ```
                   <day>Tuesday</day>
                   <day>Wednesday</day>
                   <day>Thursday</day>
                   <day>Friday</day>
   ```

4. If required, decrease the number of threads available to the archiving and deletion processes. The maximum number of threads is 7.
5. Save and close the file.
6. Restart background activities on the Content Manager service.

Specifying thread execution time

You can use threads to schedule operating system processing time.

The archive and delete background tasks use threads to move content. Threads are units of processing time that are scheduled by the operating system.

Procedure

1. Go to the *install_location*/webapps/p2pd/WEB-INF/cm/tasks/config directory.
2. Using an XML text editor, open the archiveTask.xml file.
3. For example, to configure three threads that execute from midnight to 8.00 a.m., one thread that executes from 8.00 a.m. to 5.00 p.m., no threads that execute from 5.00 p.m. to midnight, and all threads that run every day of the week, add the following <executionPeriods> XML element as a child element of the backgroundTask element.

   ```
               <executionPeriods>
           <executionPeriod>
               <threads>3</threads>
               <startTime>
                   <hour>00</hour>
                   <minute>00</minute>
               </startTime>
               <stopTime>
                   <hour>08</hour>
                   <minute>00</minute>
               </stopTime>
               <days>
                   <day>Monday</day>
                   <day>Tuesday</day>
                   <day>Wednesday</day>
                   <day>Thursday</day>
                   <day>Friday</day>
                   <day>Saturday</day>
                   <day>Sunday</day>
               </days>
           </executionPeriod>
           <executionPeriod>
               <startTime>
                   <hour>08</hour>
                   <minute>00</minute>
               </startTime>
               <stopTime>
                   <hour>17</hour>
                   <minute>00</minute>
               </stopTime>
   ```

```
            <days>
                <day>Monday</day>
                <day>Tuesday</day>
                <day>Wednesday</day>
                <day>Thursday</day>
                <day>Friday</day>
                <day>Saturday</day>
                <day>Sunday</day>
            </days>
        </executionPeriod>
    </executionPeriods>
```

4. Save and close the file.

Archiving selected formats of report outputs

You can limit archiving to limit archiving to specific output formats. By default outputs of any given format, including PDF, XML, HTML and Excel, are archived.

You can limit archiving of specific output formats to the repository.

Procedure

1. Go to the *`install_location`*`/webapps/p2pd/WEB-INF/cm/tasks/config` directory.
2. Using an XML text editor, open the `archiveTask.xml` file.
3. For example, to define the archiving of only PDF report output versions, add the following `<outputFormats>` XML element as a child element of the `runOptions` XML element.

   ```
   <outputFormats>
               <outputFormat>PDF</outputFormat>
           </outputFormats>
   ```

   You can use the existing sample `outputFormats` element and modify the list to specify output formats to be archived.

   You cannot selectively archive multiple file report output versions, for example HTML with graphics.

   Save and close the file.

Specifying that report specifications are not archived

By default, report specification output is archived. Report specifications describe how data was generated within a report.

To turn off the archiving of report specifications, you must modify two files: `CM.xml`, and either `CM_FILENET.xml` or `CM_CM8.xml`, depending on whether you archive your content to an IBM FileNet Content Manager repository or an IBM Content Manager 8 repository.

Procedure

1. Go to the *`install_location`*`/webapps/p2pd/WEB-INF/repositories/config` directory.
2. Using an XML text editor, open the `CM.xml` file.
3. Comment out or remove the following line: `<property name="specifications" metadataPropertyName="specification" useTempFile="true"`
4. Save and close the file.
5. Go to the *`install_location`*`/webapps/p2pd/WEB-INF/repositories/config` directory.
6. Do one of the following steps:
   - If you archive your content to FileNet, open the file named `CM.FILENET.xml` in a text editor.
   - If you archive your content to IBM Content Manager 8, open the file named `CM.xml` in a text editor.
7. Comment out or remove the following element:

