Administering ColdFusion Server

ColdFusion 4.0 for Windows® NT, Windows 95/98, and Solaris

Allaire Corporation

Copyright Notice

Part number: AA-ADMIN-RK

Contents

Chapter 3: Configuring ColdFusion Server 19

Chapter 6: Clustering and Load-Balancing 83

CHAPTER 1

Welcome To ColdFusion

ColdFusion is a rapid application development system for professional developers who want to create dynamic Web applications and interactive Web sites. It provides the fastest way to integrate browser, server, and database technologies into powerful Web applications. With ColdFusion, you can build everything from online stores to sophisticated business systems.

Developing applications with ColdFusion does not require coding in a traditional programming language; instead, you build applications by combining standard HTML with a straightforward server-side markup language, the ColdFusion Markup Language (CFML).

Contents

Product Features

This release marks a significant milestone in the evolution of ColdFusion as a development system for building scalable Web applications that integrate browser, server, and database technologies.

The focus of our development work has been in four major areas: rapid development, scalable deployment, open integration, and total security. Each of these areas is highlighted below.

Rapid Development

ColdFusion 4.0 continues to enhance the speed of development and ease-of-use that have been the hallmark of the development system from its beginning. ColdFusion 4.0 increases development productivity by integrating ColdFusion Studio more closely with ColdFusion Server, extending the visual tools, and expanding the functionality of the tag-based server scripting language, CFML.

New Feature Highlights

- **Two-way Visual Programming** – ColdFusion Studio 4.0 includes new, more powerful visual programming tools including a WYSIWYG design mode and enhanced visual database tools.
- **Dynamic State Simulation** – The ColdFusion Studio IDE supports establishing state for pages so developers can preview the interactions between pages that rely on multiple variables.
- **Dynamic Page Quality Assurance** – New tools support validating links, configuring dynamic page previewing and validating CFML grammar in pages.
- **One-step Deployment** – New features extend the site- and page-management features to support flexible deployment of complex applications to multiple servers, making the process of moving from development to deployment simple and straightforward.
- **Site Visualization** – ColdFusion Studio 4.0 supports the ability to visualize sites and see how pages are linked to each other across a system.
- **CFScript** – CFML supports traditional scripting syntax for complex data processing on the server using branching and looping.

Scalable Deployment

ColdFusion has already reached a point where it is being used to deliver very large volume sites and applications servicing tens of thousands of users. With the 4.0 release, we provide powerful new features that significantly enhance scalability.

New Feature Highlights

- **Load Balancing –** ColdFusion 4.0 supports native load balancing giving developers the ability to deploy large volume applications in high performance clusters that scale to meet any user demands. (Enterprise Edition only.)
- **High Availability –** ColdFusion 4.0 supports the creation of multi-server clusters with automatic fail-over if any server goes down – providing the infrastructure for deploying large volume, high-availability sites. (Enterprise Edition only.)
- **Open State Repository** – State information can be stored in a pluggable external data source so servers can be easily configured for clustering and load balancing.
- **Advanced Thread Pooling** – The Web application server offers sophisticated thread pooling using I/O completion ports and tight integration with web server APIs.
- **Integration with NT Performance Monitor** – ColdFusion Server is fully integrated with the NT Performance Monitor for increased manageability and tuning.

Open Integration

ColdFusion offers better integration with server systems including mail, web servers and directories than any other IRAD system. With the 4.0 release, this integration has been extended to support Extensible Markup Language (XML) and enterprise technologies:

- **Automatic XML Parsing** – ColdFusion Server supports automatic parsing of XML data into CFML variables and the translation of CFQUERY record sets into XML.
- **Native Database Drivers** – ColdFusion 4.0 supports native database connectivity for Oracle and Sybase. (Enterprise Edition only.)
- **CORBA** – ColdFusion 4.0 extends its integration with component standards by supporting Common Object Request Broker Architecture (CORBA) and possibly Enterprise JavaBeans. (Enterprise Edition only.)
- **ColdFusion Extensions (CFX)** – ColdFusion 4.0 supports the creation of more complex CFXs making it possible to extend ColdFusion with components created with CFML, C/C++, COM, CORBA, JavaBeans, JavaScript, and VBScript.

Total Security

ColdFusion currently provides a secure environment for development and deployment. These security features enable a much greater range of flexibility and control over security both for development and deployment.

- **Open Authentication System** – Developers can leverage a wide range of different user authentication systems in their applications from within ColdFusion including Windows NT security, LDAP directories, and proprietary user and group databases.
- **Advanced Remote Development Security** – The Remote Development Services (RDS) used by ColdFusion Studio allow for user and group security configuration for all resources including files and databases using a configurable backend authentication system that integrates with existing user and group databases.
- **Server Sandbox Deployment** – With the server sandbox, server administrators can control what resources (files, databases and components) an application has access to when it is running on a server. This allows server administrators to deploy multiple applications on the same server without creating the risk that one application will access another application's resources.

Learning About Web Development and ColdFusion

Web application development is such a new field and requires such a mix of emerging and established technologies that meeting the documentation needs of ColdFusion users is quite a challenge. The skills required to build and deploy dynamic Web content range across HTML, databases, graphic arts, networking, a slew of scripting and programming languages, and even writing!

We have tried to present information on ColdFusion development and supporting technologies so that you can pursue topics of interest to you and integrate them into your overall learning process.

While it is certainly possible for an individual to master all these skills, the team approach has quickly become the only realistic development model for delivering complex applications, and we address issues such as building and maintaining Web projects and working with version source control.

We also include pointers to many resources, both print and online, that provide additional information about ColdFusion and supporting technologies.

New to Web development?

The ColdFusion Markup Language is a tag-based language that integrates with HTML to provide greatly enhanced functionality for Web sites. The skills you are building in HTML and Web site development are a solid foundation for ColdFusion development.

ColdFusion Studio is an easy-to-use HTML editor that offers many powerful features for building and maintaining Web sites. It is also the integrated development environment (IDE) for ColdFusion. That means you can use Studio to learn HTML, to develop and test Web sites, and then to develop dynamic content with CFML.

New to ColdFusion?

../../Getting_Started_with_ColdFusion/contents.htm*Getting Started with ColdFusion*/a presents a quick tour of a ColdFusion application. ../../Developing_Web_Apps/contents.htm*Developing Web Applications with ColdFusion*/a is a good place to start learning about building ColdFusion applications.

If you want access to experienced ColdFusion developers, you can participate in the Allaire Online Forums, where you can post messages and read replies on all subjects relating to ColdFusion. Check out the Forums at http://forums.allaire.com.

Experienced Web developer?

You'll probably want to get going with your project, so take a look at the ../../Developing_Web_Apps/contents.htm*Developing Web Applications with ColdFusion*/a chapters on setting up data sources, managing input and output, the application framework, Java forms, and programming variables. ../../Getting_Started_with_ColdFusion/contents.htm*Getting Started with ColdFusion*/a includes a complete application with lots of working code samples that you can drop in to quickly prototype a project. If you want to integrate COM, CORBA, custom tags, CF API tags, LDAP, CFScript, or XML data exchange into your applications, see ../../Advanced_ColdFusion_Development/contents.htm*Advanced ColdFusion Development*/a.

Developer Resources

Allaire Corporation is committed to setting the standard for customer support in developer education, technical support, and professional services. Our Web site is designed to give you quick access to the entire range of online resources.

Allaire Developer Services	
Resource	**Description**
Allaire Web site http://www.allaire.comwww.allaire.com/a	General information about Allaire products and services.
Technical Support http://www.allaire.com/supportwww.allaire.com/support/a	Allaire offers a wide range of professional support programs. This page explains all of the available options.
Professional Education http://www.allaire.com/educationwww.allaire.com/education/a	Information about classes, on-site training, and online courses offered by Allaire.

Allaire Developer Services (Continued)	
Resource	**Description**
Developer Community http://www.allaire.com/developerwww.allaire.com/developer/a	All of the resources you need to stay on the cutting edge of ColdFusion development, including online discussion groups, Knowledge Base, Component Exchange, Resource Library, technical papers and more.
Allaire Alliance http://www.allaire.com/partnerswww.allaire.com/partners/a	The growing network of solution providers, application developers, resellers, and hosting services creating solutions with ColdFusion.

About ColdFusion Documentation

The documentation set is designed to provide support for all components of the ColdFusion development system. Both the print and online versions are organized to allow you to quickly locate the information you need.

Documentation set

The documentation set contains:

../../Getting_Started_with_ColdFusion/contents.htm*Getting Started with ColdFusion*/a — Covers system installation and basic configuration, describes the components of the ColdFusion development system, and introduces the ColdFusion Markup Language (CFML).

../../Administering_the_App_Server/contents.htm*Administering ColdFusion Server*/a — Describes configuration options for maximizing performance, managing data sources, setting security levels, and a range of development and site management tasks.

../../Developing_Web_Apps/contents.htm*Developing Web Applications with ColdFusion*/a — Presents the fundamentals of ColdFusion application development and deployment, including data sources, user interfaces, and Web technologies. The development tools in ColdFusion Studio are covered in detail.

../../Advanced_ColdFusion_Development/contents.htm*Advanced ColdFusion Development*/a — Gives an overview of CFML elements such as functions, expressions, arrays, scripting, and XML data exchange. Also discusses custom tags, CF API tags, integrating object technologies, and site management.

../../CFML_Language_Reference/contents.htm*CFML Language Reference*/a — Provides the complete syntax, with example code, of all CFML elements.

Quick Reference Card — An online (Acrobat) guide to CFML.

Documentation distribution

The ColdFusion CD-ROM contains the complete document set. The setup program installs the document set by default.

The print manuals are available in Adobe Acrobat (PDF) format from the `dochome.htm` page in the `/cfdocs` directory of your Web root. If the files are not available locally, you get them from our Web site at http://www.allaire.com/products/COLDFUSION/Documentation.cfm.

You can also access the documentation in HTML from both of these locations.

Reading online documentation

You can open the online documents in a number of ways:

- From your browser, click the ColdFusion Documentation link on the Welcome to ColdFusion page. Each page contains links to other documents and a search window.
- In ColdFusion Studio, click the Help tab in the Resources area to open the help tree. You can expand the list to select topics by title.

Documentation conventions

When reading, please be aware of these formatting cues:

- Code samples, filenames, and URLs are set in a distinct font
- Notes and tips are identified by bold type in the margin
- Bulleted lists present options and features
- Numbered steps indicate procedures
- Toolbutton icons are generally shown with procedure steps
- Menu levels are separated by the greater than (>) sign
- Text for you to type in is set in *italics*

Contacting Allaire

Corporate headquarters

Allaire Corporation
One Alewife Center
Cambridge, MA 02140

Tel: 617.761.2000
Fax: 617.761.2001

http://www.allaire.com

Technical support

Telephone support is available Monday through Friday 8 A.M. to 8 P.M. Eastern time (except holidays)

Toll Free: 888.939.2545 (U.S. and Canada)

Tel: 617.761.2100 (outside U.S. and Canada)

Postings to the ColdFusion Support Forum (http://forums.allaire.com) can be made at any time.

Sales

Toll Free: 888.939.2545

Tel: 617.761.2100
Fax: 617.761.2101

Email: mailto:sales@allaire.com/a
Web: http://www.allaire.com/store

CHAPTER 2

Introduction

Contents

Overview of Administering ColdFusion

The ColdFusion Administrator is the administrative interface of the ColdFusion Server. ColdFusion Server is the component of the overall ColdFusion Web application development system that processes ColdFusion application pages and returns HTML pages to Web clients.

The Administrator provides a browser-based interface allowing you to manage server performance, add and configure ColdFusion data sources, schedule pages, manage log files, and so on. For any ColdFusion development project, some level of administration is generally necessary to set up CFAS for your application.

Accessing the Administrator

All administrative operations are performed using the ColdFusion Administrator, which you can launch from the ColdFusion 4.0 program group in Windows, or by opening the Administrator URL in your browser. If CFAS is installed locally, you can open the following URL:

```
http://127.0.0.1/CFIDE/Administrator/index.cfm
```

To access the Administrator remotely, you open the following URL:

```
http://hostname/CFIDE/Administrator/index.cfm
```

Where *hostname* is the name of the system on which CFAS is installed. If you are using ColdFusion Administrator security, you will be prompted for a password. If your Web server is providing security, access to the Administrator pages is governed by the permissions defined in your Web server. Note that the Administrator's URL is case sensitive on Solaris and should be used as shown.

Initial ColdFusion administration tasks

Immediately after installing ColdFusion Server, you'll probably want to perform some of the following configuration tasks:

Initial Adminitration Tasks
If necessary, configure your Web server for ColdFusion If you are using Netscape or Apache Web servers on Solaris or HP-UX, you'll need to perform some initial configuration tasks for ColdFusion. For more information, see ../../Getting_Started_with_ColdFusion/contents.htm*Getting Started with ColdFusion*/a
Add, configure, and verify ColdFusion data sources You use the Administrator to create ColdFusion data sources for your applications. You can configure ODBC data sources or employ a native database driver to access your Oracle or Sybase databases (Enterprise Edition only). For more information about data sources, see Chapter 4, Managing Data Sources.

Initial Adminitration Tasks (Continued)
Configure Admininstrator email ColdFusion error pages include an email address link to the ColdFusion administrator. You'll also need to define a default mail server hostname. Defining the email address of the administrator allows users of your ColdFusion applications to report errors they may encounter. You could, for example, use a messaging service to receive email by pager alerting you to any errors encountered in a ColdFusion application. For more information, see Chapter 3, Configuring ColdFusion Server.
Configure ColdFusion log file options ColdFusion produces a number of different log files you can use to monitor server errors and activity. In addition, you can log all email messages sent by ColdFusion to a log file. For more information, see Chapter 3, Configuring ColdFusion Server.

Summary of Administrative Tasks

The things you may need to do to set up and run the ColdFusion Server fall into several categories:

- Installing and configuring ColdFusion
- Managing data sources
- Managing server performance and resources
- Managing security for users, applications, and server resources

You can learn more about each of these areas of ColdFusion administration by referring to the information in the following table:

Information about ColdFusion Administration	
Subject	**Where to find it**
Installing ColdFusion	See ../../Getting_Started_with_ColdFusion/contents.htm*Getting Started with ColdFusion*/a.
Configuring ColdFusion data sources	Chapter 4, Managing Data Sources.
Native database drivers for Oracle and Sybase databases	
Configuring OLE-DB data sources	

Information about ColdFusion Administration (Continued)	
Subject	**Where to find it**
Setting debugging options	Chapter 3, Configuring ColdFusion Server.
Configuring Administrator email	
Managing log files	
Clustering and load-balancing	Chapter 6, Clustering and Load-Balancing.
Using CGI with ColdFusion	Chapter 8, Configuring Basic Security.
Configuring basic security for remote development and administration	Chapter 8, Configuring Basic Security
Configuring Advanced security for ColdFusion resources	Chapter 9, Configuring Advanced Security

ColdFusion Server Professional Edition

The Professional Edition offers the full range of features required for delivering advanced Web applications including support for connecting to any ODBC database, sending dynamic email and integrating other server and browser technologies into secure Web applications.

Professional Edition	
Category	**Description**
Databases	All ODBC databases OLE-DB
Platforms	Microsoft Windows NT 4.0 and 5.0 (NSAPI, ISAPI, WSAPI, and CGI) Sun Solaris 2.5.1 and higher (NSAPI, Apache API, and CGI)
Other	Additional features not supported in the Workgroup Edition: • Supports scheduling of batch processes and page requests to create push applications • Static page publishing • Open client state repository, allowing the use of any backend database for storing client state information • Support for Microsoft Transaction Server (MTS) to increase the reliability of transaction-intensive applications

ColdFusion Server Enterprise Edition

The Enterprise Edition offers the advanced features required for delivering large scale Web applications including support for native database drivers, CORBA, and enterprise JavaBeans as well as automatic load-balancing and dynamic fault tolerance.

Enterprise Edition	
Category	**Description**
Databases	All ODBC databases OLE-DB Native drive support for Sybase System 11 and Oracle 7.3 and 8
Platforms	Microsoft Windows NT 4.0 and 5.0 (ISAPI) Sun Solaris 2.5.1 and higher (NSAPI)
Other	Additional features not available in the Workgroup or Professional editions: • Native database drivers for Oracle and Sybase databases • Enterprise object standards: CORBA and enterprise JavaBeans • Clustering, load-balancing, and fail-over

The ColdFusion Administrator

The Administrator is a Web application you use to configure the ColdFusion Server, and to set various server options. The Administrator includes options for managing a wide range of server settings.

You can open the Administrator by selecting the ColdFusion Administrator icon in the ColdFusion 4.0 program group (Windows), or by opening the following URL:

`http://hostname/CFIDE/Administrator/index.cfm`

Where *hostname* is the name of the server where ColdFusion is installed. The following table describes the purpose of each category in the Administrator.

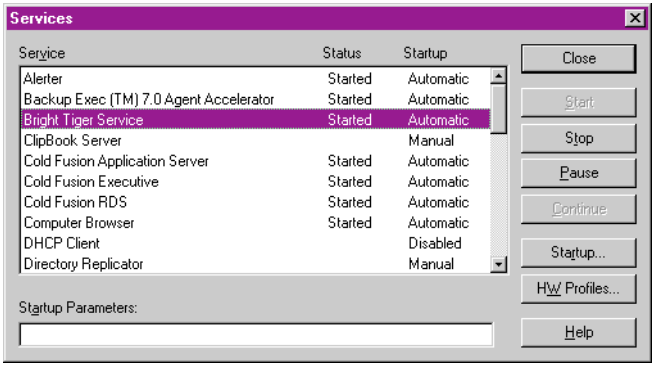
ColdFusion Administrator Options	
Category	**Description**
Server	Includes options for tuning server performance, as well as: • Configuring Administrator and ColdFusion Studio Basic and Advanced Security • Enabling and configuring ColdFusion application, session, and client variables • Mapping directories • ColdFusion version information
Data Sources	Use to configure ColdFusion data sources, including: • Native database drivers for Oracle and Sybase databases • ODBC data sources • Verifying a ColdFusion data source
Extensions	Includes options for registering Java applets and CFX tags, custom tags written in C++.
Logging	You use the Logging pages to configure a ColdFusion Administrator email address, and to: • Specify a directory for ColdFusion log files • Set mail logging options • View ColdFusion log files
Automated tasks	The Automated tasks pages provide options for: • Adding new scheduled tasks • Specifying how often ColdFusion checks for new scheduled tasks to execute
Miscellaneous	Use the Mail page to specify a default mail server hostname as well as other mail-related configuration options.

ColdFusion Services on Windows NT

By default, ColdFusion employs four separate services under Windows NT. The following table explains the purpose of each one.

ColdFusion Services on Windows NT	
Service	**Purpose**
Bright Tiger Service	Manages CFAS load-balancing and failover. For more information about clustering, which enables load-balancing and failover in ColdFusion, see Chapter 6, Clustering and Load-Balancing.
ColdFusion Application Server	The main CFAS service. ColdFusion pages cannot be processed if this service is not running.
ColdFusion Executive	Polls the ColdFusion Application Server service and automatically restarts the ColdFusion Application Server if it is not running.
ColdFusion RDS	The ColdFusion Remote Development Service provides security, directory and file browsing, and debugging services for ColdFusion Studio.
SiteMinder Authentication Service	Only present if you chose the advanced security option during ColdFusion setup. Provides user authentication services for advanced security.
SiteMinder Authorization Service	Only present if you chose the advanced security option during ColdFusion setup. Provides access authorization services for advanced security.

You can use the Windows NT Services Control Panel to view and manage these and other Windows NT services.



ColdFusion Processes on Solaris

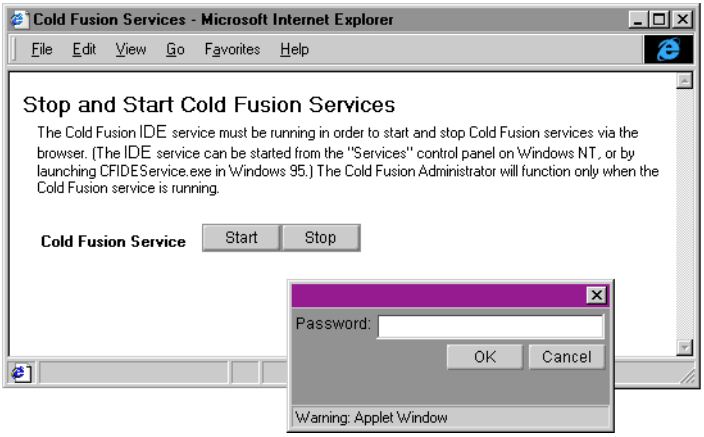
ColdFusion runs these processes on the system:

- `cfexec` - Starts/stops the other processes and manages page scheduling
- `cfserver` - The application server process
- `cfrdsservice` - Provides system support for the Administrator
- `ipaliasd` - Provides IP failover capability for ColdFusion Server
- `dbeng50` - Database services for clustering ColdFusion servers

In addition, the `windu_registryd40` process provides an emulation of the Windows registry database. This process must be running (as the root user) in order for ColdFusion to function. The start script will start this process if it isn't running (such as during system startup). The stop script does not stop the registry process.

Starting and Stopping ColdFusion

Normally, ColdFusion services are started during ColdFusion setup and configured to run whenever you start your system. However, if you need to start ColdFusion services, click the Start-Stop icon in the ColdFusion program group. If a password is configured for the Administrator, you will be prompted to enter a password before you can start or stop ColdFusion services.



Windows NT

During setup, ColdFusion is installed as a series of system services in Windows NT. Ordinarily, ColdFusion is launched at startup time. To manage how the services are run, use the Services Control Panel in Windows NT.

To prevent ColdFusion from running at startup:

1. Open the Services Control Panel.
2. Select the ColdFusion Application Server service.
3. Click Stop to halt the service immediately, click Startup to configure startup options for ColdFusion.