   ```
   <property repositoryName="REPORTEXECUTIONSPECIFICATION"
   repositoryType="ASSOCIATED"
   metadataPropertyName="specification">
   ```

```
                                <associatedObjectTypes>
                                     <objectType name="VERSIONSPECIFICATION">
                                         <properties>
                                            <property repositoryName="cmis:name"
repositoryType="STRING"
metadataPropertyName="reportVersionDefaultName"  valueHandler="com.cognos.cm.
repositoryPluginFramework.
PropertyValueAppendStringHandler" valueHandlerArgument="_specification"/>
                                        </properties>
                                    </objectType>
                                </associatedObjectTypes>
                            </property>
```

Note: In the `CM.xml` file, the `objectType` name value is `<objectType name="$t!-2_VERSIONSPECIFICATIONv-1">`.

8. Restart background activities on the Content Manager service. For more information, see the *IBM Cognos Analytics Administration and Security Guide*.

Appendix A. IBM Cognos Configuration command-line options

Use command-line options with the configuration command to modify the behavior of IBM Cognos Configuration when it starts.

Table 41: Command line options and descriptions

Option	Descriptions
`-h`	Displays commands for IBM Cognos Configuration.

`-s`	Runs IBM Cognos Configuration in silent mode.
	Uses property values specified in the `cogstartup.xml` file to configure installed components and then starts all services.
	`./cogconfig.sh -s`
	`cogconfig.bat -s`

`-stop`	Stops all IBM Cognos services.
	`./cogconfig.sh -stop`
	`cogconfig.bat -stop`

`-startupfile` *`path/filename.xml`*	Runs IBM Cognos Configuration using a file other than the `cogstartup.xml` file in the *`install_location`*`/configuration` directory.

`-test`	Uses property values specified in the `cogstartup.xml` file to test configuration settings.
	`./cogconfig.sh -test`
	`cogconfig.bat -test`

`-notest`	Starts IBM Cognos Configuration with the automatic testing tasks disabled.
	`./cogconfig.sh -notest`
	`cogconfig.bat -notest`
	This option should not be used for the first time you start the product or if you are making configuration changes.

`-utf8`	Saves the configuration in UTF-8 encoding.
	`./cogconfig.sh -s -utf8`
	`cogconfig.bat -s -utf8`

Table 41: Command line options and descriptions (continued)

Option	**Descriptions**

`-l` *`language ID`*	Runs IBM Cognos Configuration using the language specified by the language identifier.
	To run the configuration tool in silent mode using Simplified Chinese
	`./cogconfig.sh -l zh-cn`
	`cogconfig.bat -l zh-cn`

`-e` *`filename.xml`*	Exports the current configuration settings to the specified file.
	`./cogconfig.sh -e` *`filename`*`.xml`
	`cogconfig.bat -e` *`filename`*`.xml`

`-log`	Creates a `cogconfig.`*`timestamp`*`.log` error log file in the *`cognos_location`*`/logs` directory.
	`./cogconfig.sh -log`
	`cogconfig.bat -log`

`-java:{local|env}`	Runs IBM Cognos Configuration on Microsoft Windows operating systems using the Java Runtime Environment version that is defined as either
	• `env`: environmentally using the JAVA_HOME environment variable
	• `local`: locally from the *`install_location`*`/bin/jre` directory
	If you do not set this flag, IBM Cognos uses the JAVA_HOME environment variable setting.
	To run IBM Cognos Configuration in silent mode, using the local JVM, type the following command:
	`./cogconfig.sh -s -java:local`
	`cogconfig.bat -s -java:local`

You can use more than one command-line option at a time. For example, you can run IBM Cognos Configuration in silent mode and send all error messages to a log file.

Appendix B. Troubleshooting

Use this troubleshooting reference information and these solutions as a resource to help you solve specific problems you may encounter during or after the installation of IBM Cognos Business Intelligence components.

Problems are characterized by their symptoms. Each symptom can be traced to one or more causes by using specific troubleshooting tools and techniques. After being identified, each problem can be fixed by implementing a series of actions.

When you are troubleshooting, log files can help you. Another valuable troubleshooting tool is the Support Community, which is available on the IBM Support Portal (Opens in new window). The Support Community can help with solutions to problems for all IBM Cognos products.

When you cannot resolve a problem, the final resource is your technical support representative. To analyze a problem, your technical support representative requires information about the situation and the symptoms that you are experiencing. To help isolate the problem, collect the necessary data before you contact your representative.

Troubleshooting a problem

Troubleshooting is a systematic approach to solving a problem. The goal of troubleshooting is to determine why something does not work as expected and how to resolve the problem.

The first step in the troubleshooting process is to describe the problem completely. Problem descriptions help you and the IBM technical-support representative know where to start to find the cause of the problem. This step includes asking yourself basic questions:

- What are the symptoms of the problem?
- Where does the problem occur?
- When does the problem occur?
- Under which conditions does the problem occur?
- Can the problem be reproduced?

The answers to these questions typically lead to a good description of the problem, which can then lead to a resolution of the problem.

What are the symptoms of the problem?

When starting to describe a problem, the most obvious question is "What is the problem?" This question might seem straightforward; however, you can break it down into several focused questions that create a more descriptive picture of the problem. These questions can include:

- Who, or what, is reporting the problem?
- What are the error codes and messages?
- How does the system fail? For example, is the problem a loop, hang, crash, performance degradation, or incorrect result?

Where does the problem occur?

Determining where the problem originates is not always easy, but it is one of the most important steps in resolving a problem. Many layers of technology can exist between the reporting and failing components. Networks, disks, and drivers are only a few of the components to consider when you are investigating problems.

The following questions help you to isolate the problem layer:

- Is the problem specific to one platform or operating system, or is it common across multiple platforms or operating systems?
- Is the current environment and configuration supported?

If one layer reports the problem, the problem does not necessarily originate in that layer. Part of identifying where a problem originates is understanding the environment in which it exists. Take some time to completely describe the problem environment, including the operating system and version, all corresponding software and versions, and the hardware. Confirm that you are running within an environment that is supported; many problems can be traced back to incompatible levels of software that are not intended to run together or have not been fully tested together.

When does the problem occur?

Develop a detailed timeline of events leading up to a failure, especially for cases that are one-time occurrences. You can most easily develop a timeline by working backward: Start at the time an error was reported (as precisely as possible, even down to the millisecond), and work backward through the available logs and information. Typically, you need to look only as far as the first suspicious event that you find in a diagnostic log.

To develop a detailed timeline of events, answer these questions:

- Does the problem happen only at a certain time of day or night?
- How often does the problem happen?
- What sequence of events leads up to the time that the problem is reported?
- Does the problem happen after an environment change, such as an upgrade or an installation of software or hardware?

Under which conditions does the problem occur?

Knowing which systems and applications are running at the time that a problem occurs is an important part of troubleshooting. These questions about your environment can help you to identify the cause of the problem:

- Does the problem always occur when the same task is being performed?
- Does a certain sequence of events need to occur for the problem to occur?
- Do any other applications fail at the same time?

Answering these types of questions can help you explain the environment in which the problem occurs and correlate any dependencies. Remember that just because multiple problems might have occurred around the same time, the problems are not necessarily related.

Can the problem be reproduced?

Problems that you can reproduce are often easier to solve. However, problems that you can reproduce can have a disadvantage. If the problem as a significant business impact, you do not want it to recur. If possible, re-create the problem in a test or development environment, which typically offers you more flexibility and control during your investigation. Answer the following questions:

- Can the problem be re-created on a test system?
- Are multiple users or applications encountering the same type of problem?
- Can the problem be re-created by running a single command, a set of commands, or a particular application?

Searching knowledge bases

You can often find solutions to problems by searching IBM knowledge bases. You can optimize your results by using available resources, support tools, and search methods.

About this task

You can find useful information by searching the information center for IBM Cognos, but sometimes you need to look beyond the information center to resolve problems.

Procedure

To search knowledge bases for information that you need, use one or more of the following approaches:

- Find the content that you need by using the IBM Support Portal.