Solaris

Two scripts are provided to start and stop the ColdFusion processes:

```
<installdir>/coldfusion/bin/start
<installdir>/coldfusion/bin/stop
```

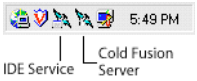
These scripts can only be run as root. In addition, the ColdFusion installation also installs the following scripts to start and stop ColdFusion during system boot and shutdown:

```
/etc/init.d/coldfusion
/etc/rc1.d/K19coldfusion
/etc/rc3.d/S25coldfusion
```

Windows 95 and Windows 98

Since Windows 95 and Windows 98 do not have a services architecture, ColdFusion must be run as an ordinary executable.

When ColdFusion is running in Windows 95 or 98, two icons appear in the system tray:



To halt the ColdFusion service or to access the ColdFusion Administrator, right mouse click the IDE service icon.

To run ColdFusion at startup, place a shortcut for the ColdFusion icon in the Startup program group.

Stopping ColdFusion

Stopping ColdFusion services may be necessary in the following instances:

- To install a new ODBC driver package
- To replace or upgrade your Web server software
- To upgrade or reinstall your ColdFusion program files
- To update or replace database files

The Stop/Start Services page can also be used to restart the ColdFusion Server after a critical failure or error. The Start-Stop page is available only from the local

workstation. You can move the Start-Stop page to a directory in your Web server document directory. If you do so, you need to make sure the file is secured using your native Web server security.

CHAPTER 3

Configuring ColdFusion Server

This section covers basic ColdFusion administration.

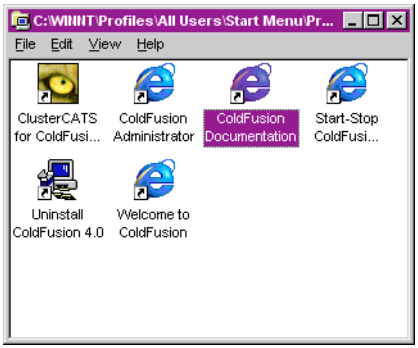
Contents

The ColdFusion Administrator

You use the Administrator to perform a variety of administrative tasks for the ColdFusion Server, such as adding and configuring a data source, or scheduling application page execution, configuring security settings, and so on. During the ColdFusion installation process, you specify an Administrator password that is used to prevent unauthorized access to the Administrator pages.

To open the ColdFusion Administrator:

1. Click the ColdFusion Administrator icon in the ColdFusion program group



   or

2. Open the administrator by loading the following URL:

   `http://hostname/CFIDE/Administrator/index.cfm`

Where *hostname* is the name of the server hosting ColdFusion. Note that on Solaris, the URL path is case-sensitive.

Remote administration

To access ColdFusion Administrator pages remotely, you load the following URL:

`http://hostname/CFIDE/administrator/index.cfm`

where *hostname* is the name of the system on which ColdFusion is installed. If you are using ColdFusion Administrator security, you will be prompted to enter a password. If your Web server is providing security, access to the Administrator pages is governed by the permissions defined in your Web server.

Once the Administrator page loads, click one of the Administrator links to work with a specific area of the Administrator.

ColdFusion Administrator Options	
Category	**Description**
Server	Includes options for tuning server performance, as well as: • Configuring Administrator and ColdFusion Studio passwords and security options • Enabling and configuring ColdFusion application, session, and client variables • Mapping directories • ColdFusion version information
Data Sources	Use to configure ColdFusion data sources, including: • Native database drivers for Oracle and Sybase databases • ODBC data sources • Verifying a ColdFusion data source
Extensions	Includes options for registering Java applets and CFX tags: custom tags written in C++.
Logging	You use the Logging pages to configure a ColdFusion Administrator email address, and to: • Specify a directory for ColdFusion log files • Set mail logging options • View ColdFusion log files
Automated tasks	The Automated tasks pages provide options for: • Adding new scheduled tasks • Specifying how often ColdFusion checks for new scheduled tasks to execute
Miscellaneous	Use the Mail page to specify a default mail server hostname as well as other mail-related configuration options.

Starting and Stopping ColdFusion

Generally speaking, you should always stop and restart ColdFusion Server after making any changes that affect a data source, connection parameter such as caching, thread count, and so on. Specifically, you stop and restart ColdFusion services after making any of the following changes in the Administrator:

- After changing any server settings on the Server Settings page.
- After changing the scheduled task refresh interval. This setting in the ColdFusion Administrator determines how often ColdFusion checks for newly scheduled tasks.
- Enabling the performance monitoring options in the ColdFusion Administrator. This feature allows you to use the native Windows NT performance monitor to track ColdFusion performance-related data. For more information, see "Monitoring ColdFusion Performance" on page 32.
- Changing the user account under which ColdFusion runs.
- Changing an existing data source setting, such as Page timeout, Buffer size, or Maintaining database connections.

Using batch files to start and stop ColdFusion (Windows)

You can use batch files in Windows NT to stop and restart ColdFusion services. The Windows NT NET START and NET STOP commands can be used in batch files to start and stop ColdFusion services, as in the following excerpt:

```
NET STOP "Cold Fusion Application Server"
NET START "Cold Fusion Application Server"
```

Batch files, as well as other executables, can be scheduled in Windows NT. Refer to your Windows NT documentation for more information about scheduling, and stopping and starting NT services.

Note You must be logged in with Administrator rights to execute these batch commands.

Using scripts to start and stop ColdFusion (Solaris)

Two scripts are provided to start and stop the ColdFusion processes:

```
<installdir>/coldfusion/bin/start
<installdir>/coldfusion/bin/stop
```

Note You must be logged in with root privileges to run these scripts.

In addition, the ColdFusion installation installs the following scripts to start and stop ColdFusion during system boot and shutdown:

```
/etc/init.d/coldfusion
/etc/rc1.d/K19coldfusion
/etc/rc3.d/S25coldfusion
```

ColdFusion runs the following processes on the system:

- `cfexec` - Starts/stops the other processes and manages page scheduling
- `cfserver` - The application server process
- `cfideservice` - Provides system support for the Administrator

- `ipaliasd` - Provides IP failover capability for ColdFusion Server
- `dbeng50` - Database services for clustering ColdFusion servers

In addition, the `windu_registryd42` process provides an emulation of the Windows registry database. This process must be running (as the root user) in order for ColdFusion to function. The start script will start this process if it isn't running (such as during system start-up). However, the stop script does not stop the registry process.

The Server Settings Page

The Administrator Server Settings page contains several configuration options you can set or enable to manage the ColdFusion server. Many of these options can significantly affect server performance. Use the following table to find out about options on the Server Settings Administrator page.

Server Settings Options	
Option	**Description**
Limit simultaneous requests	Use this value to limit the number of simultaneous requests for the ColdFusion server. Once ColdFusion reaches this limit, requests are queued up and handled in the order received.
Timeout requests	Set a value to limit the amount of time ColdFusion waits before terminating a request.
Restart unresponsive server	This option allows you to restart the ColdFusion Server service (daemon) in the event some ColdFusion component does not respond within the specified amount of time.
Enforce strict attribute validation	Enables strict attribute validation rules. ColdFusion tag attributes that are not relevant to the execution of a tag will not be allowed. When disabled, irrelevant attributes may be passed to CFML tags without effect. Strict attribute validation improves template execution time and can help prevent many CFML coding errors.
Template cache size	Use this option to specify how much memory you want to reserve for caching ColdFusion pages. For best performance, assuming your server has enough memory, you should set this value to the total number of kilobytes of all your active ColdFusion pages.
Trusted cache	Allows ColdFusion to use cached application pages (templates) without first checking to see if they've been changed.

Server Settings Options (Continued)	
Option	**Description**
Limit database connection inactive time	Use this option to limit the amount of time ColdFusion allows a cached database connection to remain inactive. This option is ignored if the option to maintain database connections has not been enabled for an individual data source.
Limit maximum number of cached queries	

When changing values on this page, be sure to stop and restart ColdFusion for these options to take affect. For more information on stopping and starting ColdFusion, see ../../Getting_Started_with_ColdFusion/contents.htm*Getting Started with ColdFusion*/a.

Configuring Administrator Security

Security options in ColdFusion have been greatly enhanced in this release. There are now two levels of security you can implement: Basic and Advanced. With Basic Security, a password secures access to the ColdFusion Administrator and to files, directories, and data sources from ColdFusion Studio. Knowing these passwords gives you complete access to all resources and the all ColdFusion Administrator pages.

Advanced Security allows you to authenticate individual users and associate specific access rights based on user login or group association. ColdFusion Advanced Security gives you the ability to enforce security at a very granular level. For example, you can define security domains and policies that allow you to secure specific areas of the ColdFusion Administrator or specific ColdFusion resources, including the execution of specific ColdFusion tags. This security framework allows you to authenticate individual users, and, once authenticated, control access to a wide range of operations, such as adding or deleting data sources, setting server performance options and so on.

ColdFusion Security has three different operational contexts:

- Runtime Security, where ColdFusion developers use the CFAUTHENTICATE tag to authenticate users accessing ColdFusion pages. Also, in situations where you are either hosting a ColdFusion application on your server, or deploying a ColdFusion application to a hosted server, all resources that fall within a specified directory location can be secured.
- Remote Development Security (RDS), where developers accessing ColdFusion resources from Studio are authenticated prior to receiving authorization to access these resources

- Administrator Security, where individual administrative operations, such as adding or removing a data source, changing ColdFusion server settings, or accessing security settings are secured against unauthorized access.

For detailed information about configuring security options in the ColdFusion Administrator, see Chapter 8, Configuring Basic Security

For information about advanced security in ColdFusion, see Chapter 9, Configuring Advanced Security.

For more information about implementing runtime security measures, refer to ../../Developing_Web_Apps/contents.htm*Developing Web Applications with ColdFusion*/a.

Managing Client Variables

ColdFusion 4.0 introduces a number of options designed to give you greater flexibility in managing client variables. Client variables in ColdFusion give you the ability to determine the identity of a client visiting your site. Identifying clients and customizing page content for users requires the ability to manage client state.

ColdFusion allows the following ways of managing client variables:

- Using the system Registry to store client variables
- Using browser cookies
- Using an external data source of your choice

Planning client state management

The method you choose to store client variables will depend on a number of factors. Among the most important factors is whether your site is currently using, or will be using server clustering to provide load balancing and fail-over support. In addition, there are a number of other factors to consider:

Client Variable Storage		
Storage Type	**Advantages**	**Disadvantages**
System registry	• Simple implementation • Good performance • Registry can be exported easily to other systems • Server-side control	• Need to be aware of the registry's maximum size limit as defined in the System Control Panel (Windows NT only) • Tied to the host system: Not practical for clustered servers or a round-robin DNS configuration

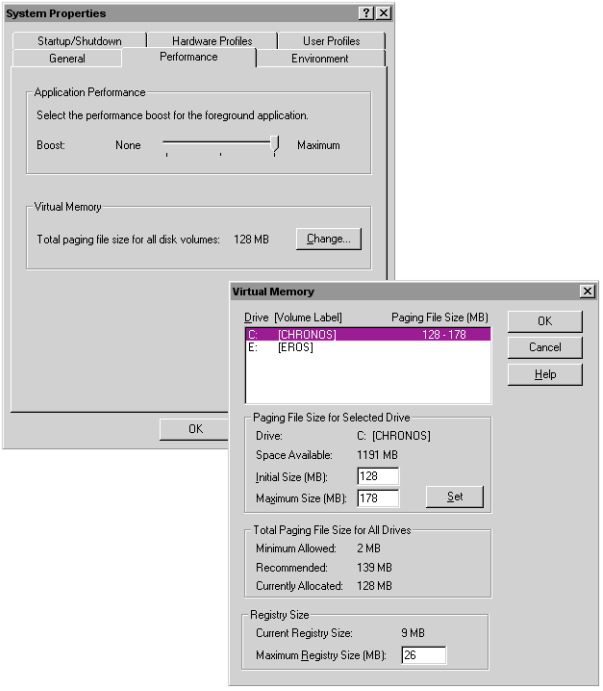
Client Variable Storage (Continued)		
Storage Type	**Advantages**	**Disadvantages**
Browser cookies	• Simple implementation • Good performance • Can be set to automatically expire • Client-side control	• Users can configure browsers to disallow cookies • ColdFusion limits individual cookie data to 4 KB • Netscape Navigator allows only 20 cookies from any one host; ColdFusion uses three cookies to store read-only data, leaving only 17 additional cookies available for use
External repository	• Can use existing data source • Portability: Not tied to a single server • OS portability in a mixed environment	• Requires database transaction to read/write variables • Somewhat more involved to implement

Increasing maximum registry size (Windows NT)

Windows NT notifies you if your registry data is approaching the limit defined for registry size in the System Properties dialog. If you receive this message, you can open the System Properties dialog and increase the minimum size of your system registry.

To increase maximum registry size:

1. Open the System Control Panel and click the Performance tab.
2. In the Virtual Memory group box, click the Change button to open the Virtual Memory dialog.



3. At the bottom of the dialog, the current registry size is reported. Specify a new maximum registry size in MB.

Checking registry size (UNIX)

Unlike Windows NT, ColdFusion for Solaris and HP-UX does not impose limits on the size of the registry. However, it's still a good idea to be aware of the size of your registry. Registry data is stored in the following file:

`<installdir>/coldfusion/.windu.hostname/windu_reg.dat`

State Management and Server Clustering

When using ClusterCATS for ColdFusion to cluster Web servers, and you want to use client variables, you must use an external repository to store client variables, since the system registry, which is bound to an individual system, can't be dynamically accessed by any other system.

Configuring a data source in a clustering environment

Like any other ColdFusion data source, the data source you specify to store your client variables can live anywhere on your network that is accessible to ColdFusion. When you add a new data source to ColdFusion for storing client variables (we recommend dedicating a data source for this purpose rather than using an existing data source) you can enable an option for ColdFusion to automatically create the tables necessary for storing client variables.

However, in a cluster of servers all accessing the same data source for client variables, ColdFusion only needs to create the necessary tables once. As you add the client variables data source to each ColdFusion Server in the cluster, you do not need to choose the option to have ColdFusion create the tables necessary to support client variables, since they have already been created when you added the data source for the first server in the cluster. If you inadvertently enable the option to automatically create client variable database tables, ColdFusion generates a SQL error.

For information about managing state in a clustered environment, see Managing State in a Clustered Environment .

Enabling External Client State Management

You enable client state management in the ColdFusion Server using the Administrator to specify a data source repository where you want to store client variables.

Although you can select and use an existing data source to store client variables, Allaire recommends creating a new data source specifically for the purpose of storing client variables. By separating data sources, you can more easily define security options for the data sources used in your ColdFusion environment.

When creating a new data source for client variables, you do not need to create any tables in the data source. ColdFusion automatically creates the tables necessary to store client variables.

To create a client variable data source:

1. Open the ColdFusion Administrator to the Data Sources page.
2. Enter a data source name in the text entry box and click Add.
3. In the Create Data Source page, enter information about the new data source location (path) as well as other options.

Excel and Text data sources do not appear as valid data sources for use in configuring an external client data source repository. Neither data source type supports the SQL required for the client variable repository. In addition, OLE DB data sources are not supported for use as a client data source repository.

4. Click Create to create the new data source.

To enable your client variable data source:

1. Open the ColdFusion Administrator to the Variables page, which is in the Server group.
2. Select the name of the data source you want to use for storing client variables in the drop down list box, and click Add.
3. On the Create Client Variable Storage page, select the options you want.

Client variable storage options

When you configure a data source for client variable storage, you have several options for configuring the data source:

- Purging variables older than a specified number of days
- Configuring global client variable updates
- Automatically creating tables in the client variable data source

Purge client variables

Ordinarily, you don't want to have client variables preserved indefinitely. ColdFusion allows you to set a limit to the length of time a client variable remains active. You can configure your client variable data source to expire client variables after some number of days you specify.

As an example of how this can be useful, take the case of an online store. A user adds items to his or her shopping basket, the details of which are stored as client variables in a ColdFusion data source, but never completes the transaction, instead, choosing to end the session. You want to be able to easily clear the contents of the shopping cart after some number of days. Enabling ColdFusion to purge clients can help keep your client variables data source from getting cluttered with data you don't need.

Disable global client variable updates

By default ColdFusion updates client variables for every page request. Use this option if you don't want ColdFusion to perform these updates. When updates are disabled, ColdFusion only updates global client variables when they are first created and when they are updated. Since updating global client variables for every page request requires a trip to the data source and back, disabling updates helps to improve the performance of your application pages.

Create client variable data source tables

Use this option to allow ColdFusion to create the tables necessary for client variables when you first configure the data source for this purpose. As you configure other servers in your cluster to use this client variables data source, be sure to disable the option for ColdFusion to create the necessary tables. If you inadvertently enable automatic table generation, ColdFusion generates a SQL error because it tries to create tables that already exist.

Migrating Client Variable Data

If you need to migrate your client variable data to another data source, you need to know the structure of the database tables used to store this information. Client variables stored externally use two small database tables with the following simple structure. Data types shown in these tables are those used for a Microsoft Access database. Your database may require different data types.

CDATA	
Column	**Data Type**
cfid	char(20)
app	char(64)
data	memo

CGLOBAL	
Column	**Data Type**
cfid	char(20)
data	memo
lvisit	date

Creating client variable tables

You can use the following example ColdFusion page as a model for creating client variable database tables in your own database. Not all databases support the same column data type names, so you may have to alter some data types for your database. Refer to your database documentation for the proper data type.

Sample table creation page

```
<!---- Create the Client variable storage
tables in a datasource. This example applies
to Microsoft Access databases --->

<CFQUERY NAME="data1" DATASOURCE="#DSN#">
CREATE TABLE CDATA
(
    cfid char(20),
    app char(64),
    data memo
)
</CFQUERY>

<CFQUERY NAME="data2" DATASOURCE="#DSN#">
    CREATE UNIQUE INDEX id1
    ON CDATA (cfid,app)
</CFQUERY>

<CFQUERY NAME="global1" DATASOURCE="#DSN#">
CREATE TABLE CGLOBAL
(
    cfid char(20),
    data memo,
    lvisit date
)
</CFQUERY>

<CFQUERY NAME="global2" DATASOURCE="#DSN#">
    CREATE INDEX id2
    ON CGLOBAL (cfid)
</CFQUERY>

<CFQUERY NAME="global2" DATASOURCE="#DSN#">
    CREATE INDEX id3
    ON CGLOBAL (lvisit)
</CFQUERY>
```

Enabling Application and Session Variables

Session and application variables are enabled with this option. These options override any individual use of the CFAPPLICATION tag to enabled application or session variables. If these variables are disabled in the Administrator, they cannot be used in any ColdFusion application.

Specifying timeouts

Use the Application Variables and Session Variables Maximum Timeout and Default Timeout settings to specify the lifespan for these variable types. The default timeout

for application variables is two days. The default timeout for session variables is 20 minutes.

Monitoring ColdFusion Performance

ColdFusion provides a set of counters for monitoring the performance of the ColdFusion Server. This allows you to use the Windows NT Performance Monitor administration utility to monitor ColdFusion performance. This enhancement to NT Performance Monitor is installed automatically by the ColdFusion setup.

ColdFusion counters available

ColdFusion supports 11 different counters you can enable in the Windows Performance Monitor:

- Average database transaction time
- Average queue time
- Average request time
- Bytes incoming per second
- Bytes outgoing per second
- Database hits per second
- Page hits per second
- Cache pops per second
- Number of queued requests
- Number of running requests
- Number of timed out requests

To enable the Performance Monitor for ColdFusion:

1. Open the ColdFusion Administrator to the Miscellaneous Debugging page.
2. Click the Enable performance monitoring option. The default is off.
3. Click Apply to save the new setting.

To configure the Performance Monitor:

1. From the Windows Start menu, select Programs > Administrative Tools > Performance Monitor.
2. In the Performance Monitor, select Edit > Add to Chart or File > Open to open an existing chart.

   In the Add to Chart dialog, select ColdFusion Server from the Object drop-down list. You can change any of the display options (Color, Scale, Width, Style) for a counter before adding it.

3. Click one or more selections in the Counters list, then click the Add button. The counters are listed at the bottom of the Chart View.
4. Click the Explain button to display embedded help for the selected counter.

ColdFusion Version Information

The Version Info Administrator page provides ColdFusion Server profile information. The values shown correspond to several ColdFusion server variables as follows:

Windows NT Server Information Variables	
Variable	**Description**
Server.ColdFusion.ProductName	Stores the ColdFusion product name, for example, **ColdFusion Engine**.
`Server.ColdFusion.ProductVersion`	Stores ColdFusion product release information, for example, **4,0,0,0**.
`Server.ColdFusion.ProductLevel`	Stores ColdFusion product level information, for example, **Professional**.
`Server.ColdFusion.SerialNumber`	Stores ColdFusion serial number information.
`Server.OS.Name`	Stores the server operating system name, for example, **Windows NT**.
`Server.OS.Version`	Stores the operating system version, for example, **4.0**.
`Server.OS.AdditionalInformation`	Stores additional information about the operating system, for example, **Service Pack 3**.
`Server.OS.BuildNumber`	Stores the build number of the host operating system, for example, **1381**.

Solaris version information

On Solaris, these server variables store slightly different information:

Solaris Server Information Variables	
Variable	**Description**
`Server.ColdFusion.ProductName`	Stores the ColdFusion product name, for example, **ColdFusion Engine**.
`Server.ColdFusion.ProductVersion`	Stores ColdFusion product release information, for example, **4, 0, 0, 0**.
`Server.ColdFusion.ProductLevel`	Stores ColdFusion product level information, for example, **Enterprise**.
`Server.ColdFusion.SerialNumber`	Stores ColdFusion serial number information.
`Server.OS.Name`	Stores the server operating system name, for example, **UNIX**.
`Server.OS.Version`	Stores the operating system version, for example, **5.5.1**.
`Server.OS.AdditionalInformation`	Stores additional information about the operating system, for example, **SunOS**.
`Server.OS.BuildNumber`	Stores the build number of the host operating system, for example, **Generic_103640-19**.

The ColdFusion Logging Page

ColdFusion generates log files you can use to help monitor ColdFusion server activity as well as activity in your ColdFusion applications. ColdFusion generates several different log files, most of which are written to `\Cfusion\Log` on Windows and `/opt/coldfusion/log` directory on Solaris. The Administrator mail error log is written to `\cfusion\Mail\Log` (Windows) and `/opt/coldfusion/mail/log` (Solaris). All log files are written in comma delimited format.

In addition to logging options, the Logging page contains a few other administrative options.

Administrator email address

When you enter an administrator's email address in the Administrator Logging page, this email address appears with any error messages generated by ColdFusion. This facility can help users report errors. Note that this email address can be overridden in the application framework page, `Application.cfm`.

Log directory

The default location for ColdFusion log files in Windows is `cfusion\log`. For Solaris, the default location is `opt/coldfusion/log`. You can specify a new location for ColdFusion log files by entering a new value in the Log Directory list box.

Log slow pages

ColdFusion allows you to track pages in your applications that take longer than a specified length of time to process. You can specify the amount of time ColdFusion allows before writing an entry to the `server.log` file.

Logging email messages

In addition to system logs, ColdFusion writes a log of errors generated by SMTP mail server used to post mail from ColdFusion applications. You can choose to log warning messages, information messages, or error messages.

In Windows, the mail log file is stored by default in `cfusion\mail\log`. On Solaris, the mail log file is stored by default in `/opt/coldfusion/mail/log`.

To enable email logging:

1. Open the ColdFusion Administrator to the Mail Logging page.
2. Select the error severity you want and click to enable the **Log all email messages** checkbox.
3. Click Apply to complete the operation.

Log files created by ColdFusion

ColdFusion creates nine different log files.

ColdFusion Log Files	
Log Filename	**Description**
`exec.log`	Logs problems with the ColdFusion Server service. If the ColdFusion service hangs or if the service was unable to access the system registry, that information is written to `cfexec.log`.
`rdseservice.log`	Logs errors occurring in the ColdFusion RDS service, which provides file, debugging, directory, and database browsing services for ColdFusion Studio.
`application.log`	Logs every ColdFusion error reported back to a user. All application page errors, including ColdFusion syntax errors, ODBC errors, and SQL errors, are written to this log file. Every error message that is displayed on a user's browser is logged here, along with the visitor's IP address and browser information, if possible.
`webserver.log`	Logs errors occurring in the Web server and the ColdFusion stub.
`schedule.log`	Logs scheduled events that have executed. Indicates whether the event succeeded, provides the scheduled page URL, the date and time executed and a task ID.
`server.log`	Logs errors that occurred in the communication between ColdFusion and your Web server. This file is meant primarily to help Allaire Technical Support personnel.
`customtag.log`	Logs errors generated in custom tag processing.
`remote.log`	The Network Listener Module (NLM) writes various messages to the `remote.log` file relating to a distributed ColdFusion configuration.
`errors.log`	Logs errors generated in attempts to send mail from ColdFusion applications. Stored in `cfusion\mail\log` (Windows) or `/opt/coldfusion/mail/log` (Solaris).

Log file format

All ColdFusion log files share the same comma-delimited format consisting of five separate fields as follows:

ColdFusion Log File Format		
Field	**Field**	**Description**
1	Severity	"Information," "Warning," or "Error."
2	Thread ID	Service Thread ID. This information is only useful to Allaire Technical Support personnel.
3	Date	Date that the error occurred.
4	Time	Time that the error occurred.
5	Details	Description of the error (with error number, if appropriate).

Mapping Directories

The Mappings page in the ColdFusion Administrator allows you to create logical aliases for physical directories on your server. Mapping directories is only necessary if you want to use ColdFusion with CGI or if you want to use absolute references to ColdFusion pages with the CFINCLUDE tag.

For information about using ColdFusion with CGI instead of one of the standard Web server APIs (NSAPI, ISAPI, Apache API, or WSAPI), see Chapter 7, Using CGI with ColdFusion.

The Web server APIs supported by ColdFusion (NSAPI, ISAPI, Apache API, and WSAPI) perform document type mapping, which makes directory mapping in ColdFusion unnecessary. When a browser loads a file with the `.cfm` extension, the Web server recognizes that file type as a ColdFusion application page.

Using the Extensions Pages

Use the ColdFusion Administrator Extensions pages to register Java applets and CFX tags, custom tags built with C++.

Managing CFX tags

The CFX Tags page in the ColdFusion Administrator is used to Register and manage ColdFusion custom tags built with C++.

ColdFusion allows you to build extensions or custom tags in two ways:

- Using C++ to code DLLs (Windows) or shared objects (Solaris) that provide a custom tag you can use in your application pages.
- Using CFML to create custom tags you invoke in your application pages.

To use a CFX tag you must first register it with ColdFusion. This process simply tells ColdFusion where to find the required DLL when it attempts to process the CFX tag in an application page.

Note A wide variety of custom tags of both types is available from the http://www.allaire.com/taggalleryColdFusion Tag Gallery/a.

CFX tag samples

Source code and compiled versions of two sample CFX tags are installed with ColdFusion (you can register and use them in your application pages). You must first compile this code before registering the DLLs or shared objects in the ColdFusion Administrator. These examples can be found in `opt/coldfusion/cfx/examples` (Solaris) and `cfusion\cfx\examples` (Windows).

The two CFX tag examples installed with ColdFusion are as follows:

- `directorylist` — Returns a directory listing.
- `ntuser_db` — (Windows NT only) Allows you to modify Windows NT user permissions.

To register a CFX tag:

1. Open the CFX Tags page in the ColdFusion Administrator.
2. Enter a name for the CFX tag you are adding. Tag names must be prefixed with `CFX_`.
3. Click Add to open the New CFX Tag page.
4. Enter the path to the library you want to use or browse your system to locate the library you want to use.
5. Enter the procedure that implements the tag. The procedure name must correspond with an existing procedure in the DLL or shared object you've specified. Procedure names are case-sensitive.
6. Click Keep library loaded to prevent reloading the library into memory each time a referenced page is accessed.
7. Enter a description and click Add to finish.

Registering a Java applet

The Applets page in ColdFusion allows you to register Java applets for use in ColdFusion forms with the CFAPPLET tag. Registering the applet before using it in ColdFusion applications allows you to encapsulate the applet in a simple, easy-to-use

interface. The CFAPPLET tag you use to place the applet can be used to override any parameters you define in the Administrator Registered Applets page.

Before you can use CFAPPLET to place a Java applet in your CFFORM, you must register the applet in the ColdFusion Administrator.

Applets Administrator page

You can use the CFAPPLET tag to place Java applets in a CFFORM. However, before you can use the tag you need to register your applet using the ColdFusion Administrator. Once your applet is registered with ColdFusion, using the CFAPPLET tag in your code is very simple since all parameters are predefined in the Administrator. Since parameters are predefined in the Administrator, you only need to specify parameter values you want to override for a particular instance. With CFAPPLET, you could enter just the applet source and the form variable name you want to use:

```
<CFAPPLET APPLETSOURCE="Calculator"
    NAME="calc_value">
```

You can define all other parameters when you register the applet in the Administrator. Using the HTML APPLET tag, you'd have to invoke all the applet's parameters every time you wanted to use it in an page.

The new Registered Applets page in the ColdFusion Administrator allows you to register Java applets you want to place in your ColdFusion pages with the CFAPPLET tag.

To register a Java applet:

1. Install the Java class files and any other files required for the class. You'll need to specify the codebase argument when registering the applet, so take note of the installed path.
2. In the ColdFusion Administrator, open the Register New Applet page by clicking the Applets button.
3. Enter the necessary information. Each field corresponds to values you would enter in the HTML APPLET tag.
4. Enter the parameter name and value pairs required for your applet. If necessary, you may need to refer to whatever documentation exists for your applet.
5. When you're done, click Create.

Applet registration fields are explained in the following table.

Java Applet Registration Fields	
Field	**Description**
Codebase	Enter the base URL of the applet: the directory that contains the applet components. The applet class files must be located within the Web browser root directory. Example: `http://servername/classes`
Code	This is the name of the file that contains the applet subclass. The filename is relative to the codebase URL. The *.class file extension is not required.
Method	Enter the method name in the applet that returns a string value. You use this method name in the NAME attribute of the CFAPPLET tag to populate a form variable with the method's value. If the applet has no method, leave this field blank.
Height	Enter a measurement in pixels for the vertical space for the applet.
Width	Enter a measurement in pixels for the horizontal space for the applet.
Vspace	Enter a measurement in pixels for the space above and below the applet.
Hspace	Enter a measurement in pixels for the space on each side of the applet.
Align	Choose the alignment you want.
Java Not Supported Message	This message is displayed by browsers that do not support Java applets. If you want to override this message, you specify a different message in the CFAPPLET tag NOTSUPPORTED attribute.
Parameter Name	Enter a name for a required applet parameter. Your Java applet will typically provide the parameter name needed to use the applet. Enter each parameter in a separate parameter field.
Value	For every parameter you enter, define a default value. Your applet documentation will provide guidelines on valid entries.

ColdFusion Administrator Debugging Options

ColdFusion can provide important debugging information for every application page requested by a browser. When enabled, debug output is shown in a block following normal page output. The debug output can help you track down programming problems.

There are also important runtime debugging options available in ColdFusion Studio. For more information about these options, such as setting breakpoints, see ../../Developing_Web_Apps/contents.htm*Developing Web Applications with ColdFusion.*/a

You can select from the following debug output options:

- Show variables
- Show processing time
- Show SQL and data source name
- Show query information

Note By default, when you enable any of these options, debug output becomes visible to all users. You can, however, restrict debug output to a selected IP address.

To restrict debug output to a specific IP number:

1. Enter the IP number you want to receive debug output, and click Add. Debug output will be visible only to the specified IP address.
2. To disable debug output to a specific IP address, select the address and click Remove.

If debugging output options have been selected and no IP address specified, debug output will be displayed to all users.

Configuring Administrator Mail

You use the ColdFusion Administrator Mail page to specify a mail server to handle sending automated mail messages from the server.

Enter a valid mail server (either a mail server name or IP address) as well as a server port number and connection timeout.

To verify that your mail server connection works, you can send a test message.

Indexing Data with Verity

The Verity Search'97 indexing and searching technology, which has been incorporated into ColdFusion, provides a means for creating collections of indexed data optimized for fast retrieval.

To use Verity searching and indexing technology you:

1. Create a Verity collection using the ColdFusion Administrator Verity page or using the CFCOLLECTION tag at runtime.
2. Populate a collection with data using options on the ColdFusion Administrator Verity page to index specific directories, or using the CFINDEX tag at runtime.
3. Build searching and indexing capability using the CFINDEX and CFSEARCH tags into your application.

For more information about populating and searching Verity collections using the CFINDEX and CFSEARCH tags, see ../../Developing_Web_Apps/contents.htm*Developing Web Applications with ColdFusion*/a.

Using the Verity Collections page

The Verity Collections page in the Administrator provides a means for creating collections. Collections can also be created and populated externally using native Verity tools. See your Verity documentation for more information about using native Verity tools.

Use the Verity Collections page to:

- Create and name collections
- Populate a collection with text file data from a specified directory.
- Purge, repair, optimize, delete, or update a collection.

Creating a collection

Before you can search collections using the CFSEARCH tag in your ColdFusion application, you must first create the collection and then populate it with data.

To create a collection, follow these steps:

1. Open the Administrator Verity page.
2. Enter a name for your collection.
3. If necessary, specify a path for the collection.
4. Select a language from the drop down list box.
5. Click Create.

Now, you can populate the collection with data.

Populating a collection

Once you've created a collection, you can populate it with data from text and binary files in a directory you specify. Data from a ColdFusion query can only be indexed using the ColdFusion CFINDEX tag in a ColdFusion application page.

Verity indexes all supported file types found in the target directory. See Verity Supported File Types for more information.

Verity Supported File Types

The ColdFusion Verity implementation supports a wide array of document types. This means you can index Web pages, ColdFusion applications, and many binary document types and produce search results that include summaries of these documents.

The following table lists the supported document types.

Supported Document Types	
Documents	**Versions**
Text files	
HTML, CFML, DBM, SGML, XML,	N/A
ANSI, ASCII, Plain Text	N/A
Word processors	
Adobe Acrobat (PDF)	All
Adobe FrameMaker (MIF)	All
Aplix Words	4.2
Corel WordPerfect for Windows	5.x 6, 7, 8
Corel WordPerfect for Macintosh	2, 3
Lotus AMI Pro	2, 3
Lotus AMI Pro Write Plus	all
Lotus Word Pro	96, 97
Microsoft Office	95, 97
MS Rich Text Format (RTF)	1.x, 2.0
MS Word for Windows	2, 6, 95, 97
MS Word for DOS	4, 5, 6
MS Word for Macintosh	4.0, 5.0, 6.0
MS Notepad, WordPad	all
MS Write, MS Works	all
XYWrite	4.12
Spreadsheets	

Supported Document Types (Continued)	
Documents	**Versions**
Corel QuattroPro	7, 8
Lotus 1-2-3 for DOS/Windows	2.0, 3.0, 4.0, 5.0, '96, '97
Lotus 1-2-3 for OS/2	2
MS Excel	3, 4, 5, '95, '97
MS Works	all
Presentation	
Corel Presentations	7.0, 8.0
Lotus Freelance	96, 97
MS PowerPoint	4.0, 95, 97

To create an index of data from a directory:

1. Create a collection in the Administrator.
2. If not already selected in the list of collections, select the collection you want to populate and click Index.
3. Edit the list of file extensions, if necessary.
4. Enter a directory path you want to index in the form:
5. Enter a URL to return for documents returned in a search operation against this collection. For example, if you are indexing the ColdFusion documentation directory and subdirectories, the directory you index could be `c:\inetpub\wwwroot\cfdocs`. You would enter the return URL as:

   `http://my_server/cfdocs/`
6. Click Index. ColdFusion populates the collection with data from the specified directory.

Note that Verity collections, including those that index query data, can be created using the CFCOLLECTION tag, and can be populated using the CFINDEX tag in your ColdFusion application pages.

Repairing, Optimizing, Purging, and Deleting Collections

Verity collections that return erroneous data or have other problems can often be repaired using the Repair and Optimize feature in the Verity page of the ColdFusion Administrator.

When you need to clear a collection of data, use the Purge feature to delete the contents of the collection without deleting the collection itself.

Warning! A limitation in the Verity implementation may cause problems if you repair a Verity collection and then attempt another action such as a Purge before the repair has completed processing. In the event that a problem does occur, you should delete the affected collection, re-create it, and then re-populate the collection with the original data.

The safest approach is this: During a repair, NO OTHER ACTION should be taken.

Using ColdFusion in a Distributed Configuration

ColdFusion 4.0 can be configured in a distributed manner where the ColdFusion engine is running on a separate computer from the Web server. Running ColdFusion in this way might be called distributed or remote ColdFusion.

To run distributed ColdFusion, you must make the following changes to a standard installation:

- On the Web server side, you must notify the ColdFusion Web server plug-in that you want it to talk to a ColdFusion engine on another machine. You do this simply by making appropriate entries in an INI file.
- On the ColdFusion engine side, you must run an additional piece of software, known as the Network Listener Module, that listens for incoming ColdFusion requests and forwards them to the ColdFusion engine running on that machine. The ColdFusion engine itself is a standard release version of the engine with no special modifications to accommodate remoting.

In addition to allowing the ColdFusion engine to be located on a separate machine from the Web server, distributed ColdFusion provides the following unique capabilities:

- It allows the machine hosting the Web server to potentially be of a different architecture from the machine hosting the ColdFusion engine.
- It allows more than one Web server to be served by the same ColdFusion engine.

To provide some degree of security for the data being transferred between the Web server and the ColdFusion engine, that conversation is encrypted using a standard, 56-bit DES encryption algorithm.

Although it's possible for a ColdFusion engine to simultaneously service both local and remote requests, it is not possible for a single Web server to simultaneously dispatch both local and remote ColdFusion requests. When starting up, the ColdFusion Web server plug-in determines if it's to run in local or remote mode and remains in that mode until it's shutdown.

Distributed ColdFusion and clustering

The distributed ColdFusion configuration is not supported when ColdFusion is also configured for clustering. The reason is that the clustering component in ColdFusion,

which runs as part of the Web server, needs to be able to communicate with the ColdFusion engine. This arrangement assumes that the ColdFusion engine and the Web server are on the same machine, which is not necessarily the case in a clustered environment.

Changes in the 4.0 version

Remoting capabilities similar to what are now available in ColdFusion 4.0 were first provided as a special, add-on feature of ColdFusion 3.1.1. It was not possible to run the standard, release version of ColdFusion 3.1.1 in this manner. To do so, it was necessary to purchase and install special versions of the ColdFusion Web server plug-in modules on the Web server side and a separate listener module on the ColdFusion engine side. In ColdFusion 4.0 all the necessary pieces are provided as part of the standard distribution. All the supported Web server plug-ins have been enhanced to include the capability to send and receive ColdFusion data via TCP/IP, and the engine-side listener module is available as part of the standard release.

Configuring Distributed ColdFusion

Before trying to run ColdFusion in a distributed configuration, you must perform a standard installation of ColdFusion on all the machines involved. On the computer running the Web server, this guarantees that the ColdFusion server plug-ins are correctly loaded by the Web server. On the computer running the ColdFusion engine, this guarantees that the engine is set up and operating correctly.

Having complete, standard installations of ColdFusion available on all machines also provides a useful baseline environment so that validation can be done in the absence of the remote extensions. Should problems arise using ColdFusion in remote mode, it's possible to run ColdFusion locally to determine whether or not the problems are related to the distributed configuration.

If, after successfully testing your remote configuration, you wish, for security reasons, to disable the ColdFusion engine installed on the computer hosting the Web server, you can do this easily by renaming the following executable files in the `cfusion/bin` (Windows) `coldfusion/bin` (Solaris) directory:

- `cfserver`
- `cfrdsservice`
- `cfexec`

This prevents any ColdFusion server-side process from running while generally preserving your ColdFusion configuration.

Using the modified plug-in

In ColdFusion 4.0 all the Web server plug-ins are remote-capable so no special installation is required. All you need to do is let the plug-in know that you want to run in remote mode. You do this by putting the following information in an INI file and

putting that file in the root directory of your ColdFusion installation on the machine running the Web server. That INI file must be named `cfremote.ini`. To enhance security, this INI file may be optionally set to be automatically deleted after being read at startup.

Here is a sample of the INI file with comments explaining what the various fields do. This sample may be cut and pasted and used as a template to get started.

```
;-------------------------------------------------------------------
;
; Sample INI file for ColdFusion Remoting.
;
; Place this file in the root directory of your ColdFusion installation.
; It must be named "cfremote.ini".
;
; !IMPORTANT! * All values (the strings on the right hand side of
;               the equals sign) must be quoted using double
;               quotes.
;             * All info is case insensitive..
;             * Lines beginning with a semicolon are treated as
;               comments and are ignored.
;

; Use this to turn on/off the remoting capability.
;
; Valid values: Yes, No.
;
REMOTING = "YES"


; Use this to specify the IP address of the remote computer running
; the ColdFusion Server.
;
; Valid values: a valid IP address, e.g.: 139.56.205.102.
;
IP = "205.181.21.61"

; Use this to specify the port on that computer on which the remote
; ColdFusion Network Listener Module is listening.
;
; Valid values: a valid port number (integer).
;
PORT = "1234"

; Use this to specify that the data sent between the machine running
; the Web server and the machine running the ColdFusion Application
; Server be encrypted.
;
; Valid values: Yes, No.
;
ENCRYPTION = "YES"

; Use this to specify the key used to encrypt the data.
;
```

```
; Valid values: any string of up to 127 ASCII chars.
;
KEY = "doglips"

; Use this to have this INI file be deleted after it is read at
; startup. (This is a security feature as it keeps your key from
; being read by others.)
;
; Valid values: Yes, No.
;
DELETE = "NO"

; Use this to write a message to the ColdFusion "webserver.log"
confirming that
; remoting is active and what startup parameters (except the encryption
; key) were used.
;
; Valid values: Yes, No.
;
MESSAGE = "YES"
;
;-------------------------------------------------------------------
```

As with all warning and error messages from any of the ColdFusion Web server plug-ins, such text is written to the ColdFusion log file `webserver.log` in the log subdirectory of the directory into which you installed ColdFusion (on the machine hosting the Web server.) This file should be the first place you look if you encounter problems running ColdFusion in a distributed configuration since, for a variety of practical and security reasons, ColdFusion will not run in distributed mode if any information in the INI file is missing or incomplete.

The Network Listener Module (NLM)

The NLM is a stand-alone program that acts as a network front-end for the standard ColdFusion Server. It runs on the same computer on which the ColdFusion Server is running. It listens for incoming requests via TCP/IP and forwards them on to the local ColdFusion Server. The ColdFusion Server then processes those requests, returning the results to the listener module which, in turn, returns them via the original TCP/IP connection. It is a silent, background process with no user interaction. On NT, it runs as an NT service. On UNIX, it runs as a daemon. For debugging or other special purposes, it may also be run as a command line program by specifying the appropriate command line option (-i) at startup.

Installing the module on Windows NT

On NT, the module consists of a single executable file, `cfdist.exe`. Before you can run the listener as an NT service, you must perform the following installation step.

To install the network listener module as a service:

1. Run the listener with the following special command line argument:

```
cfdist.exe -sINSTALL
```

2. If installation was successful, it should now appear on your Services list under the name ColdFusion NetListener. If it doesn't show up, look in the module's log file, `distributed.log` in the log subdirectory of your ColdFusion installation, for information about why the install failed.

Note Once you've installed the module as an NT service you cannot move the executable file unless you uninstall and reinstall it in its new location.