  The IBM Support Portal is a unified, centralized view of all technical support tools and information for all IBM systems, software, and services. The IBM Support Portal lets you access the IBM electronic support portfolio from one place. You can tailor the pages to focus on the information and resources that you need for problem prevention and faster problem resolution. Familiarize yourself with the IBM Support Portal by viewing the demo videos about this tool. These videos introduce you to the IBM Support Portal, explore troubleshooting and other resources, and demonstrate how you can tailor the page by moving, adding, and deleting portlets.
- Search for content about IBM Cognos by using one of the following additional technical resources:
  - IBM Cognos Analytics APARs (problem reports)
  - IBM Cognos forums and communities.
- Search for content by using the IBM masthead search.

  You can use the IBM masthead search by typing your search string into the Search field on any ibm.com® page.
- Search for content by using any external search engine, such as Google, Yahoo, or Bing.

  If you use an external search engine, your results are more likely to include information that is outside the ibm.com domain. However, sometimes you can find useful problem-solving information about IBM products in newsgroups, forums, and blogs that are not on ibm.com.

  Tip: Include "IBM" and the name of the product in your search if you are looking for information about an IBM product.

Getting fixes

A product fix might be available to resolve your problem.

Procedure

To find and install fixes:

1. Determine which fix you need (Fix Central) (opens in new window) (http://www.ibm.com/support/fixcentral/)
2. Download the fix. Open the download document and follow the link in the "Download package" section.
3. Apply the fix by following the instructions in the "Installation Instructions" section of the download document.
4. Subscribe to receive weekly email notifications about fixes and other IBM Support information.

Contacting IBM Support

IBM Support provides access to a variety of IBM resources for help with software questions.

Before you begin

After trying to find your answer or solution by using other self-help options such as technotes, you can contact IBM Support. Before contacting IBM Support, your company must have an active IBM maintenance contract, and you must be authorized to submit problems to IBM. You should also have the following information at hand:

- Your customer identification number

- Your service request number, if it is an ongoing service request
- The phone number where you can be reached
- The version of the software you use
- The version of the operating environment you use
- A description of what you were doing when the problem occurred
- The exact wording of any error messages that display
- Any steps you took to attempt to solve the problem

For information about the types of available support, see the Support portfolio topic in the *Software Support Handbook* (opens in new window).

Procedure

Complete the following steps to contact IBM Support with a problem:

1. Define the problem, gather background information, and determine the severity of the problem. For more information, see the Getting IBM support (opens in new window) topic in the *Software Support Handbook*.
2. Gather diagnostic information.
3. Submit the problem to IBM Support in one of the following ways:
   - Using IBM Support Assistant (ISA): Use this feature to open, update, and view an Electronic Service Request with IBM. Any data that has been collected can be attached to the service request. This expedites the analysis and reduces the time to resolution.
   - Online through the IBM Support Portal (opens in new window): You can open, update, and view all your Service Requests from the Service Request portlet on the Service Request page.
   - By phone: For the phone number to call, see the Directory of worldwide contacts (opens in new window) web page.

Results

If the problem that you submit is for a software defect or for missing or inaccurate documentation, IBM Support creates an Authorized Program Analysis Report (APAR). The APAR describes the problem in detail. Whenever possible, IBM Support provides a workaround that you can implement until the APAR is resolved and a fix is delivered. IBM publishes resolved APARs on the IBM Support Web site daily, so that other users who experience the same problem can benefit from the same resolution.

Exchanging information with IBM

To diagnose or identify a problem, you might need to provide IBM Support with data and information from your system.

In other cases, IBM Support might provide you with tools or utilities to use for problem determination.

Sending information to IBM Support

To reduce the time that it takes to resolve your problem, you can send trace and diagnostic information to IBM Support.

Procedure

To submit diagnostic information to IBM Support:

1. Open a problem management record (PMR). You can use the IBM Support Assistant (opens in new window) or the IBM Service Request tool (opens in new window).
2. Collect the diagnostic data that you need. Diagnostic data helps reduce the time that it takes to resolve your PMR. You can collect the diagnostic data manually or automatically.
3. Compress the files by using the TRSMAIN or AMATERSE program. Download the free utility from the IBM to the IBM Cognos Analytics system and then install the utility using the TSO RECEIVE command.
4. Transfer the files to IBM. You can use one of the following methods to transfer the files to IBM:

- The Service Request tool (opens in new window)
- Standard data upload methods: FTP, HTTP
- Secure data upload methods: FTPS, SFTP, HTTPS
- Email

If you are using an IBM Cognos product and you use ServiceLink / IBMLink to submit PMRs, you can send diagnostic data to IBM Support in an email or by using FTP.