Once installed as a service, you can start, stop, pause or continue the listener's operation as you would any NT service. You can start or stop the listener independent of any of the other ColdFusion services although, of course, the listener must be running to receive remote network requests. Note that when starting the service (from the NT Services Control Panel applet), you will need to specify -p switch and possibly the -k switch in the Startup Parameters box in the Services applet.

Please refer to the list of command line options below.

To uninstall the listener

Invoke `cfdist.exe` with the `-sREMOVE` command line option. Notice of successful removal will be written to the listener log.

Installing the module on UNIX

On UNIX, the listener module consists of a single executable file, in this case named simply `cfdist`. It is not necessary to perform any special installation step on UNIX.

To start the listener as a daemon:

Type the executable's name (without the -i switch) and the process will start. Because it's running as a daemon, the command will return immediately having launched the process in the background. You will probably use at least the -p switch when starting the daemon.

Please refer to the list of command line options below.

To stop the daemon process:

You need to kill it by its process ID. Use the `ps` command to get the PID and then kill the process as demonstrated below.

```
ps -deaf  | grep cfdist | grep -v grep
```

It returns the PID in a string something like:

```
ckintzin   980     1  0 15:48:12 ?        0:00 cfdist
```

The first number is the PID. Use it in the kill command to stop the process:

```
kill -INT 980
```

Repeating the `ps` command should now return nothing, indicating the process is now dead.

Listener Module Command Line Options

The Network Listener Module (NLM) executable, `cfdist` (`cfdist.exe` on Windows NT) takes the following command line options at startup. Of these options, you'll probably only use the -p option on a regular basis.

Listener Module Command Line Options	
Option	**Description**
-v	Verbose. This option prints out confirmation of the command line options in use, and on what port the program is running. It also prints information about each connection that comes in. This can be useful to confirm that requests are, indeed, reaching the remote computer.
-p*nnnn*	Port number where *nnnn* is the port number. If no port number is specified, the program automatically selects an unused port on which to run. In most cases, you use this option to guarantee that you're using the same port as the remote Web server.
-i	Interactive. Run from a command line not as a daemon/service. In order for verbose commentary to appear on the terminal, you must be running in interactive mode. Aside from the display of debugging output, however, there is no difference in operation between running the program from a command line or running it as a daemon/service.
-r	Reuse. (UNIX Only) If the specified port appears to be in use, try to use it anyway. Sometimes TCP/IP connections don't get closed down immediately. In those cases the connections can take a few minutes to timeout and close down. Unfortunately, these lingering connections will prevent the program from restarting on the same port because it thinks that port is in use. To overcome this and allow you to restart without waiting or switching to another port, you can use this option. Be careful, however, not to use this option indiscriminately as it could result in multiple versions of the listener running at the same time.
-k*xxxx*	Key for encryption. (where *xxxx* is the string used as the key) The key may be any string of printable ASCII chars up to 127 characters long.
-sINSTALL	Setup, install-mode. (NT Only) Install the process as an NT service. Its service name will be ColdFusion NetListener.
-sREMOVE	Setup, remove-mode. (NT Only) Uninstall the service.

The program will print out a list of available options along with a brief description of their purpose anytime you enter an unknown option at the command line.

Using the INI file to specify startup options

It is also possible to specify startup options for the listener in an INI file. This INI file is similar to the INI file required on the Web server side, but is available on the ColdFusion engine side as a convenience (since all the required information may be supplied as command line options at startup time.) Below is a template for this INI file. If used, it must be placed in the root directory of your ColdFusion installation (on the machine hosting the ColdFusion engine), and it must be named `cfdist.ini`. To enhance security, this INI file may be optionally set to be automatically deleted after being read at startup.

```
;-------------------------------------------------------------------
;
; Sample INI file for CFDist (AKA the "ColdFusion Listener Module").
;
; Place this file in the root directory of your ColdFusion installation.
; It must be named "cfdist.ini"
;
; !IMPORTANT! * All values (the strings on the right hand side of
;               the equals sign) must be quoted using double
;               quotes.
;             * All info is case insensitive..
;             * Lines beginning with a semicolon are treated as
;               comments and are ignored.
;

; Use this to specify the port at which to listen for incoming ColdFusion
; requests
;
; Valid values: a valid port number (integer).
;
PORT = "1234"

; Use this to specify that the data sent between the machine running
; the Web server and the machine running this program be encrypted.
;
; Valid values: Yes, No.
;
ENCRYPTION = "YES"

; Use this to specify the key used to encrypt the data.
;
; Valid values: any string of up to 127 ASCII chars.
;
KEY = "doglips"

; Use this to have this INI file be deleted after it is read at
; startup. (This is a security feature as it keeps your key from
; being read by others.)
;
; Valid values: Yes, No.
;
DELETE = "NO"
```

```
; Use this to write a message to the ColdFusion "remote.log" confirming
that
; remoting is active and what startup parameters (except the encryption
; key) were used.
;
; Valid values: Yes, No.
;
MESSAGE = "YES"
;
;-------------------------------------------------------------------
```

The listener also writes various informative messages to the `remote.log` file in the log subdirectory of your ColdFusion installation (on the machine hosting the ColdFusion engine.)

CHAPTER 4

Managing Data Sources

ColdFusion uses ODBC to communicate with a wide range of databases. Before you can use a database in a ColdFusion application, you must register the ODBC data source in the ColdFusion Administrator.

Contents

About ColdFusion Data Sources

Before a database can be used with a ColdFusion application, it must be configured as a ColdFusion data source. You do this using the ColdFusion Administrator, Data Sources page. The specific databases you can configure for ColdFusion depend on the platform on which ColdFusion Server is installed and on whether you're running ColdFusion Server Workgroup, Professional, or Enterprise editions.

Databases supported by ColdFusion

ColdFusion uses ODBC to interact with data sources. In addition, two native database drivers are available for configuring Oracle 7.3 and 8.0 databases, and Sybase System 11 databases. However, not all ColdFusion Server editions support all database types. The following table describes database support in ColdFusion Server.

Databases Supported by ColdFusion	
ColdFusion Edition	**Databases Supported**
Workgroup	Desktop databases through ODBC: • Microsoft Access • Microsoft FoxPro • Inprise (Borland) dBase • Inprise Paradox • Lotus Approach • ASCII text • Microsoft Excel
Professional	All ODBC data sources OLE DB data sources (Windows only)
Enterprise	All ODBC data sources OLE DB data sources (Windows only) Sybase System 11 and Oracle 7.3 and 8.0 through native database drivers (Solaris and Windows NT)

Configuring ODBC Data Sources for Windows

Although you can use any valid ODBC data source on your system as a ColdFusion data source, creating, or registering, the data source in ColdFusion allows you to use the extended options available through ColdFusion. Valid ODBC data sources already on your system are available to your ColdFusion pages, but unless they are registered

with ColdFusion they cannot be configured with ColdFusion-specific options. For more information see “ColdFusion Settings” on page 67.

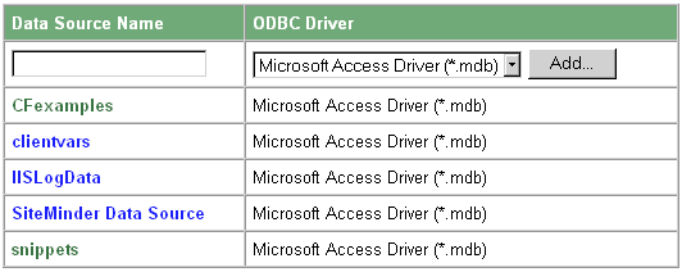
To add an ODBC data source to ColdFusion:

1. Open the ColdFusion Administrator by clicking on the ColdFusion Administrator icon in the ColdFusion program group (Windows) or by opening the Administrator URL:

   `http://hostname/CFIDE/administrator/index.cfm`

   The Administrator opens by default on the Server Settings page.

2. Click the ODBC link under the Data Sources label. The ODBC Data Sources page appears.



3. Enter a name for the new data source and select an ODBC driver from the drop down list. Click Add.

Note When naming a ColdFusion data source, do not use the following names: Registry or Cookie.

4. At the Create ODBC Data Source page, enter information about the new data source.

   For information about ODBC for specific data source types, see “ODBC Data Source Options (Windows)” on page 55 or “ODBC Data Source Options (Solaris)” on page 61.

5. If you make edits to the data source settings, click the Update button to save those changes.

6. Click the CF Settings button to access a number of ColdFusion-related ODBC options. For more information about these ColdFusion settings, see “ColdFusion Settings” on page 67.

7. Click the Verify Data Source link in the Administrator navigation bar to verify your data source. See “Verifying ColdFusion Data Sources” on page 74.

ODBC Data Source Options (Windows)

When creating or updating an ODBC data source, you use the Create ODBC Data Source page in the Administrator. This page offers a number of options for configuring

your ODBC data source. The options visible on the ODBC Data Source page vary based on the database driver being used.

For information about driver-specific options, refer to the following sources of information:

- Your database documentation
- ODBC driver documentation, including help files you may have on your system (check `\winnt\system32\*.hlp`)

Microsoft SQL Server ODBC options

ColdFusion ODBC options for Microsoft SQL Server data sources are described in the following table.

Microsoft SQL Server ODBC Options	
Option	**Description**
Data Source Name	A name for your ODBC data source.
Description	Descriptive information about the data source.
Server	The name of the server hosting the database you want to use.
	Use Trusted Connection — Allows SQL Server to authenticate on the user's Windows NT login. You can use this option if the SQL Server database is using an Integrated or Mixed security mode. Integrated security uses NT authentication schemes for all connections. Only trusted connections are allowed to connect to SQL Server. It's not necessary to populate the ColdFusion username and password fields because SQL Server ignores these values. Mixed security allows both trusted and nontrusted connections. If the username and password are left blank, SQL Server will use NT domain credentials. However, if you do pass a username and password, SQL Server tries to authenticate using the passed information.

Microsoft SQL Server ODBC Options (Continued)	
Option	**Description**
Login Info	Database — The name of the SQL Server database.
	Language — The national language used by SQL Server.
	Generate Stored Procedure for Prepared Statement — Stored procedures are created for prepared statements when this option is selected. The SQL Server driver prepares a statement by placing it in a procedure and compiling that procedure.
Translation	Convert OEM to ANSI characters — If the SQL Server client computer and SQL Server are using the same non-ANSI character set, select this option. For example, if SQL Server uses code page 850 and this client computer uses code page 850 for the OEM code page, selecting this option will ensure that extended characters stored in the database are properly converted to ANSI for use by Windows-based applications.

dBase ODBC Options

ColdFusion ODBC options for dBase data sources are described in the following table.

dBase ODBC Options	
Option	**Description**
Data Source Name	A name for your ODBC data source.
Description	Descriptive information about the data source.
Database Directory	The path dBase database you want to use as an ODBC data source.
Database Version	Enter the version number of the dBase database you want to use. ColdFusion supports dBase versions III, IV, and 5.0.
Driver Settings	Collating Sequence — Select the collating sequence you want to use. The collating sequence determines the sequence in which the fields are sorted.
	Page Timeout — Specifies the period of time, in tenths of a second, that a page (if not used) remains in the buffer before being removed.

Microsoft Access ODBC options

ColdFusion ODBC options for Microsoft Access data sources are described in the following table.

Microsoft Access ODBC Options	
Option	**Description**
Data Source Name	A name for your ODBC data source.
Description	Descriptive information about the data source.
Database File	Click the Browse button to select a database file for a file-based ODBC data source.
System Database	Specify a database file to make it accessible to the system or any user, rather than the local user. Note that Access data sources created with ColdFusion and specified as a Database File are automatically created as System Databases.
Driver Settings	Page Timeout — The length of time in milliseconds before a request for a ColdFusion page times out.
	Buffer Size — The total number of bytes ColdFusion uses to cache application pages. To optimize ColdFusion performance, enter a value.
Default Login	A username/password combination ColdFusion uses to access the data source. If your ODBC data source requires a username or password, enter them here. To verify your data source, you need to enter login information here.

Microsoft Excel ODBC options

ColdFusion ODBC options for Microsoft Excel data sources are described in the following table.

Microsoft Excel ODBC Options	
Option	**Description**
Data Source Name	A name for your ODBC data source.
Description	Descriptive information about the data source.
Workbook/Directory	The path and filename of the Excel workbook you want to use as the ODBC data source.

Microsoft Excel ODBC Options	
Option	**Description**
Version	Enter the version number of the Excel workbook you want to use. ColdFusion supports Excel versions 3.4, 4.0, and 5.0.
Driver Settings	Rows to Scan — The number of rows to scan to determine the data type of each column. The data type is determined given the maximum number of kinds of data found. If data is encountered that does not match the data type guessed for the column, the data type will be returned as a NULL value. Enter a number from 1 to 16 for the rows to scan. The value defaults to 8; if it is set to 0, all rows are scanned. A number outside the limit will return an error.

Microsoft Text ODBC options

ColdFusion ODBC options for Microsoft Excel data sources are described in the following table.

Microsoft Text ODBC Options	
Option	**Description**
Data Source Name	A name for your ODBC data source.
Description	Descriptive information about the data source.
Database Directory	The directory where the text files are found.
Extensions List	Lists the file name extensions of the text files on the data source. To use all files in the directory, enter *.*. To use only those files with certain extensions, add each extension you want to use.

Configuring ODBC Data Sources for Solaris

ColdFusion Application Server for Solaris (Enterprise edition) supports ODBC 3.0. Intersolv documentation on the ODBC 3.0 drivers can be found in:

```
<installdir>/odbc/doc/odbchelp.pdf
```

This is an Adobe Acrobat file. You can download the Acrobat reader from the Adobe Acrobat web site, http://www.adobe.com.

The following drivers are available:

Solaris ODBC Drivers and Data Sources	
Type	**Supports**
dBase/FoxPro	dBase IV and V files, and FoxPro files version 3.0
IBM DB2/6000	DB2/6000, DB2 v.5
INFORMIX	INFORMIX 7.x or 9.x via INFORMIX-Connect 9.13
OpenIngres	CA-OpenIngres 1.x, 2.x
Oracle	Oracle 7.x and 8
Sybase 11	Sybase driver for System 11 clients (threaded)
Text	ASCII text files

Configuring data sources for ColdFusion involves modifying the `<installdir>/odbc/odbc.ini file`. The `odbc.ini` file provides a means for mapping a data source name (DSN) to a particular ODBC driver. The ColdFusion Administrator can make these changes via a web browser based facility. In addition, this facility provides an interface to change ColdFusion specific settings for a data source, such as login and timeout info.

To add a data source for ColdFusion:

1. Open the ColdFusion Administrator.
2. Click the Data Sources label.
3. Enter the name of the Data Source you want to add and select the appropriate driver from the pull-down list.

   When naming a ColdFusion data source, do not use the following names: Registry or Cookie.
4. Click the Add button.
5. Enter the ODBC options you want, such as the database you want to use, and a description of the data source and click Create.
6. To set any environment variables your database client library may require, edit the ColdFusion start script found in `<installdir>/coldfusion/bin`.

For information about particular database drivers, refer to the Intersolv ODBC documentation, distributed as an Acrobat file in:

`<installdir>/coldfusion/odbc/doc/odbchelp.pdf`

ODBC Data Source Options (Solaris)

When creating or updating an ODBC data source, you use the Create ODBC Data Source page in the Administrator. This page offers a number of options for configuring your ODBC data source. The options visible on the ODBC Data Source page vary based on the database driver being used.

For information about driver-specific options, refer to the following sources of information:

- Your database documentation.
- An Adobe Acrobat file is provided in `<installdir>/odbc/doc/odbchelp.pdf`.

ODBC drivers on Solaris are supplied by Intersolv.

Note On Solaris, you need to edit the `coldfusion/bin/start` script to include the database variable, for example, `ORACLE_HOME`, `SYBASE`, or `INFORMIXDIR` and the library path set in `LD_LIBRARY_PATH`.

Intersolv dBase/FoxPro ODBC options

ColdFusion ODBC options for dBase/FoxPro data sources are described in the following table.

Intersolv dBase/FoxPro ODBC Options	
Option	**Description**
Data Source Name	A name for your ODBC data source.
Description	Descriptive information about the data source.
Database Directory	The path and filename of the Excel workbook you want to use as the ODBC data source.
Database Version	Enter the version number of the Excel workbook you want to use. ColdFusion supports Excel versions 3.4, 4.0, and 5.0.

Intersolv dBase/FoxPro ODBC Options	
Option	**Description**
Driver Settings	Use lowercase file extension (.dbf) — Specifies whether lowercase file extensions are accepted. If enabled, lowercase extensions are accepted. If disabled, only uppercase extensions are accepted.
	Use international collating sequence — Determines the order that records are retrieved when you issue a Select statement with an Order By clause. If disabled, the driver uses the ASCII sort order. This order sorts items alphabetically with uppercase letters preceding lowercase letters. For example, "A, b, C" would be sorted as "A, C, b." If enabled, the driver uses the international sort order as defined by your operating system. This order is always alphabetic, regardless of case; the letters from the previous example would be sorted as "A, b, C."

Intersolv Text ODBC options

ColdFusion ODBC options for dBase/FoxPro data sources are described in the following table.

Intersolv dBase/FoxPro ODBC Options	
Option	**Description**
Data Source Name	A name for your ODBC data source.
Description	Descriptive information about the data source.
Database Directory	The path and filename of the directory you want to use as the ODBC data source.
Extensions List	Lists the file name extensions of the text files on the data source. To use all files in the directory, enter *.*. To use only those files with certain extensions, add each extension you want to use.

Intersolv IBM DB2/6000 options

ColdFusion ODBC options for IBM DB2/6000 data sources are described in the following table.

Intersolv IBM DB2/6000 ODBC Options	
Option	**Description**
Data Source Name	A name for your ODBC data source.
Description	Descriptive information about the data source.
Database Name	The name of the DB2/6000 database.
Cursors	Preserve cursors at the end of each transaction —Enable this option if you want cursors to be held at the current position when the transaction ends. Doing so may impact the performance of your database operations.

Intersolv Sybase System 11 options

ColdFusion ODBC options for Sybase 11 data sources are described in the following table.

Intersolv Sybase System 11 ODBC Options	
Option	**Description**
Data Source Name	A name for your ODBC data source.
Description	Descriptive information about the data source.
Database Name	The name of the database to which you want to connect.
Server Name	The name of the server containing the Sybase tables you want to access. If not supplied, the initial default is the server name in the DSQUERY environment variable. On UNIX, the name of a server from your $SYBASE/interfaces file.
Workstation ID	The workstation ID used by the client.

Intersolv Sybase System 11 ODBC Options (Continued)	
Option	**Description**
Performance	Row Limit — The number of rows the driver retrieves from the server for a fetch. Enabling this option can increase performance by reducing network traffic.
	Create stored procedures — This option determines whether stored procedures are created on the server for every call to SQLPrepare. When enabled, stored procedures are created for every call to SQLPrepare. This setting can result in bad performance when processing static statements. When disabled, the driver does not create stored procedures.
	Disable database cursors for Select statements — Determines whether database cursors are used for Select statements. In some cases performance degradation can occur when performing large numbers of sequential Select statements because of the amount of overhead associated with creating database cursors.
Customization	Enable Password Encryption from Open Client Library to Server — Determines whether password encryption can be performed from the Open Client Library to the server.

Intersolv Oracle 7/8 options

ColdFusion ODBC options for Oracle 8 data sources are described in the following table.

Intersolv Oracle 8 ODBC Options	
Option	**Description**
Data Source Name	A name for your ODBC data source.
Description	Descriptive information about the data source.
Connect String	The client connection string designating the server and database to be accessed.
Performance	Include REMARKS in Catalog Functions — Specifies whether the result column REMARKS for the catalog functions SQLTables and SQLColumns and COLUMN_DEF for the catalog function SQLColumns have meaning for Oracle.
Customization	Enable scrollable cursors — Enables scrollable cursors for the data source. Both Keyset and Static cursors are enabled.

Intersolv INFORMIX 7.x/9.x options

ColdFusion ODBC options for INFORMIX 7.x/9.x data sources are described in the following table.

Intersolv INFORMIX 7.x/9.x ODBC Options	
Option	**Description**
Data Source Name	A name for your ODBC data source.
Description	Descriptive information about the data source.
Database Name	The name of the database to which you want to connect.
Server Host Name	The name of the machine on which the INFORMIX server resides.
	Use INFORMIX registry for Logon ID and Password — Determines whether the drive reads the Logon ID and Password directly from the INFORMIX registry.
Cursors	Preserve cursors at the end of each transaction — Determines whether cursors will be preserved or closed at the end of each transaction. Enable this attribute if you want cursors to be held at the current position when the transaction ends. Enabling this option may impact the performance of your database operations.
	Enable scrollable cursors — Determines whether the driver provides scrollable cursors. The INFORMIX driver can use scrollable cursors only if there are no long columns (SQL_LONGVARCHAR or SQL_LONGVARBINARY) in a Select list. If you enable this option, you must not include long columns in the Select list.
	Enable Insert cursors — Determines whether the driver can use Insert cursors during parametrized inserts.

Intersolv OpenIngres 1.x/2.x ODBC options

ColdFusion ODBC options for OpenIngres data sources are described in the following table.

Intersolv OpenIngres ODBC Options	
Option	**Description**
Data Source Name	A name for your ODBC data source.
Description	Descriptive information about the data source.
Database Name	The name of the database to which you want to connect.
Server Name	The name of the virtual node that you defined using the OpenIngres NETU utility. This virtual node tells OpenIngres which system to call, how to call it, and the user's name and password.
OpenIngres Options ID	The flags allowed on the OpenIngres SQL command line. Examples are: • -l (locks the database exclusively) • -u (logs on as username) • +w or -w (waits/doesn't wait for the database if someone has already opened it exclusively) • +U or -U (enables/disables user updating system tables and locks the database exclusively) • +Y or -Y (enables/disables user updating system tables but does not lock the database exclusively)
Performance	Repeated Cache Size — Determines whether all Update and Insert statements are to be run as repeated statements. This attribute improves the performance of applications that repeat the same set of SQL statements.

Intersolv OpenIngres ODBC Options (Continued)	
Option	**Description**
	Long Data Buffer — An integer value that specifies, in 1024-byte multiples, the maximum amount of data that will be transferred to the client for unbound long data result columns.
	Optimize SELECT statements as repeated queries — Determines whether the driver optimizes Select statements or runs them as repeated queries.
	User Select Loops instead of Cursors — Enables the retrieval of multiple rows using the Select loop model instead of cursors.
	Substitute parameters for hard coded values in repeated statements — Determines whether the driver substitutes parameters for hard coded values in repeated statements. This option is convenient in applications that do not use dynamic parameters.
Driver Settings	Enable OpenSQL — Provides the ability to access data sources using OpenSQL.

ColdFusion Settings

To define a number of advanced ODBC and ColdFusion options, select a data source and click the CF Settings button. These options apply to both Windows and Solaris platforms. ColdFusion data source options are described in this table:

ColdFusion ODBC Settings	
Option	**Description**
Login Timeout	The amount of time in seconds before ColdFusion times out the Administrator login page.
Limit Connections	Click to enable and then specify the number of simultaneous connections you want to allow for the current data source. **Note**: If you enable Limit Connections without specifying a limit for simultaneous connections, ColdFusion defaults to unlimited connections.

ColdFusion ODBC Settings (Continued)	
Option	**Description**
ColdFusion Login	Define a username and password if the current ODBC driver does not support username and password protection, or to override the current ODBC username and password definition. Any username and password specified in a CFQUERY tag overrides the values specified in the ColdFusion login. Also, when creating a data source using a native database driver for Oracle databases, you use the username and password options to pass login information to the Oracle database.
Maintain database connections	Ordinarily, a connection to a data source is established for every operation that requires it. However, you can improve performance by caching the database connection. To do so, click to enable this checkbox.
Restrict SQL Operations	Select the SQL operations you want to restrict for the current data source. ColdFusion will not execute the SQL operations you select in this list.

Click the Create or Update button to save your settings.

Configuring Native Database Drivers

The Enterprise edition of ColdFusion Application Server includes support for Sybase System 11, Sybase Adaptive Server 11.5, and Oracle 7.3 and 8.0 databases through native database drivers on Windows and Solaris.

Native database driver options vary according to the type of data source you are creating. For information about ColdFusion-specific settings, see "ColdFusion Settings" on page 67.

Software requirements

In order to use the native database drivers, you may need additional client software. The following table details requirements for each database and each supported platform.

Software Requirements for Native Database Drivers	
Database	**Client Software**
Oracle 7.3	Oracle 7.3.x client
Oracle 8.0	Oracle 8.0 client
Sybase System 11 Sybase Adaptive Server 11.5	Sybase Open Client version 11.1.0 with Update 11.1.1 applied (Solaris and Windows NT)

The database client software and ColdFusion Application Server must reside on the same system.

Summary of steps

To create an Oracle data source using the native driver:

1. Install the required client software, referring to the software requirements table above.
2. Use the SQL Net Easy Configuration utility to create a database alias. The Solaris version of this utility can be found in `$ORACLE_HOME/bin/net8wiz.sh`.
3. Create the data source in the Cold Fusion Administrator Native Drivers page.
4. Edit the `coldfusion/bin/start` script to include the following values:
   - The database variable `ORACLE_HOME`
   - The library path set in `LD_LIBRARY_PATH`.

To create a Sybase data source using the native driver:

1. Install the required client software, referring to the software requirements table above.
2. Verify the connection to the database using a tool like Sybase SQL Advantage.
3. Create the data source in the Cold Fusion Administrator Native Drivers page.

Example: Configuring the Oracle 8 native driver

The following scenario depicts the typical configuration steps for using the Oracle 8 native database driver. This procedure was written against version 8.0.4.0.0 of the Oracle 8 Client.

Before you get started

Before you get started, make sure you have the following information handy:

- The name of the host system where the Oracle database resides.
- The System Identifier (SID) for your Oracle 8 database.
- A login ID and password for connecting to the Oracle 8 database.

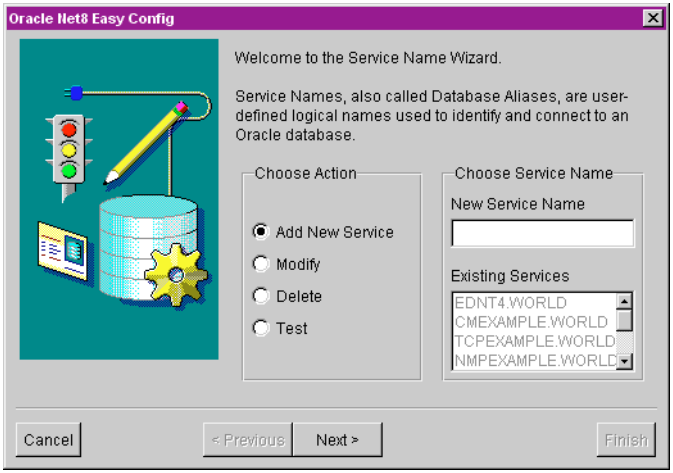
First step: Install the Oracle 8 Client:

1. Install the Oracle 8 Client software.
2. Select the Database administrator or Application user option in the following dialog. In this example, we chose Application user.
3. Step through options involving stopping Oracle services that may be running on your system, and choosing whether to install online documentation.

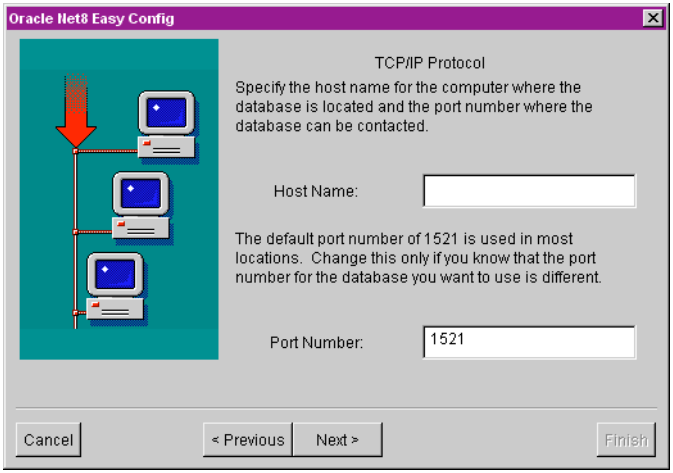
Second step: Run the Oracle Net8 Easy Config utility:

This step creates a database alias you use to reference the Oracle database when creating the data source in the ColdFusion Administrator. The process of creating the database alias writes all of the database connection information to a configuration file called `tnsnames.ora`.

1. Open the Oracle Net8 Easy Config utility. The icon is found in your Oracle for Windows NT program group. On Solaris, this utility is found in `$ORACLE_HOME/bin/net8wiz.sh`.
2. You want to add a new service, so enter a New Service Name and click Next.



3. In the resulting dialog, select TCP/IP as the networking protocol to connect with and use the Oracle 8 database you want to use in your ColdFusion application.
4. In the dialog that appears, you now need to enter the host name of the server where the Oracle 8 database resides. We took the default for the port number.



5. After entering a hostname, you enter the Database SID, which identifies your specific Oracle database instance. The default is ORCL, but your database SID might be different. See your database administrator (DBA) for this information.
6. In the next dialog, you test the database service you have created. To test the connection to the Oracle database, you'll need to enter a valid username and password for accessing the Oracle database. If you don't have this information, see your DBA.

   Now you need to create the data source in ColdFusion.

Creating the data source in ColdFusion:

1. Open the ColdFusion Administrator to the Data sources, Native Drivers page.
2. Enter a data source name and select the Oracle 8 native driver from the drop down list.
3. When you click Add, ColdFusion opens the configuration page for the data source. Here you enter information that tells ColdFusion where to find the database. The options that are most important for a successful connection are:
   - Host string — Enter the exact database alias you created using the Oracle Net8 Easy Config utility.
   - ColdFusion Login username and password — These options appear when you click the CF Settings button. The username and password are the same as those used in the Oracle Net8 Easy Config connection test. If you don't know what the username and password should be, see your Oracle 8 DBA.
4. Once you have created the data source, open the Verify Data Source page in the Administrator to verify that ColdFusion can connect to the Oracle 8 database.

Oracle 8.0 native database options

ColdFusion native database options for Oracle 8.0 data sources are described in the following table.

Oracle 8.0 Native Database Driver Options	
Option	**Description**
Data Source Name	A name for your ODBC data source.
Description	Descriptive information about the data source.
Host String	Enter the database alias you created using the Oracle Net8 Easy Config utility. To find the database alias for the database you want to connect to, you can use the Oracle Net8 Easy Config utility.

What to do if the connection test fails

If the basic information you entered in the Oracle Net8 Easy Config is correct, then a visit to your local Oracle 8 DBA is probably in order. First thing to do is check the basic connection information: hostname, SID, username and password. You can do this using the Net8 Easy Config utility or by directly inspecting the `tnsnames.ora` file.

In addition, on Solaris, make sure you have the Oracle client library and `ORACLE_HOME` defined in the `coldfusion/bin/start` script.

In some cases, connection problems were solved by clearing your system of the Oracle 8 Client and reinstalling it. Unfortunately, Oracle does not provide an uninstaller for the Oracle 8 Client.

ColdFusion Native Database Driver Options

Refer to the following tables for information about options for each native database driver.

Sybase native database options

ColdFusion native database driver options for Sybase System 11 and Sybase Adaptive Server 11.5 data sources are described in the following table.

Sybase System 1/Adaptive Server 11.5 Native Database Driver Options	
Option	**Description**
Data Source Name	A name for your ODBC data source.
Description	Descriptive information about the data source.
Server	Enter the name of the server hosting the Sybase System 11 database.
Default Database	Enter the name of the default database to use on the specified server.

Oracle 7.3/8.0 native database options

ColdFusion native database options for Oracle 7.3/8.0 data sources are described in the following table.

Oracle 7.3/8.0 Native Database Driver Options	
Option	**Description**
Data Source Name	A name for your ODBC data source.
Description	Descriptive information about the data source.
Host String	Enter the database alias you created using the Oracle Net8 Easy Config utility. To find out what the database alias is for the database you want to connect to, you can use the Oracle Net8 Easy Config utility to find out.

Configuring OLE DB Data Sources: Windows Only

ColdFusion developers can now access a range of new data stores through Microsoft OLE DB, including:

- MAPI-based data stores such as Microsoft Exchange and Lotus Mail
- Non-relational data stores, such as Lotus Notes
- LDAP 2.0 data
- Data from OLE applications like word processors and spreadsheets
- Mainframe data
- HTML and text files, flat-file data

Enabling this capability requires installation of OLE DB providers available from third-party vendors. The provider software handles data processing in response to requests from the OLE DB consumer, in this case ColdFusion.

After installing and configuring the provider software, open the ColdFusion Administrator Data Sources OLE DB page and add data stores supported by that provider. As with other ColdFusion data sources, you enter a name and description and select advanced settings as needed. You will also need to enter:

- Provider — The ProgID
- ProviderDSN — The data source name

The data source displays on the main OLE DB page and can be used in data queries.

Performance gains can be made by running an OLE DB provider, instead of an ODBC driver, to process SQL. This is dependent on how the provider implements the data call. Some providers route OLE DB calls through the ODBC Driver Manager, while others go directly to the database. Providers that go directly to the database are akin to native drivers in providing an alternative to ODBC. Providers are available for all the major relational DBMS products as well as the data stores listed above.

OLE DB is a Microsoft specification. For more information, including a list of provider vendors, go to their OLE DB site: http://www.microsoft.com/data/oledb/.

Verifying ColdFusion Data Sources

The ColdFusion Administrator includes a facility for verifying data sources configured for ColdFusion. This is a useful way of making sure that a data source has been correctly configured and is available to your ColdFusion application pages.

Note A username and password is required for data sources to be verified. To define a username and password for a data source, edit the properties for the data source.

To verify a ColdFusion data source:

1. In the Administrator contents frame, select Verify Data Source, an option under the Data Sources link.

2. Select a data source from the drop down list and click Verify. If the specified data source is not accessible, ColdFusion let's you know with an error message.

Note If a connection test fails, it is sometimes useful to run a CFQUERY against the failed data source to get a more helpful error messages.

CHAPTER 5

Scheduling and Static Page Generation

This chapter explains how you can use ColdFusion to perform scheduled processes and to generate static pages. Often the two are combined to allow the periodic regeneration of data that doesn't need to be available dynamically to a ColdFusion application.

Contents

About Scheduling ColdFusion Pages

The ColdFusion Administrator includes a scheduling facility that allows you to schedule the execution of ColdFusion pages and to generate static HTML pages. The scheduling facility can be very useful for applications that do not require user interactions or customized output. Often, ColdFusion developers use this facility to schedule daily sales reports, corporate directories, statistical reports, and so on: Information that is more often read than written.

Here's how it works. Instead of executing a query every time the page is requested, the static page is served up to users containing information generated by the scheduled event. Response time is faster since there is no database transaction, just an HTML page.

ColdFusion allows you to schedule pages to execute on a daily, weekly, or monthly basis. You can specify a time of day for execution, and you can schedule a page to be run only once on a specified date.

When a scheduled page executes, a message is written to a log file, `schedule.log`, which specifies the name of the scheduled action, the page that was executed, and whether the page executed successfully or not. For more information about log files, see Chapter 3, Configuring ColdFusion Server.

Scheduling a ColdFusion Page

The ColdFusion Administrator allows you to schedule the execution of application pages. To access the scheduling facility, open the Administrator and click the Scheduler button.

The scheduling facility has two parts:

- Scheduler Settings page — Where you specify how often ColdFusion checks for newly scheduled tasks.
- The Scheduled Tasks page — Where you define new tasks or change existing scheduled tasks.

There are three areas you define in scheduling an event:

1. The start/end date and interval.
2. The URL of the file you want to execute.
3. Publishing information if you want to save output to a file. This is the mechanism you use for creating static HTML pages by processing a ColdFusion page.

Note In the Operation list box on the Scheduled Tasks page, HTTPRequest is currently the only operation supported. Later releases of ColdFusion may add additional operations to this list box.

Specifying the Interval for a Scheduled Task

Often, you'll want to schedule a page to run at a regular interval for a fixed period of time. For example, to generate an employee list, it's not usually necessary to generate the list dynamically. Instead, you could schedule the page that generates the list to run every night during off peak hours.

By default, when you open the Add Scheduler Task page, ColdFusion enters the current date and time as the Start date and time for the new event. If you find that a scheduled event is not executing, check your start date and time values.

When entering an end date and time, if you leave the End Date and Time fields blank, ColdFusion runs the scheduled event until you explicitly stop the event by editing the task parameters, or by deleting the task in the Administrator.

You can choose from the following Intervals when scheduling a recurring ColdFusion event:

- Daily
- Weekly
- Monthly
- One-time
- Daily at specified intervals

To define the start/end time and interval:

1. Open the ColdFusion Administrator and click the Scheduler button.
2. Enter a name for the task you want to schedule and click the Add New Task button. The Add Scheduler Task page appears, where you provide details about the operation you want to schedule.
3. Enter start and end dates for the task. Note that the end date is optional. You might want the task to be executed without a limit.
4. Select the type of schedule: One-time, Recurring, or Daily and enter scheduling information according to the type of schedule you want for your task. Enter all time values using the 24 hour clock. For example, enter 03:00 for 3:00AM and 15:00 for 3:00PM.

Note When scheduling a new event, you must set the execution time far enough in the future for ColdFusion to update its internal scheduled task list. By default, ColdFusion checks every 15 minutes for newly scheduled tasks. You can modify this interval using the Scheduler Settings page.

Specifying the Page to Execute

When you schedule a ColdFusion page to execute, the page can be local or remote. With the proper access rights, you can schedule a page on a remote server by specifying the server name in the URL field.

Specify the application page to execute:

1. Enter the URL for the page you want to execute in the URL text entry box. This is not limited to local pages. You can execute pages on a remote ColdFusion server as well, assuming you have the proper access rights to do so.
2. Specify a username and password as necessary if the page you want to execute is secured in a directory that requires a username and password for access.
3. Enter a request timeout setting. The timeout setting helps avoid requests that stall because of an overloaded web server, network problem, or a page that takes too long to execute for whatever reason.
4. If requests need to be routed through a proxy server, enter the URL for that server.

For information about saving scheduled output to a file, see Saving Scheduled Output to a File.

Saving Scheduled Output to a File

You can use the Publish option to specify an output file for the scheduled task. For example, you could schedule a page that generates an employee list every night and make the page output available to end users. You do this by specifying an output directory and page and then linking to that page from relevant places in your Web site.

If you elect to publish an output file but do not specify a directory name or file name, ColdFusion ignores the request to publish the page. If you are having trouble outputting a file, check that the path is correctly specified. ColdFusion will not create directories referenced in the output path that do not exist.

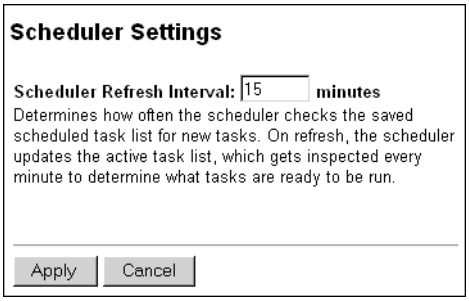
To specify an output file:

1. To specify an output file, enter both full path and file information. Path information can be referenced in the following forms: using the UNC naming convention in Windows, for example, `\\hostname\path` or using an absolute path reference.
2. Enable the Resolve URL option to replace any relative URLs used in links returned in the result page to absolute URLs.

Defining the Scheduler Refresh Interval

By default, ColdFusion checks the scheduled task list for newly scheduled tasks every 15 minutes. You can change this setting so that ColdFusion checks more or less

frequently, by entering a new value on the Scheduler Settings page in the ColdFusion Administrator.



To change the interval ColdFusion checks for newly scheduled tasks, enter an interval value, in minutes. After changing the Scheduler refresh interval, make sure you stop and restart the ColdFusion Executive and ColdFusion Application Server services (Windows NT) or run the stop and start scripts (Solaris).

For information about running ColdFusion start and stop scripts in Solaris, see Chapter 3, Configuring ColdFusion Server.

For information about starting and stopping ColdFusion services on Windows NT, see Chapter 3, Configuring ColdFusion Server

Logging Scheduled Events

ColdFusion writes information about all scheduled events to a log file you can view to verify that events occurred or to troubleshoot scheduled events that did not execute properly. The log file can be found in:

`\cfusion\log\schedule.log`

Here's some sample output from the `schedule.log` file:

```
"Information","TID=258","07/13/98","17:34:59","Scheduled
action mongo, template http://maximus/cfdocs/mongo.cfm
completed successfully."
```

For information about ColdFusion log files, see Chapter 3, Configuring ColdFusion Server.

CHAPTER 6

Clustering and Load-Balancing

This chapter describes how to set up ColdFusion clustered servers, which allow you to configure server load balancing and fail-over options.

Contents

About ClusterCATS for ColdFusion

ClusterCATS for ColdFusion is a Web server clustering technology that provides load balancing, fail-over and other services to assure high availability for the ColdFusion Application Server (CFAS). ClusterCATS allows you to cluster distributed Windows NT or SUN Solaris Web servers into a single, high-performance, highly available environment of Web server resources.

A server cluster consists of two or more Web servers located on a LAN or across a WAN. Web servers included in a cluster operate as a single entity to provide rapid and reliable access to resources on those Web servers. A cluster can help your web site avoid the consequences of busy and failed servers, slow networks. With ClusterCATS you can avoid bandwidth, latency, and congestion problems.

Rapid and reliable access

A ClusterCATS cluster provides users with rapid and reliable access to content by directing HTTP requests to the optimum Web server in the cluster. ClusterCATS determines which server in a cluster should respond to a request by employing the following services:

- **Failover** — Providing alternate Web servers in the event of server overloading, or hardware and software failures.
- **Load balancing** — Balancing HTTP request load among a cluster of Web servers through HTTP redirection.

ClusterCATS for ColdFusion features

ClusterCATS provides these important features.

- Load-balancing
- Ability to mix platforms within a single cluster
- The ability to set server load thresholds
- Centralized system administration
- Load calculation of ColdFusion service
- Email-based alarms for a wide range of failure types
- Support for Netscape Enterprise Server on Solaris
- IIS 3.x and IIS 4.0 support on Windows NT
- Session state awareness
- Server restriction capability

ClusterCATS for ColdFusion Components

ClusterCATS for ColdFusion consists of two separate, installable components:

- ClusterCATS Server for Sun Solaris and Windows NT
- ClusterCATS Explorer (Windows NT only)

You install the ClusterCATS server on every server or machine you want to include in a cluster. You use the ClusterCATS Explorer to create and administer server clusters.

ClusterCATS Server

ClusterCATS Server runs on Windows NT and Sun Solaris. Each ClusterCATS Server monitors the status of all other Web servers that are included in a cluster and tracks application and transaction resource availability.