All of these data exchange methods are explained on the IBM Support site (opens in new window).

Receiving information from IBM Support
Occasionally an IBM technical-support representative might ask you to download diagnostic tools or other files. You can use FTP to download these files.

Before you begin

Ensure that your IBM technical-support representative provided you with the preferred server to use for downloading the files and the exact directory and file names to access.

Procedure

To download files from IBM Support:

1. Use FTP to connect to the site that your IBM technical-support representative provided and log in as `anonymous`. Use your email address as the password.
2. Change to the appropriate directory:
   a) Change to the `/fromibm` directory.

   ```
   cd fromibm
   ```

   b) Change to the directory that your IBM technical-support representative provided.

   ```
   cd nameofdirectory
   ```

3. Enable binary mode for your session.

   ```
   binary
   ```

4. Use the `get` command to download the file that your IBM technical-support representative specified.

   ```
   get filename.extension
   ```

5. End your FTP session.

   ```
   quit
   ```

Subscribing to Support updates

To stay informed of important information about the IBM products that you use, you can subscribe to updates.

About this task

By subscribing to receive updates, you can receive important technical information and updates for specific Support tools and resources. You can subscribe to updates by using one of two approaches:

RSS feeds and social media subscriptions
The following RSS feeds and social media subscriptions are available for IBM Cognos Analytics:

- RSS feed for a developerWorks® forum (opens in new window).
- RSS feed for the Support site for IBM Cognos Analytics (opens in new window)

For general information about RSS, including steps for getting started and a list of RSS-enabled IBM web pages, visit the IBM Software Support RSS feeds (opens in new window) site.

My Notifications

With My Notifications, you can subscribe to Support updates for any IBM product. You can specify that you want to receive daily or weekly email announcements. You can specify what type of information you want to receive, such as publications, hints and tips, product flashes (also known as alerts), downloads, and drivers. My Notifications enables you to customize and categorize the products that you want to be informed about and the delivery methods that best suit your needs.

Procedure

To subscribe to Support updates:

1. Subscribe to the *Product* RSS feeds.
2. To subscribe to My Notifications, begin by going to the IBM Support Portal (opens in new window) and clicking **My Notifications** in the **Notifications** portlet.
3. If you have already registered for My support, sign in and skip to the next step. If you have not registered, click **Register now**. Complete the registration form by using your email address as your IBMid and click **Submit**.
4. Click **Edit profile**.
5. Click **Add products** and choose a product category; for example, **Software**.
6. In the second list, select a product segment; for example, **Data & Information Management**.
7. In the third list, select a product subsegment, for example, **Databases**.
8. Select the products that you want to receive updates for.
9. Click **Add products**.
10. After selecting all products that are of interest to you, click **Subscribe to email** on the **Edit profile** tab.
11. Select **Please send these documents by weekly email**.
12. Update your email address as needed.
13. In the **Documents list**, select the product category; for example, **Software**.
14. Select the types of documents that you want to receive information for.
15. Click **Update**.

Results

Until you modify your RSS feeds and My Notifications preferences, you receive notifications of updates that you have requested. You can modify your preferences when needed (for example, if you stop using one product and begin using another product).

Log Files

Log files can help you troubleshoot problems by recording the activities that take place when you work with a product.

Operations performed in IBM Cognos Analytics are recorded in various log files for tracking purposes. For example, if you experienced problems installing IBM Cognos Analytics, consult the transfer log file to learn what activities the installation wizard performed while transferring files.

Before you begin viewing log files, ensure that they contain the information that you need.

Use IBM Cognos Administration to set the level of detail to log for each category.

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

Use IBM Cognos Configuration to specify the size, number, and location of log files, and to configure the properties of the log server.