Each ClusterCATS server:

- Manages the distribution and synchronization of content for optimal retrieval
- Intelligently directs user URL requests to the optimum Web server within the cluster

ClusterCATS Explorer

ClusterCATS Explorer is Windows administrative utility you use to create and manage ClusterCATS clusters. ClusterCATS Explorer provides all required functions for centrally managing one or more clusters. Using a Windows Explorer-like graphical interface, you configure, view, monitor, and perform other management tasks, such as:

- Creating and removing clusters
- Adding and removing servers from a cluster and setting server load threshold levels
- Registering cluster administrators
- Selecting events for alarms and specifying the recipients of alarm email distributions

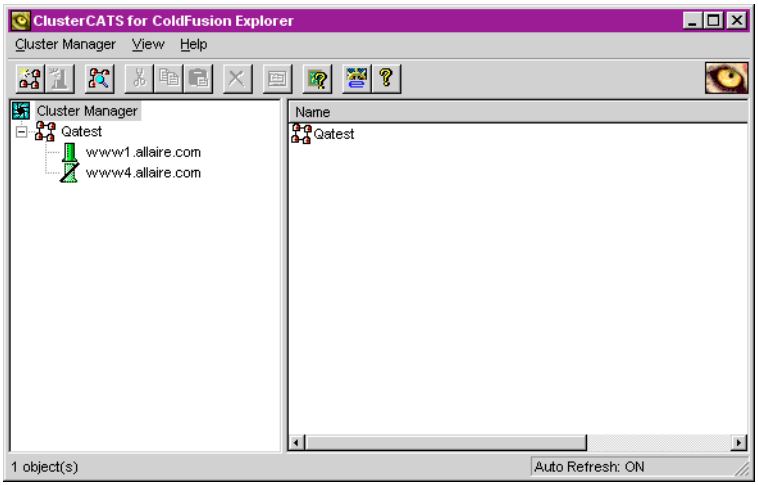
Note If you plan to run ClusterCATS for SUN Solaris, you need at least one Windows NT system for your system management station.

The ClusterCATS Explorer Main Window

The ClusterCATS Explorer presents a view of your cluster in much the same manner as the Microsoft Explorer presents a view of the files and directories that reside on your own computer. Each of the objects in a ClusterCATS cluster configuration — clusters, servers, files, and applications — are represented by a unique icon. You can

manipulate these icons in much the same manner as you expand and collapse directory trees in the Explorer application.

[This screen shot needs to be replaced with the CF version]



The ClusterCATS interface comprises four distinct areas:

- **Toolbar** — Button access to the most frequently used ClusterCATS functions.
- **Left Pane** — Contains various views of cluster objects.
- **Right Pane** — Contains the view folder and files for the object currently selected in the left pane.

Refresh Status

The ClusterCATS Explorer has an auto refresh feature. When auto refresh is turned off, the server status is updated every five seconds. Disabling auto refresh can improve performance when you are running on a slow link.

Turn on Auto Refresh from the View > Auto Refresh menu. To manually refresh the Explorer display, press F5 or select View > Refresh to get an update of directories and files in the current cluster.

ClusterCATS Explorer icons

Each of the objects comprising a Cluster has a unique icon by which it is identified. Some of the icons can be displayed in several states. Figure 2 illustrates each of the icons and their states.

ClusterCATS Explorer Icons		
Context	**Description**	**Icon**
Cluster Objects	Cluster Manager	
	Folder	
	Folder Collection	
	Web Server	
	Cluster	
	File	
	File Collection	
	Probe	
	Probe's Server Location	
Web Server States	Unreachable or Unknown	
	Normal	
	Busy	
	Restricted	
File States	Normal	
	Restricted	

About Creating and Managing Clusters

You create and manage a cluster from the ClusterCATS Explorer. Even if your site is only comprised of Netscape Enterprise servers on SUN Solaris, you will still need to manage them from a Windows NT-based ClusterCATS Explorer.

System management for UNIX and Windows NT clusters entails the following tasks.

- Building the cluster
- Configuring email support options
- Adding and removing servers from the cluster
- Managing cluster state
- Configuring HTTP redirection
- Configuring server failover
- Configuring authentication and alarms

Sections that follow detail each of these operations.

Building a Cluster

Each time you create a new cluster, you must undertake a one-time startup process that defines the cluster's components and their relationships to each other.

To create a new cluster:

1. Start the ClusterCATS Explorer by clicking the ClusterCATS icon in your Windows program group. The ClusterCATS Explorer window displays.
2. Select Cluster Manager > New Cluster from the ClusterCATS Explorer main menu. The New Cluster dialog appears.
3. Enter the name of the new cluster and the domain name of the first Web server you want to include in the cluster. Your domain name may differ from the physical server name. The Web server name you add must be the fully qualified host name for the server.
4. Click OK. ClusterCATS adds the cluster under the Cluster Manager in the ClusterCATS Explorer window.

When ClusterCATS creates the cluster, icons for the cluster, content, and the first server appear in the Cluster Manager tree.

Choosing cluster-specific names

When you name your cluster and the servers that will be part of it, the servers must take the name of the host name or the virtual server that you have created on the parent Web server. Most likely, if you are working with a site planner or a specific department in your company during the deployment phase, you will need to choose a

descriptive name for the cluster that conveys the purpose for the overall cluster, such as Sales, Customer Support, and so on. Make your cluster names logically consistent with their purpose.

Configuring Email Support Options

Cluster CATS email support makes it possible for you to receive vital information about your ClusterCATS cluster on a daily basis. Simply add the name of the server that is your SMTP gateway and the email addresses of anyone in your organization who needs to receive the support information.

Report mail includes the following information:

- Cluster name and each server in the cluster
- Files
- Disk space
- Log Files

Support mail includes the following information:

- Cluster ID, cluster name, and number of servers
- The specifics about each of these features are included on a per-server basis

To configure email support options:

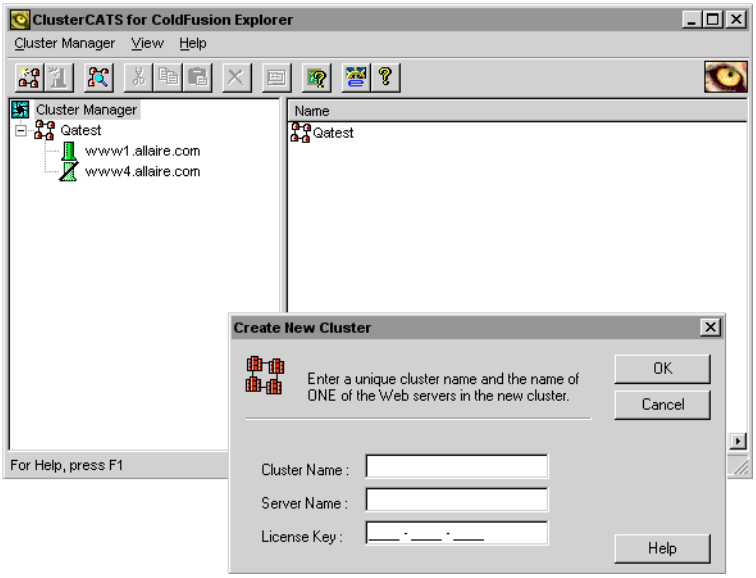
1. In the ClusterCATS Explorer window, select the cluster icon.
2. Select Configure > Support from the main menu. The Support dialog box displays.
3. Add a list of comma-separated email addresses where you want support email sent. Support email provides your organization with the following information:
   - Customer ID
   - License key
   - Cluster name and number of current servers
   - Server names with statistics for failover, redirect
4. Enter a list of report email addresses of people you want to receive report email. Report email is an automatically generated daily report containing the following statistics:
   - **Total Disk Space** — Total disk space on the system drives where the web root directory resides
   - **Log Size** — Total size of all the IIS (Windows) or Netscape (Solaris) log files

Adding and Removing Servers from the Cluster

Once the new cluster and the Administrative Manager are created, you can add additional Web servers to the cluster. During this process, each of the new servers and their associated content is included in the overall ClusterCATS Server definition.

To add an additional server:

1. In the ClusterCATS Explorer window, select the cluster to which you want to add a new member.



2. Enter the fully qualified server name for the second server and click OK. The server is added to the cluster.

To remove a server from a cluster:

1. Select the server you want to delete in the ClusterCATS Explorer.
2. Select Server > Delete on the ClusterCATS menubar.

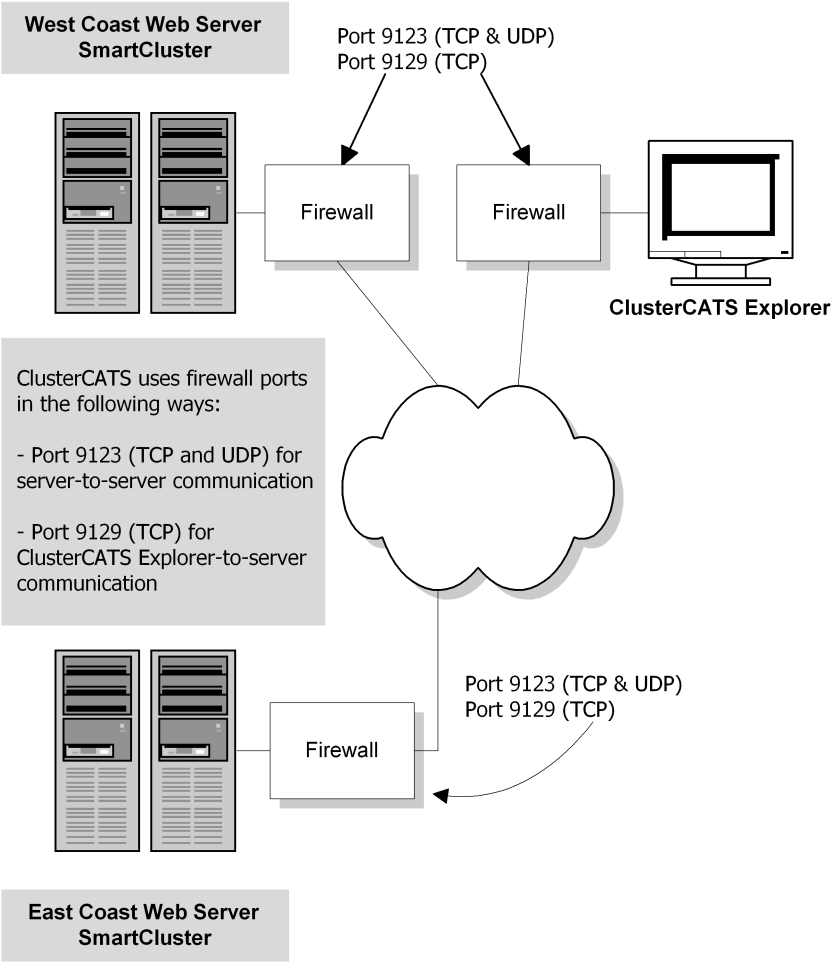
The selected server is deleted from the cluster you selected.

Using ClusterCATS with a Firewall

You can configure ClusterCATS to work across your Internet firewall. For example, you could set up your cluster so that the ClusterCATS Explorer is outside your firewall. Or, you could have an arrangement where two or more ClusterCATS Servers talk to each other and the ClusterCATS Explorer through the firewall.

To use ClusterCATS with a firewall in configurations like those mentioned, you need to open ports in your firewall software as illustrated below. ClusterCATS needs a port to communicate between the Explorer and the Server so you can change configurations. You also need a port for Server to Server communication to allow load information to be communicated between servers efficiently.

The following graphic shows a company with two server clusters. Both clusters are connected to the Internet through a firewall. The ClusterCATS Explorer runs on a system at corporate headquarters providing remote cluster management options.



Managing State in a Clustered Environment

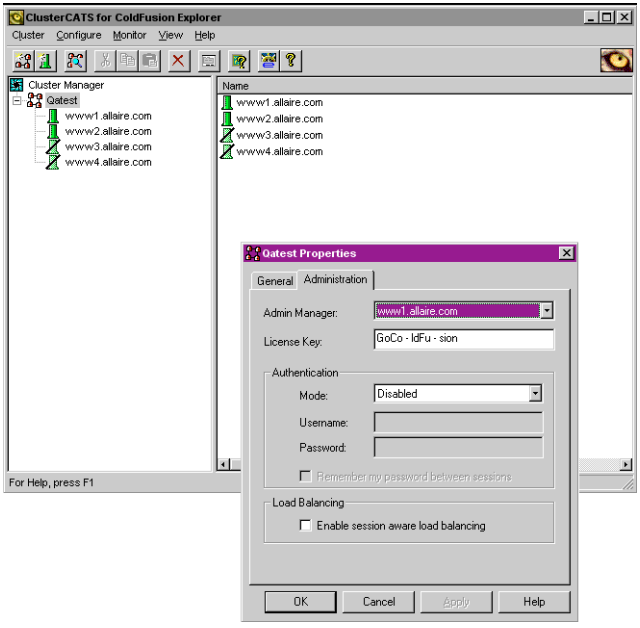
Because of the nature of a clustered environment, ColdFusion variables that are stored in memory or the registry, such as application, session, and server variables, are not sustained by default when a user is *balanced*, or shifted from one server in a cluster to another in order to balance server load. For example, using server variables in a clustered server environment won't work, since server variables are not carried from one server in a cluster to another when users are shifted to another server. State cannot be maintained correctly. Client variables, however, can be sustained because they can be stored in an external repository. If you are planning to migrate a ColdFusion application that uses session and server variables to a clustered server environment, you need to consider how to deal with this issue.

How to maintain session variables

An option in the ClusterCATS Explorer allows you to override the mechanism that would otherwise balance a session among servers in the cluster. Here's how to do it.

To maintain session variables in a cluster:

1. Make sure session variables have been enabled in the ColdFusion Administrator, Variables page.
2. Open the ClusterCATS for ColdFusion Explorer.
3. Right click the cluster in which you want to enable session aware load balancing, and select Configure > Administration. The properties dialog for the selected cluster appears.



4. At the bottom of the dialog, click to enable the **Enable session aware load balancing** option.

Once enabled, ClusterCATS maintains session state by ensuring the current session remains connected to the server on which state was set. After being balanced on initial connection, the user will not be shifted or balanced to another server in the cluster during the session.

Note There may be significant site performance costs associated with enabling this feature, since users will never be balanced to other servers in a cluster, regardless how heavy the load may be on the server maintaining state.

Configuring HTTP Server Redirection

You can configure ClusterCATS redirection to occur for a number of different reasons. However, in each case, what happens is the same: requests initially handled by one server are routed to another server in the cluster. For example, ClusterCATS enables load balancing in a cluster of servers. Load is distributed among a group or cluster of servers. This is achieved by setting limits to the amount of traffic a server can handle. When the level of incoming traffic reaches that predefined level, all subsequent traffic is redirected to the other servers in the cluster.

ClusterCATS supports four types of redirection:

- Combined with DNS round robin to distribute requests among servers in your cluster
- Through ClusterCATS transparent redirection of HTTP requests

- By setting ClusterCATS load threshold, gradual redirect threshold, and Web server state maintenance levels
- By setting preferred server selections

Using ClusterCATS with DNS round robin

ClusterCATS works in conjunction with the round robin DNS you may already have in place. More importantly, ClusterCATS eliminates the following two major problems associated with round robin DNS:

1. **Server failure** — Round robin DNS cannot detect server failure. If any server in a ClusterCATS cluster fails, another server on that subnet will immediately and transparently assume the IP address of the failed server.
2. **Server overload** — Round robin DNS cannot detect server overloading. In a ClusterCATS cluster, load thresholds are configured on each server. If actual server load exceeds the load threshold, ClusterCATS transparently redirects the user to another web server. Once redirected, user requests and responses will flow to and from that server directly, minimizing response times throughout the user session.

Scheduling and DNS round robin

ClusterCATS clusters support DNS scheduling. With scheduling, you can have client URL requests redirected using DNS round robin to cycle the request through the servers in your round robin cluster. To do this, you create a global name in the DNS hierarchy at the desired level where the round robin name will reside.

For example, if you have three servers named: server1.sales.us.company.com, server2.sales.us.company.com, and server3.sales.us.company.com, you need a DNS object — for example, www.sales.us.company.com, (or ussales.company.com) — created at the appropriate level in DNS. Note that your DNS name server must support round robin names.

So that ClusterCATS operates effectively with round robin DNS, you need to make sure it is configured properly. For example, for a single location Web server farm consisting of four servers, you need to configure round robin DNS across all four servers for the domain name and individual IP addresses for each server name. As an example, your DNS tables would look something like the table below.

Example DNS Tables with Round Robin Enabled	
Host Name	**IP Address**
www.mycompany.com	193.168.0.1
	193.168.0.2
	193.168.0.3
	193.168.0.4

Example DNS Tables with Round Robin Enabled	
Host Name	**IP Address**
www1.mycompany.com	193.168.0.1
www2.mycompany.com	193.168.0.2
www3.mycompany.com	193.168.0.3
www4.mycompany.com	193.168.0.4

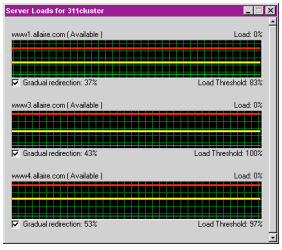
round robin DNS distributes the initial domain level requests across all four servers. From there, ClusterCATS distributes load to avoid failed or overloaded servers.

How ColdFusion Calculates Load for ClusterCATS

Because ColdFusion reports load data to ClusterCATS, you can view the load on the ColdFusion server at any time using the ClusterCATS Explorer Server Load Monitor.

To view ClusterCATS server load:

1. Select the cluster you want to monitor in the ClusterCATS Explorer.
2. In the Monitor menu, select Load. The Server Load display for the selected cluster appears, as shown below:



[Need real-world screen shot]

The load monitor shows three lines:

- Top line (red): Load Threshold
- Middle line (yellow): Gradual Redirection Threshold
- Bottom line (green): ColdFusion Application Server Load

Configuring Server Response Time Thresholds

ClusterCATS allows you to define two server response time thresholds:

1. **Gradual Redirect Threshold** — The server will redirect a percentage of new requests in an attempt to reduce server load and prevent the server from entering a busy state. As actual server load increases, the percentage of redirected new requests also increases.
2. **Busy Load Threshold** — The server redirects all new requests received. In summary, ClusterCATS is able to exploit the benefits of round robin DNS in distributing load while eliminating the inability of round robin DNS to detect server failures and overloads. To eliminate server overloads, we use the HTTP redirect mechanism.

HTTP Server Redirection: What ClusterCATS Does

In redirecting HTTP requests, the ClusterCATS Server evaluates the cluster's state with the following availability parameters, in the order shown:

1. HTTP server state
2. ColdFusion server load

This policy works in both centralized and distributed ClusterCATS Server configurations. In a centralized ClusterCATS cluster with all Web servers at one site, the ClusterCATS Server will only redirect if the server is busy or restricted.

Manually Configuring HTTP Server Redirection

You can manually configure HTTP server redirection in several ways:

- You can set redirection threshold levels for complete and gradual redirection
- You can Restrict access to cluster Objects and force failover
- You can maintain server state by overriding redirection on specific folders and files
- You can maintain server state by overriding redirection on application URLs that require state

Setting HTTP Redirection Threshold Levels

ClusterCATS gives you the ability to set the threshold at which a server goes into a busy state and begins redirecting all user requests to other available servers in the cluster. There are two redirection thresholds you can configure with ClusterCATS:

- Load threshold
- Gradual redirection threshold

You configure these threshold levels so that as a server approaches a certain load level, requests are redirected to other servers in the cluster based on their availability.

You can set these two threshold levels to be very close to ensure that your server availability remains at a very consistent level. Or you can set your load redirection and gradual redirection thresholds far apart, allowing your server to handle wider acceptable levels of traffic.

Much of your redirection threshold configuration decisions hinge on the architecture of your application and where the bulk of your processing resources need to be allocated.

Load threshold

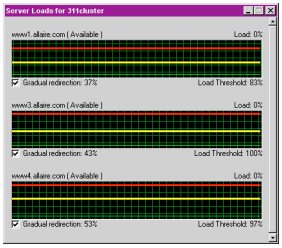
The load threshold defines when the server's state transitions from available to busy. When the load exceeds the threshold that you configure, all user requests are redirected to other servers in the cluster, based on their own availability.

Gradual redirection threshold

Gradual Redirection lets you set a secondary threshold at which user requests begin being redirected. If the Gradual Redirection threshold is set close to the Redirection threshold, then a greater portion of user requests are redirected. If it is set further away from the Redirection threshold, then fewer requests are redirected.

To configure gradual redirection using the Server Load dialog:

1. Select one of the servers or select the cluster in the left pane of the Explorer.
2. Right click on one of the server icons. Select Monitor > Load. The Server Load dialog box displays.
3. Grab the Red Load Threshold line with the cursor. Move the red line up or down to reset the server's load threshold level. As you move the line, the load threshold percentage changes.



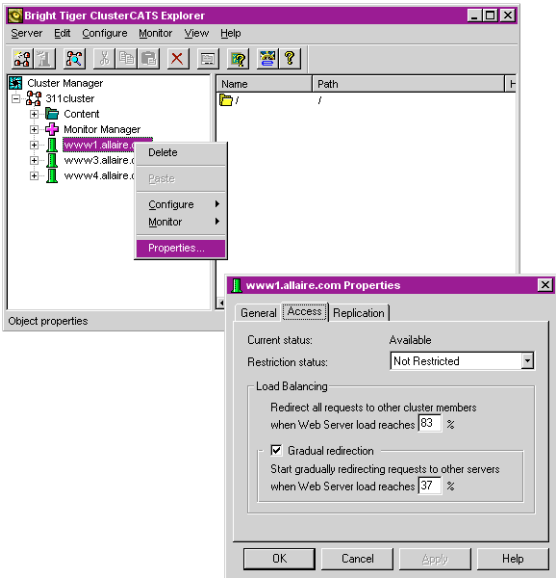
[Need real-world screen shot]

To configure gradual redirection using the Server Properties dialog:

You can also set this number on the Access tab of the Server Properties box.

1. Right click on the Server icon.

2. Select Configure > Access. The Properties dialog appears for the current server, with the Access tab selected.



3. In the Load Balancing section, enter a load number at which you want the server to start redirecting user requests.

To set up gradual redirection:

1. Select one of the servers or select the cluster.
2. Right click on one of the server icons. Select Monitor > Load. The Server Load dialog box displays.
3. Click on the Gradual Redirection threshold in the lower left-hand corner of the box. A yellow line appears below the red line. This is the Redirection threshold line. Grab the yellow Load Threshold line with the cursor. Move the yellow line up or down to reset the server's gradual redirection start point. Notice the number in the lower left-hand corner of the dialog box. It changes to a % as you move the line. The closer you move the line to the red line, the more redirects occur. The further you move the line away from the red line fewer requests are redirected.

You can also set this number on the Access tab of the Server Properties box.

1. Right click on the Server icon
2. Select Configure > Access.
3. In the Load Balancing section, click on Gradual Redirection and plug in a load number at which you want the server to start gradually redirecting user requests.

Configuring Server Failover

Bright Tiger uses a concept called IP Aliasing to accomplish Web server failover. To enable failover, two or more Web servers run ClusterCATS Server on the same subnet. Failover relies on IP aliasing being available clusterwide, so there must be at least two Web servers running ClusterCATS Server on each subnet throughout the cluster. A widely distributed cluster could consist, for example, of two or more servers on each subnet in the cluster.

Each ClusterCATS Server sends out a heart beat on a periodic time interval. If a heart beat is not heard from a server, a remaining web server in the cluster will assume the failed server(s) IP address and begin accepting requests intended for the failed server.

If either of the servers in the cluster fail, the remaining server assumes the failed server's IP address, becoming the Alias Server. Once the Alias server assumes a failed server's IP address, it handles all HTTP traffic addressed to the failed server.

Authenticating ClusterCATS Administrators

ClusterCATS security is provided through an authentication facility you can enable to keep unauthorized users from accessing a cluster and its content. When authentication is enabled for a specific cluster, only authorized users will be able to add that cluster to their ClusterCATS Explorer view.

Authentication can be turned on or off based on your specific security needs. By default, authentication is disabled. It can be enabled through the ClusterCATS Explorer user interface.

ClusterCATS authentication can take one of the following three forms:

- No Authentication
- Windows NT domain Authentication (must have an NT server in the cluster)
- Local-User Authentication

You should select one of these modes based on your need to restrict access to the content stored on the Web servers that are part of your clusters.

No authentication

When authentication is disabled on a specific cluster, any ClusterCATS Explorer can add that cluster to their Cluster Manager view. Once the cluster is added, administrators have unrestricted access to the content in that cluster.

Using Windows NT Domain Authentication

Before you can enable NT domain authentication on any specific cluster, you must create an NT user group with a name in the form: "BT_*clustername*" within the domain you want to secure.

You or the domain administrator can do this through the standard Windows NT User Manager for Domains utility. Once you create a "BT_clustername" group, any of the users you add to that group are authenticated to view the cluster. All members of the cluster must be from the same Windows NT domain unless a trusted relationship has been set up between two or more domains by the system administrator.

A "BT_*clustername*" global group must exist in the domain from which the ClusterCATS Explorer is executed. Cluster members in other domains need only the trust relationship. ClusterCATS Explorer determines what servers exist in which NT domain by communicating with any Windows NT domain controller for the domain. The list of servers that exist in the Windows NT domain can be viewed by looking at the Network Neighborhood Windows NT utility. If no trust relationship exists, then cluster members must be from the same Windows NT domain.

To set up Windows NT domain authentication:

1. You or someone with administrator privileges in the NT domain where all of the servers reside must create a new security group. The group name has to take the form: "BT_*clustername*." You'll need to go up the domain hierarchy until you reach a common level for all servers in the cluster.
2. Log into the domain as administrator, Start Programs > Administrative Tools > User Manager for Domains.
3. Select User>New Global Group. Add the group name and then add yourself as a member of the group. You can now administer that cluster. To add other administrators, simply add them to the same BT_clustername group. Ensure that this process is completed before you complete the next step.
4. In the ClusterCATS Explorer window, right click the icon of the cluster where you want to configure authentication and select Properties from the popup menu.
5. Click the Administration tab on the cluster properties dialog.
6. In the Authentication field, NT domain, click OK. Authentication for the selected cluster is enabled. Only authorized administrators (people who are part of the BT_* group created in the Step 1) can add that cluster to their view.

Using Local-User Authentication

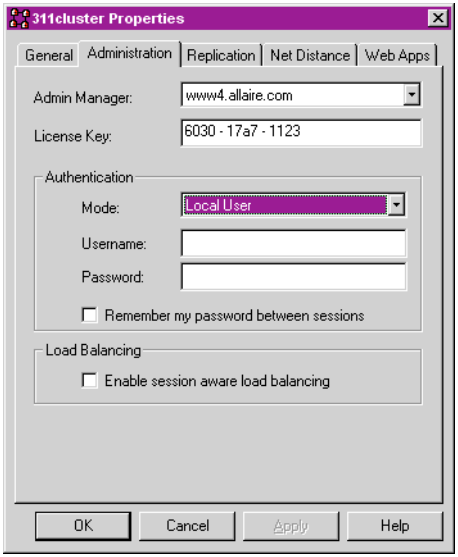
If you opt to use Local-User Authentication, you can authenticate specific users on a per-server basis. Local users of a server are users that have an account on a specific system where the Web server resides. If a cluster has several Web servers included and you only have an account on one, for example, then you can add the cluster to your

ClusterCATS Explorer view, but you will only have access to the server where you have an authorized account.

Local-user authentication is turned on or off on the Cluster Properties Access box.

To enable local-user authentication:

1. Right click the cluster you want in the ClusterCATS Explorer and select Properties from the popup menu.
2. Click the Administration tab on the cluster properties dialog.



3. In the Authentication Mode drop down list box, select Local User.
4. Enter a user name and password and click OK. Local Authentication for the specified user in the selected cluster is enabled. Only authorized administrators can add the cluster to their ClusterCATS Explorer view.

Make sure all authorized users for Local User Authentication have an account on each machine running the IIS server and are listed in a local group with the name BT_*clustername* where *clustername* is the name of the cluster. Alternatively, authorized users can also be administrators listed in the Administrator's Group (on each machine running the IIS server).

To disable authentication:

1. In the ClusterCATS Explorer window, right click on a cluster icon. Select Configure > Administration.
2. In the Cluster Properties dialog box (Administration tab), select Disable authentication in the Authentication field. Authentication is now disabled.

Configuring ClusterCATS Alarms

The alarm notification feature of ClusterCATS provides you with instant feedback on critical events that take place within a Cluster. You can set alarms on the following features. Once the event triggers the alarm you are notified via email of the event. Alarms can be configured to warn you about:

- Disk Failure
- HTTP Server Failure
- Server Busy Warning
- Server Unreachable
- Web Server Failover

To configure an alarm:

1. In the right pane of the ClusterCATS Explorer window, select the cluster to which you want to add an alarm.
2. Click the right mouse button and select Configure > Alarm Notification. The Alarm Notification window appears.
3. Select the event you want and enter the email address of the person (or account) you want to receive email notification of the event.
4. Enter the default SMTP host where your mail is delivered.
5. Click OK. Notification for this event is enabled. If the event you chose occurs, an email message is sent to the designated account. See the list below for the notification schedule for each event.

Alarm Event Notification Schedule	
Event type	**Notification occurs...**
Disk Failure	Immediately
HTTP Server Failure	Immediately
Server Busy Warning	Every 24 hours
Server Unreachable	Immediately
Web Server Failover	Immediately

Session-Aware Load Balancing

When you enable this feature, the ClusterCATS software load balances a Web server by redirecting users to another Web server before the user has established a new session. Once a user has started a session by typing in a URL or using an existing bookmark,

ClusterCATS will not redirect the request. This feature is an alternative to the "Do not redirect" feature.

Note This feature can be defeated by using absolute links in a page. By doing so, the HTTP request is routed back to the cluster entry point and redirected according to the current load threshold and without regard to the state of the requesting client. To avoid this inadvertent loss of state, be sure to use only relative linking in your application pages.

To set up session aware load balancing:

1. In the ClusterCATS Explorer Main window, right click on the cluster where you want session-aware load balancing enabled. Select Configure > Administration. The cluster properties dialog box displays.
2. On the Administration tab, click on the, Enable session-aware load balancing box to enable this feature.

HTTP POST Redirects

Most web-based forms use the HTTP POST command instead of the HTTP GET to send data back to the server. The reason for this is that POST allows you to hide the data from the user whereas the GET command includes the data as parameters in URL.

Netscape Navigator and Internet Explorer Browsers turn redirected POST commands into GET commands, therefore, ClusterCATS hides the data and assigns it a unique ID. It then sends the data to the server and modifies the URL so it includes the unique ID. Once connected to the server, the URL ID is matched with the data so that the server can correctly process it.

ClusterCATS on Solaris

Because there is no ClusterCATS Explorer on Solaris, a number of utilities are available for managing the ClusterCATS server installed on Solaris systems:

- ClusterCATS server commands for stopping, starting, and administering the ClusterCATS server on Solaris.
- A variety of network management tools to check the Bright Tiger configuration, display information about host systems running Bright Tiger, and a packet-sniffing tool for displaying packets being sent to a specific network interface card (NIC).

ClusterCATS server commands

Bright Tiger ClusterCATS provides several commands for configuring and managing your ClusterCATS server on Solaris. These commands allow you to configure your ClusterCATS Server options and to manage the ClusterCATS daemons. Once the Bright

Tiger ClusterCATS Server has been installed on Solaris, there is no need to manage the Server components unless you wish to reconfigure one of the Server options. The three main commands are:

- `btadmin`
- `bt-start-server`
- `bt-stop-server`

See Using the Solaris btadmin Utility for more information about the btadmin utitility and "Using the Solaris bt-start and bt-stop Utilities" on page 107 for more information about bt-start-server and bt-stop-server.

Using the Solaris btadmin Utility

The btadmin utility takes several different forms:

- For starting and stopping daemons
- For enabling or disabling Bright Tiger options
- For configuring Bright Tiger options
- For showing and resetting options, and for getting online help

Stopping and starting daemons with btadmin

```
btadmin [start/stop/restart daemon]
    [configure option]
```

You can start and stop the following daemons with btadmin.

Starting and Stopping daemons with btadmin	
Daemon	**Description**
appmgr	Application manager daemon.
failover	Failover daemon.
ns-httpd	HTTP daemon.

Examples

```
btadmin start appmgr
btadmin stop failover
btadmin restart ns-httpd
```

Enabling and Disabling options with btadmin

btadmin [enable/disable *option*]

You can enable or disable the following Bright Tiger options with btadmin.

Enabling and Disabling options with btadmin	
Option	**Description**
btcats	Bright Tiger ClusterCATS server
failover	Server failover (ipaliasd)
ns-httpd	HTTP daemon

Examples

```
btadmin enable btcats
btadmin disable failover
```

Configuring Bright Tiger options with btadmin

`btadmin [configure option]`

Use btadmin with the configure option to configure the following Bright Tiger options.

Configuring Bright Tiger options with btadmin	
Option	**Description**
btcats	Bright Tiger ClusterCATS server
failover	Server failover (ipaliasd)
load	Load Balancing preference
nsroot	Configure new Netscape Server root directory (used when Netscape Server is moved).

Examples

```
btadmin configure btcats
```

Resetting the cluster with btadmin

You can reinitialize your ClusterCATS cluster configuration on the current server using the following form of the btadmin utility:

```
btadmin reset
```

Showing the current ClusterCATS Server configuration

You can display the ClusterCATS Server settings on the current server using the following form of the btadmin utility:

```
btadmin show
```

Getting help for btadmin

To get help for the btadmin utility, use the help option:

```
btadmin help
```

Using the Solaris bt-start and bt-stop Utilities

The bt-start-server and bt-stop-server utilities can be used to stop and start the Netscape Server.

```
bt-stop-server [-f]
```

Use the -f option to stop the Netscape server without prompting the user for confirmation.

```
bt-start-server
```

Starts the Netscape server.

Solaris Network Management Tools

A number of Bright Tiger network management tools are provided that you can use to troubleshoot and analyze your server systems and network.

- btcfgchk — Displays information about your IP and DNS configurations.
- hostinfo — Displays information about a specific domain name.
- sniff — Displays packets that a specific network interface card is hearing.

Using btcfgchk

To run btcfgchk use the following syntax:

```
/<bt-installdir>/program/btcfgchk
```

The following sample output shows how btcfgchk reports configuration information for a system with one network adapter, and two IP addresses:

```
btcfgchk FQHN is hartford.brighttiger.com
El90x1 [PRIMARY]:
```

```
hartford.brighttiger.com        192.168.0.31
255.255.255.0
hartford.brighttiger.com

hartford1.brighttiger.com       192.168.0.32
255.255.255.0
hartford1.brighttiger.com
```

Errors reported by btcfgchk

Errors reported by btcfgchk generally involve a misconfiguration of your DNS Server. Bright Tiger requires that DNS be setup to provide both forward and reserve mappings. Forward mapping is when the hostname is translated to an IP address. Conversely reserve mapping is taking an IP Address and mapping it to its hostname. ClusterCATS expects the mapping to be 1 to 1 (one hostname, one IP Address).

The following table shows errors btcfgchk may report.

Errors reported by btcfgchk	
Error	**Explanation**
Hostname does not map to a single IP address	The main hostname for this system is not mapping to 1 IP address. Possible problems are: The main hostname of the system could not be resolved to any IP address. The DNS tab of the TCP/IP property sheet in the network control panel applet shows you the hostname and the domain. Your fully qualified hostname is the combination of these two fields. Make sure there are no typos in these names. If using DNS, type: `nslookup <fully qualified hostname>` This will verify that the hostname is correct. If you're using local hosts file, look in the hosts file (`/etc/hosts`) to make sure the fully qualified hostname entry contains no typos. There is a DNS entry for this name. or: The hostname is a DNS Round Robin name. If you run the Bright Tiger hostinfo tool and see more than one IP address, this is the problem.
No adapter associated with hostname found	btcfgchk is unable to find the PRIMARY network adapter. The PRIMARY network adapter should be the network adapter containing the IP address of the main hostname.
Error: Duplicate Primary Adapter	btcfgchk found two network adapters with the same IP address. Use the command `ifconfig -a` to look at your adapter information.

Errors reported by btcfgchk	
Error	**Explanation**
Name lookup for <hostname> failed	btcfgchk was not able to determine the IP address for the specified host. Possible problem: • Your DNS server may be down. Use nslookup to see if it can contact your DNS server.

<IP address 1> reverse maps to <hostname> which then forward maps to <IP address 2>	btcfgchk did a lookup on <IP address 1> and found what hostname it is mapped to. It then took the hostname returned and verified that this name maps back to the IP address specified. The verification failed.
	There is likely an issue with your DNS setup. Use Bright Tiger hostinfo the tool to gather more information on how the names/IP Address are configured.
	`hostinfo <IP address 1>`
	`hostinfo <hostname returned from initial hostinfo>`

Error looking up <hostname> by name	Bright Tiger could not resolve the given hostname to an IP addresses. Use nslookup to look up the hostname in DNS, or look in your `/etc/hosts` file if using local hosts file.
Hostname a round robin name, or does not map to configured IP address	The hostname maps to more than 1 IP address (DNS Round Robin) or maps to an IP address not found on this machine. Use the Bright Tiger tool: `hostinfo <hostname>` If you see more than one IP address, it is DNS Round Robin. If you see one IP address, check to see if that address is configured on this machine. You can use `ipconfig/all` to view the IP addresses on this machine.
Hostname not found in any reverse mapping Probable forward mapping misconfiguration for <hostname>	For each IP address found on the system, an attempt was made to find the corresponding hostname. None of the IP addresses on the system reverse mapped to the system's main fully qualified hostname. The problem is either: • The hostname maps to the wrong IP address. • The IP address that the hostname maps to does not have an entry in the DNS for the reverse map. nslookup does not return the hostname.
Probable round robin configuration for <hostname>	The hostname does not map to a single IP address. Use the hostinfo tool to view the IP address it maps to.

Using the Bright Tiger hostinfo utility

Hostinfo displays information about a specific domain name.To run hostinfo:

```
#cd <btinstall-dir>/program/
```

Set the default directory to the Programs Directory under Bright Tiger.

```
#<btinstall-dir>/program> hostinfo domain_name
```

The following shows sample output for hostinfo for a set of DNS round robin host names.

```
##<btinstall-dir>/program> hostinfo www.brighttiger.com
Information for host 'www.brighttiger.com':

FQHN: www.brighttiger.com
Primary Address: 0.0.0.0
Domain: .brighttiger.com
Aliases: btweb1.brighttiger.com
    btweb2.brighttiger.com
    www.brighttiger.com
Addresses: 444.87.27.76 444.87.27.77
```

Hostinfo displays the domain name, the primary address and any aliases. If the primary address is 0.0.0.0, the domain is using round robin and the round robin names will appear under the Alias and the round robin addresses will appear under Addresses.

Using the Bright Tiger sniff utility

Sniff displays packets that a specific Network Interface Card (NIC) is hearing. To run sniff:

```
#/<btinstall-dir>/program/sniff
```

The following shows sample output for sniff:

```
Mail Test Environment Variables:
   BTMailHost,     BTSender,       BTRecipients,   BTSubject,    BTText
 Packet Test Environment Variables:
   BTPort,         BTMcastTTL,     BTUcastCount,   BTBcastCount,
BTMcastCount
   BTSendInterval, BTDoLocalBind,  BTUcastAddress, BTBcastAddress
   BTMcastAddress, BTLocalAddress, BTSendSize,     BTRecvSize
   BTConsole,      BTLogFile,      BTSystem

 Press keys at run-time:
  d - dump sniff configuration information
  H - display this and more help
  h - display this help
  l - run load balance test thread
  m - run mail test thread
  p - toggle packet dump display
  q, <ESC>, <ENTER> - quit all active threads and exit
  r - run UDP listener thread
```

```
  s - run packet test thread
  x - execute system command

Use the "r" command within sniff to listen to intra-cluster packets:
Listen Thread thread running on 'any' interface...

[ SrvHello    @ Tue Jun 30 17:01:57 1998] 192.168.0.213
boston1.brighttiger.com          (192.168.0.118  ) (255.255.255.0  )
sales_automation   Mcast V1.2    Available   2/90
[[ SrvHello    @ Tue Jun 30 17:01:57 1998] 192.168.0.213
somewhere.brighttiger.com        (192.168.0.213  ) (255.255.255.0  )
```

CHAPTER 7

Using CGI with ColdFusion

This chapter describes how to use ColdFusion with a Web server that does not support one of the major APIs.

Contents

CGI vs. Web Server APIs

The Common Gateway Interface (CGI) was introduced as a standard protocol for extending the functionality of Web servers with additional applications. Most CGI applications are simple executables that are launched every time they are requested. ColdFusion uses a more robust architecture. The ColdFusion Application Server runs as a multi-threaded system service and handles all of the complicated processing. The Application Server communicates with the Web server either through a very small CGI executable referred to as the stub (`cfml.exe`) or through a native Web server API.

As Web servers have developed, each vendor has introduced and implemented an application programming interface (API) for their server. The native Web server APIs offer additional features and significantly increased performance. Instead of launching a CGI executable, servers supporting an API communicate directly with the ColdFusion application server through a DLL.

In addition to introducing server APIs, many server vendors have created document type mapping, so that individual document extensions can be associated with a process. This makes it possible to create ColdFusion application pages that are stored directly in the Web server's root directory.

ColdFusion supports the following major native Web server APIs:

- Netscape API (NSAPI)
- Internet Server API (ISAPI)
- Website API (WSAPI)
- Apache API

These APIs and document type mapping are supported by these servers:

- Netscape Enterprise and FastTrack Servers
- Microsoft IIS (all versions)
- WebSite (1.1 and Pro)
- Apache

Limitations of CGI

You can use ColdFusion with a server that does not support one of the APIs and document type mapping. However, you will not be able to use the following features:

- Document type mapping. This eliminates the need for URLs that reference the ColdFusion executable file (e.g., `/cgi-shl/cfml.exe?template=`).
- Native Web server security. With document type mapping you can put ColdFusion application pages into the Web server's document directory. This enables you to use the Web server's security to protect application pages.

- Relative mappings. When application pages are stored in the Web server document directory, you can use relative URLs to refer to graphics and other files.
- Increased performance. You will not realize the increased performance provided by the Web server APIs.
- Example applications. The example applications installed with ColdFusion will not work without a server that supports one of the standard APIs.

Referencing Application Pages with CGI

ColdFusion includes a CGI script (`cfml.exe`) that is executed by your Web server whenever a user submits a form or clicks a link that references it. The CGI script communicates with the ColdFusion Application Server.

URLs and the cfml.exe script

You are probably familiar with using URLs to refer to documents and images on the Web (e.g., `http://www.myserver.com/homepage.htm`). URLs also support an extended syntax that allows you to call CGI programs and pass them parameters.

To invoke `cfml.exe` from a URL, specify the logical path to the executable on your server along with a `template` parameter indicating which application page file to use in processing the request.

To pass parameters to the script, you append a "?" to it and then specify a list of parameters in a 'key=value' format (delimited by the & character).

For example, to call the script and tell it to use an application page file called `myquery.cfm`, you would use the syntax:

`/cgi-shl/cfml.exe?template=myquery.cfm`

You can call the same application page with an additional parameter `Employee_ID=346` using the syntax:

`/cgi-shl/cfml.exe?template=myquery.cfm&Employee_ID=346`

The `cgi-shl` entry italicized in the preceding examples represents the path to your Web server's CGI directory. Your server's CGI path may be different from this (other common paths are `cgi-bin` and `scripts`). You should consult your Web server's documentation to determine the appropriate path and (if necessary) use this path instead of `cgi-shl`.

One good way to verify that your server is able to access `cfml.exe` is to create a simple form without input fields that has an ACTION that calls the `cfml.exe` script with no arguments (for example, `ACTION="/cgi-shl/cfml.exe"`). If the script is accessible, your server returns an error message that indicates an application page was not specified. If `cfml.exe` is not accessible, your server returns an error message that indicates it cannot find the script.

Application page references

The reference to the file `myquery.cfm` in the above example contains no path information. You may be wondering how ColdFusion determines where on your system to locate this file.

If you place ColdFusion application pages in the `cfdocs` directory, you can reference them using only their base name. For example, if a file called `myquery.cfm` is in the `cfdocs` directory, you need only specify `myquery.cfm` to refer to it.