When troubleshooting, the following files can assist you:

Transfer log file

This file records the components you installed, disk space information, the selections you made in the transfer dialogs, and any errors the installation wizard encountered while transferring components. It also records the activities that the installation wizard performed while transferring files.

The transfer log file is located in the `install_location\logs` directory. The file name includes the product name and time stamp. The following is an example of the file name format:

```
IBM_Cognos_Analytics_Install_04_21_2016_11_00_59.log
```

Installation Configuration log file

This log file records any configuration activities during the installation. For example, it reports the available port for the dispatcher.

The transfer summary-error log file is located in the `install_location\logs` directory. It is named `install_configuration.log`

The Startup Configuration File

This file records your configuration choices each time you save your property settings. The file name is `cogstartup.xml`.

If you are unable to save your configuration, or are having problems you can revert to a previously saved configuration file. The backup configuration files are located in the `install_location/configuration` directory. The following is an example of the file name format for backup configuration files:

```
cogstartup_200811231540.xml
```

The Startup Configuration Lock File

This file is created each time you open IBM Cognos Configuration. It prevents you from opening more than one IBM Cognos Configuration window.

If you experience problems opening IBM Cognos Configuration, you can check the `install_location/configuration` directory for the `cogstartup.lock` file. If the file exists and IBM Cognos Configuration is not open, it means that IBM Cognos Configuration did not shut down properly the last time you used it. You can delete the lock file and then open IBM Cognos Configuration.

The Locale Configuration File

This file records the configuration choices you make in IBM Cognos Configuration for product and content locales, locale mapping, and currency support.

If you experience problems with language support in the user interface or in reports, use these files to track your changes. The backup configuration files are located in the *install_location*/configuration directory. The following is an example of the file name format:

```
coglocale_200811231540.xml
```

The Runtime Log File

The default IBM Cognos log file, named cogaudit.log file, or other log files that you configure to receive log messages from the log server, record information after you start the IBM Cognos Analytics service. They are located in the *install_location*/logs directory. If you configured another destination for log messages, check the appropriate file or database.

Some log messages indicate problems. Most messages provide information only, but others can help you to diagnose problems in your runtime environment.

The Gateway Log File

The gateways record errors in the gateway log file, which is located in the *install_location*/logs directory.

You can use the gateway log file to troubleshoot problems that prevent the gateway from processing requests or from using encryption. Symptoms of these problems are as follows:

- User IDs and passwords do not work
- Single signon does not work
- The dispatcher is running but users receives an error message advising that the IBM Cognos Analytics server is not available

The gateway log file uses the following naming format, where *gateway_interface* is cgi, mod2 (Apache 2.0 module), or isapi.

gw*gateway_interface*.log (for example, gwcgi.log)

The Uninstallation Log File

This file records the activities that the Uninstall wizard performed while uninstalling files. The log file is named cognos_uninst_log.htm and is located in the Temp directory. You can use the log file to troubleshoot problems related to uninstalling IBM Cognos Analytics components.

The Silent Mode Log File

This file records the activities that IBM Cognos Configuration performed while running in silent mode. This log file is named cogconfig_response.csv and is located in the *install_location*/logs directory.

Appendix C. Deprecation notices

This topic lists features that are deprecated in future releases of IBM Cognos Analytics.

- The use of `*install_location*\webapps\p2pd\WEB-INF\lib` for locating JDBC drivers is deprecated for future releases. It is replaced with the `*install_location*\drivers` directory.

Appendix D. About this guide

This document is intended for use with IBM Cognos Analytics. IBM Cognos Analytics is a Web product with integrated reporting, dashboarding, analysis, and event management features.

This guide contains instructions for installing, upgrading, configuring, and testing IBM Cognos Analytics.

Audience

To use this guide, you should be familiar with

- reporting concepts
- database and data warehouse concepts
- security issues
- basic Windows or UNIX administration skills
- existing server environment and security infrastructure in your organization

Finding information

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

You can also read PDF versions of the product online help files by clicking the PDF links at the top of each HTML page, or access the PDFs from the IBM Cognos product documentation web page (www.ibm.com/support/docview.wss?uid=swg27047187).

Forward-looking statements

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

Samples disclaimer

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

Index

IBM®