If you create subdirectories within the `cfdocs` directory, you can reference application pages within them using their subdirectory names. For example, if you put `myquery.cfm` in a subdirectory called `sales`, you would use `/sales/myquery.cfm` to refer to it. The URL reference to this file would then be:

```
/cgi-shl/cfml.exe?template=/sales/myquery.cfm
```

To simplify URLs for your users, you can create mappings that point to directories. These mappings work like your Web server's document mappings, but they only refer to application pages. Define mappings on the Mappings page of the ColdFusion Administrator.

CHAPTER 8

Configuring Basic Security

Basic ColdFusion security allows you to secure a number of ColdFusion Server resources with password access. This chapter describes configuration options for basic ColdFusion security.

Contents

About Basic Security

ColdFusion Server offers two levels of security: Basic and Advanced. Basic security allows you to impose the following types of control on the ColdFusion development environment:

- You can secure the ColdFusion Administrator with a password.
- You can secure access from ColdFusion Studio to data sources and files with a password.
- You can restrict the execution of specific ColdFusion CFML tags.

To access Basic security settings in the ColdFusion Administrator, open the Server, Basic Security page.

Advanced Security allows you to exercise a high degree of control over a wide range of ColdFusion resources, including CFML tags (as well as individual tag ACTION types), specific SQL operations, as well as other ColdFusion resources. For more information, see Chapter 9, Configuring Advanced Security.

Installation defaults

The ColdFusion Administrator installs with secure access enabled. The password you enter as part of the setup is saved as the default, so that when you open the Administrator for the first time, you are prompted to enter the password. We recommend that you continue to use Administrator security until you complete the ColdFusion server configuration. Once you've determined your security requirements, you may decide to set up Advanced security. For more information, see Chapter 9, Configuring Advanced Security.

Disabling Administrator security

You can disable Basic security for the ColdFusion Administrator on the Server, Basic Security page. Once you've disabled this option, anyone can open the Administrator pages and make changes to ColdFusion Server settings.

Disabling ColdFusion Studio security

You can disable file and data source security from ColdFusion Studio on the Server, Basic Security page. With Basic security disabled, you rely on the Web server's security to set permissions to ColdFusion application and document directories. In addition, you rely on your database settings to control access to data sources.

Configuring Basic Remote Development Security

Restricting access to your application page directories is the most important step you can take in making your site secure. You can do this using ColdFusion Basic security. However, you may find it necessary to provide broader access to these directories if, for

example, you have several geographically dispersed participants in a development project. In addition, a group of widely dispersed developers may require different levels of access to files and data sources.

Securing data sources

In addition to your application pages, you also need to consider data source security. Using basic security measures, you can take several steps to ensure that your data sources remain secure even when your application page directories are partially accessible:

1. If you don't need to insert, update, or delete data in the data source, configure it as read-only. You can do this in the ColdFusion Administrator ODBC Data Source Advanced page.
2. Use a database system that supports security and create a user account that has access to only selected tables and operations (such as, SELECT, INSERT). You can then configure ColdFusion to use that account when interacting with the data source.
3. Using the ColdFusion ODBC or Native Drivers page, configure ColdFusion settings to allow only certain SQL operations (such as SELECT and INSERT) in interactions with the data source.

ColdFusion Remote Development Services (RDS)

ColdFusion RDS is a component of ColdFusion Server used by the ColdFusion Administrator and ColdFusion Studio to provide remote HTTP-based access to files and databases. You can use RDS to manage ColdFusion Studio access to files and databases on a server hosting ColdFusion.

RDS provides both Basic and Advanced security services for ColdFusion, allowing you to configure the level of security you need for your situation. For more information see Chapter 9, Configuring Advanced Security.

Basic security options managed by RDS can be found in the Administrator Server, Basic Security page, where you'll find options for defining passwords and securing a subset of ColdFusion tags.

Basic Security limitations

ColdFusion Basic security hinges on the protection of a single password per server. So long as the password is kept secret, unauthorized access to the files and databases on the server is impossible. It's important to understand that this security model has two liabilities:

1. Password vulnerability. The password can be lost, stolen, or hacked.

2. Access control is generalized, that is, remote developers have access either to all files and data sources, or none. With Basic security, you can't protect individual directories and or databases.

Securing ColdFusion file resources

The following table shows how ColdFusion Basic security compares with native OS options available to you in securing files for remote development.

Securing Files from ColdFusion Studio		
Method	**Description**	**Security Model**
LAN-based	Uses the native file system to provide access to local and network drives.	Access is determined by the network permissions of user logged into workstation where Studio is being run.
FTP-based	Connects to an FTP server running on same machine as the target web server.	Permissions defined using the native security of the FTP server software.
RDS-based	Interacts with the remote file system using RDS on the target ColdFusion Server.	Files on the target server can be secured with the ColdFusion Studio password.

Securing ColdFusion data sources

The following table shows how ColdFusion Basic security can be configured to secure ColdFusion data sources.

Securing Data Sources from ColdFusion Studio		
Method	**Description**	**Security Model**
Basic security is enabled on the local workstation.	Data sources are accessed through RDS on the local ColdFusion Server.	Data sources that are accessible to the user locally are accessible through ColdFusion Studio.
Basic security is enabled on the remote server.	Data sources are accessed through RDS on the remote ColdFusion Server.	Data sources that are accessible to ColdFusion Server are accessible remotely via ColdFusion Studio.

By using a LAN based file access model and by restricting developer data source access to the local workstation, a very secure development environment can be achieved.

Using a Password to Restrict Access to RDS

The Server, Basic Security page of the ColdFusion Administrator is used to configure passwords for securing the Administrator and for preventing unauthorized access to ColdFusion data source and file resources through ColdFusion Studio.

Note Password protection is enabled by default at server installation time. If you have not explicitly disabled password access, then security is already configured for your server.

ColdFusion Studio Password

The ColdFusion Studio password, like the Administrator password is specified during ColdFusion setup. You can specify a new password in the Administrator to control database and file access from Studio. Separate Studio and Administrator passwords allow you to separate access control to ColdFusion data sources and files, and Administrator pages.

Note Whenever you make a change to Basic security settings, you need to stop and restart the ColdFusion RDS service using the Services Control Panel in Windows or the stop and start scripts on Solaris.

For more information, see Starting and Stopping ColdFusion, in Chapter 3.

Removing password-based access control: Windows

To allow ColdFusion Studio users access to files and databases without being prompted for a password:

1. In the Administrator Server page, clear the ColdFusion Studio password checkbox.
2. Open the Services Control Panel.
3. Stop and then restart the ColdFusion RDS service.

Removing password-based access control: Solaris

To allow ColdFusion Studio users access to files and databases without being prompted for a password:

1. In the Administrator Server page, clear the ColdFusion Studio password checkbox.
2. Run the ColdFusion Stop script.
3. Run the ColdFusion Start script.

Configuring Basic Runtime Security

The ColdFusion Administrator Server, Basic Security page allows you to disable execution of several CFML tags that could present security hazards:

- CFDIRECTORY
- CFFILE
- CFCONTENT
- CFOBJECT
- CFREGISTRY

When a specific tag restriction has been configured ColdFusion presents an error message when it encounters a restricted tag. For more information about these tags, refer to the ../../CFML_Language_Reference/contents.htm*CFML Language Reference*/a.

CHAPTER 9

Configuring Advanced Security

This chapter describes how to setup and configure ColdFusion Server with Advanced security features that allow you to protect a wide variety of ColdFusion resources.

Contents

Security Overview

Security options in ColdFusion have been greatly enhanced in this release. ColdFusion Server now supports several different types of Advanced Security:

- **User security** — Implemented in ColdFusion application pages by the ColdFusion developer. User Security offers runtime user authentication and authorization. See "Implementing User Security" on page 130 and ../../Developing_Web_Apps/contents.htm*Developing Web Applications with ColdFusion*/a for more information.
- **Remote Development Security (RDS)** — Where developers accessing server resources through ColdFusion Studio are authenticated before receiving access to protected resources. See ../../Developing_Web_Apps/contents.htm*Developing Web Applications with ColdFusion*/a for more information about RDS.
- **Server sandbox security** — Controlled by the ColdFusion administrator of a hosted site, offers runtime security based on directory access at hosted sites (ColdFusion Enterprise only). See "Implementing Server Sandbox Security" on page 131 for more information.
- **Administrator security** — Individual administrative operations can be secured against unauthorized access.

Choosing Advanced Security in the ColdFusion Administrator overrides any settings you may have made in the Basic Security Administrator page.

Note Advanced security is not currently supported in ColdFusion Server for Solaris.

Security Concepts

ColdFusion advanced security consists of the following elements:

Advanced Security Concepts	
Term	**Description**
Security contexts	At the top level of the security hierarchy, the security context is a kind of container in which rules, policies, and users are referenced.
Security rules	You use rules to define the access restrictions you want for a particular ColdFusion resource, such as defining which SQL statements are allowed to be executed against a specific data source or which CFML tag ACTIONS are restricted.
Users/groups	Individual users and groups are authenticated within a particular domain. A security domain can be a specified Windows NT domain or an LDAP directory.

Advanced Security Concepts (Continued)	
Term	**Description**
User directories	Defines the mechanism to use when authenticating users. Available mechanisms are: A Windows NT domain, which authenticates users with accounts on the server you specify; an LDAP directory to store user and group account information.
Security policies	A policy associates specific users or groups with a set of resource restrictions that these users have access to. These restrictions are in the form of rules, such as allowing a particular user or group to execute a SQL UPDATE on a particular data source.
ColdFusion resources	ColdFusion resources are things like data sources, Verity collections, ColdFusion tags, custom tags, specific files and so on.
Security server	A hostname or IP address you specify where the security authentication and authorization services run. These services are used to authenticate individual users or groups.
Security sandboxes	A security framework established by applying a particular security context, with all that it contains, to a directory structure. Intended mainly to help ISPs hosting ColdFusion applications to partition application pages in individually secure areas.

Implementation summary

ColdFusion advanced security is implemented by defining the following elements in order:

1. A security server.
2. A security context.
3. A user directory, either an NT domain or an LDAP directory.
4. Rules governing particular ColdFusion resources.
5. Users and groups for whom the rules will apply.
6. Policies that group users and rules together into logical elements.

Installing Advanced Security

Advanced Security is not installed by default during ColdFusion setup. To use the User security features, you must choose the Advanced Security option when installing ColdFusion 4.0.

To install Advanced Security on Windows:

1. Run the ColdFusion setup and choose the Advanced Security Services option in the Select Web Server options window.

   Choosing Advanced Security during the installation procedure causes the Microsoft Active Directory Services Interface (ADSI) Version 2.0 Setup window to appear.

2. Click Yes to install ADSI.
3. Read and accept the licensing agreement, and click OK when the installation finishes.
4. Restart your computer before accessing the ColdFusion Administrator.

See ../../Getting_Started_with_ColdFusion/contents.htm*Getting Started with ColdFusion*/a for more information about installing the ColdFusion Server.

Note Advanced Security will be supported in Solaris in a future release of ColdFusion.

ColdFusion Remote Development Security (RDS)

ColdFusion RDS provides security services to developers working in ColdFusion Studio. RDS is at the core of the security framework in a team-oriented ColdFusion development environment where groups of developers, working in ColdFusion Studio, require different levels of access to ColdFusion files and data sources.

Working in ColdFusion Studio, developers access these ColdFusion resources remotely, opening *.cfm files or accessing data sources. RDS authenticates users granting access only to those resources appropriate to their login. Authentication is carried out against the NT domain server or an LDAP directory specified in the Administrator as part of a security context.

RDS and Basic security

In addition to Advanced security and debugging, RDS also provides basic security for ColdFusion. Access to RDS for Basic security is enabled by specifying a ColdFusion Studio password on the Administrator Basic Security page. RDS security protects ColdFusion Server data sources and files, and enables file browsing and debugging as well. To access these resources, developers in ColdFusion Studio must supply a password which, when authenticated, permits access to RDS: file browsing, editing, database operations, debugging, and so on.

For more information, see Chapter 8, Configuring Basic Security.

Configuring RDS

In order to implement RDS, you use the ColdFusion Administrator to:

1. Define a security server. See "Setting Up a Security Server" on page 125 for more information.
2. Create a security context, defining the scope of the security you want to implement. See "Defining a Security Context" on page 128 for more information.
3. Set up rules and policies that match secured resources with authorized users. See "Creating Rules and Policies" on page 129 for more information.

With a security context defined, developers working in ColdFusion Studio connect to the ColdFusion Server and access resources such as files and data sources according to the rules and policies associated with their logins.

For more information about configuring RDS in ColdFusion Studio, see ../../Developing_Web_Apps/contents.htm*Developing Web Applications with ColdFusion*/a.

Setting Up a Security Server

When setting up a Security server in a non-clustered environment, the Security server is the server hosting ColdFusion, where your ColdFusion programming resources, files, data sources, custom tags, Verity collections and so on, are found. In a clustered environment, you can define a single Security server in the cluster to handle all security authentication and authorization. In this case, the other servers in the cluster all point to the Security server to authenticate and authorize users and groups.

Note You can only administer Advanced Security from the Security server.

To set up a security server:

1. Open the ColdFusion Administrator. In the Server section, select the Advanced Security page.
2. Select the Use Advanced Server Security check box. This enables you to set up a security context with policies, rules, and users.
3. Enter the physical location of the security server and click Apply. By default, this is the localhost IP# 127.0.0.1. You can supply an IP address or a logical name that can be resolved to a physical address.
4. Enter a Shared Secret, which is part of the encryption key that validates Advanced security transactions. Since the default is the same for all ColdFusion Server configurations, you should change the shared secret at least once.
5. ColdFusion reserves the Authorization and Authentication ports to pass security information. Change the port number values only in the unlikely event that these ports are already in use by some other process on the specified server.
6. Click to enable the Security Server Cache if you want ColdFusion to cache security information on the security server. This can improve performance since cached security data can be used instead of querying the security server for each operation. This cache is flushed every two hours.

7. Click to enable the ColdFusion Server Cache option if you want ColdFusion to cache security transactions. Enabling this cache can help improve performance. This cache is flushed every two hours.
8. Click to enable Security Sandbox Settings if you want to activate existing security sandbox settings. See "Implementing Server Sandbox Security" on page 131 for more information.

   You can also change the Refresh Interval setting, which determines how often a cache gets flushed. Since both user session and rules use two cache buffers apiece, if you set the refresh interval to 1 hour an entry will be cached for a minimum of 1 hour and a maximum of 2 hours.

   The Maximum Cache Entries option sets the maximum number of entries for each cache buffer. If you exceed the number, a warning is written to the `server.log` file.

Next step: Identifying User Directories.

Identifying User Directories

User and group authentication is carried out against either an existing Windows NT domain or an LDAP directory. When you set up Advanced security, you must specify at least one user directory.

Windows NT domains

Authenticating against a Windows NT domain makes sense if you are already working in a Windows NT environment or will be deploying your application code to a Windows NT environment. This method is a very quick way to implement ColdFusion Advanced security, since users and groups have already been defined. ColdFusion Advanced security doesn't provide any user/group management facilities. You manage users and groups using the Windows NT User Manager for Domains administrative utility.

Specifying an LDAP User Directory

Although ColdFusion includes a Netscape LDAP directory you can use as a user directory, you can specify any LDAP directory you may already have to provide authentication services for Advanced security. As with the Windows NT domain, you use native LDAP management tools to add or change user or group information.

To identify a user directory:

1. In the Advanced Server Security page of the Administrator, click the User Directories button.
2. Enter a name for the user directory in the User Directory text box and click Add.

3. In the New User Directory page, enter descriptive information about the directory you are creating.
4. Select Windows NT or LDAP in the Namespace drop-down menu.
5. Enter a valid server name. If you chose Windows NT as the namespace, the server name must match the domain server name. If you chose LDAP as the namespace, the server you specify must host a valid LDAP directory.

   You can add multiple user directories; once defined all user directories become available to the security contexts defined for this security server.
6. Enter a username (user's Distinguished Name DN) and corresponding password if applicable.
7. Click to enable Secure Connect to implement encrypted transmission of authentication information. Secure Connect must be enabled when accessing an LDAP server over Secure Sockets Layer (SSL).

The Add User Directory to Existing Security Context box is checked by default. This setting enables you to add users to existing security contexts automatically. If you disable this option, users must be manually associated with a security context.

Entering LDAP directory options

If you selected LDAP as the domain namespace when defining a new user directory, you need to enter information to help ColdFusion interact with the LDAP directory.

To define LDAP options:

1. Enter a Search Root. The Search Root must point to the branch of the LDAP tree where a user namespace logically begins. Typically, this branch represents an "organization" or an "organizational unit" and corresponds to one user directory.
2. Enter a Lookup Start. Used to construct the non-unique beginning of the DN string. An example would be: *uid=*.
3. Enter a Lookup End. Used to construct the part of the DN string that follows user ID. An example of a lookup end would be: *,ou=marketing,o=widgetinc.com*.
4. Enter a Search Timeout. Indicates the maximum amount of time (in seconds) you want a directory search to take.
5. Enter a Search Results. Enter the maximum number of results you want the search to return.
6. Select a Search Scope from the drop-down list. Enter the depth of your search. For example, if you want to be able to access everything under the search root, select the Subtree option. Otherwise, select the One Level option.
7. Click Add.

The Add User Directory to Existing Security Context box is checked by default. This setting enables you to add users to existing security contexts automatically.

Next step: Defining a Security Context.

Defining a Security Context

The Security Context is a logical set of resources grouped together from an administrative perspective. It does not necessarily correspond to a ColdFusion application or resource name. As its name suggests, the security context is used to establish a context in which authentication and authorization actions are carried out.

For example, you might create a security context for a particular application development effort. Within this context, you define users, groups, and rules that apply to the developers who are working on the project. Another example: You define a context for intranet users of the application you want to deploy. According to their group affiliation, different rules apply, enabling or preventing various actions based on their login.

The context helps establish which resources you want to protect.

To define the resources to be protected:

1. Open the Advanced Server Security page and click the Security Contexts button.
2. Enter a security context name and click Add.

   This is a logical name that defines the scope of the security domain. Later, in your application pages, you use this name in the CFAUTHENTICATE tag.
3. In the New Security Context page, add a description of the security context.
4. Choose the Resource Type this context governs. For these types, you also provide a corresponding name:
   - Application — Use the application name.
   - CFML — Provide a CFML tag name.
   - Collection — Provide the collection name.
   - Component — This can be a CFApplet source name, CFX name, or CFOBJECT Class name.
   - CustomTag — Specify a fully qualified file name (using forward slashes).
   - DataSource — Use ODBC or Native Driver Source Name.
   - File — Use '/' forward slashes.
   - UserObject — A logical entity you can define to use as a kind of security flag. For example, you could define TopSecret, Secret, and Confidential user objects and authenticate users based on their association with these flags.

   Avoid selecting ColdFusion resources that you do not intend to secure, since doing so can needlessly affect performance.

   The Add Existing User Directories box is checked by default to let you add users to this context automatically.
5. Click Add.

   The security context is registered. Now you define the policies and rules for this context.

Creating Rules and Policies

Within a security context, you establish rules that protect specific resources. For example, you might create a *rule* to limit write access to files at a specific pathname. A rule determines what action can be performed on a resource.

Once you've defined access rules, you define a security *policy* that matches rules to users and groups. You grant access to a protected resource by adding both rules and users to a policy. The users and user groups you add to a policy (you can think of them as *policy holders*) are authorized to use the resources protected by the security context rules, which are assigned to the policy.

In other words, a rule is a key to a door that guards access to a resource. When you create a rule, it means the key needed to open the door to this resource is available. Who will get this key is decided when you create a *policy* that includes this rule.

To establish rules about access to resources:

1. From the Advanced Server Security page, click Security Contexts.
2. On the Registered Security Contexts page, select an existing security context. The Edit Security Context page appears.
3. Click the Rules button.
4. In the Resource Rules page for the current context, provide a rule name.

   Rule names are user-defined logical names. Make the rule name easy to remember and to associate with the resource it protects. For example, if you're writing a rule to protect CFQUERY tag, you might name the rule CFQUERY. If you're writing a rule to protect all access to a particular data source, you might name it *DatasourceName*_All.
5. In the Resource Type drop-down menu, select a resource type that you want to protect. Click Add.
6. In the New Resource Rule window, describe how the rule works and click Add.

Note In the Resource Rules page, you might also create additional rules for this security context — for example, to restrict updating of data sources.

To create policies that match rules with user groups:

1. From the Advanced Server Security page of the Administrator, click the Security Contexts button.
2. On the Registered Security Contexts page, click on a security context.
3. In the Edit Security Context page, click the Policies button.
4. Provide a policy name and click Add.

   For example, you could create a top-level security policy, called **Platinum**, to grant to certain users broad access to protected resources.
5. Write a description of the policy and click Add.

The Resource Policies window appears showing the available Policies for the current Security Context. Now you can assign a policy to various rules and users.

Adding Users and Groups to a Security Policy

ColdFusion Advanced security works by authenticating users and then authorizing the actions that are to be performed on a set of ColdFusion resources that have been defined in the security context. In order for authentication to work, you need to identify and define users to ColdFusion. A policy associates rules defining access to various ColdFusion resources with a set of users.

To add users and groups to a policy:

1. From the Advanced Security page in the ColdFusion Administrator, click the Security Contexts button.
2. Select an existing security context or create a new one. On the Edit Security Contexts page, click the Policies button. ColdFusion opens the Resource Policies page for the current security context.
3. Click to open an existing policy, or define a new one. ColdFusion opens the Edit Security Policy page.
4. Click the Users button to open the Users page for the current policy. Click the Add/Remove button. ColdFusion opens the Add/Remove Users page for the current policy.
5. Select from the available groups on the right side of the list control and click the left arrow to add them to the current policy. To add individual users, you enter a login name in the Enter User box and click Add. You're done.

Note Only groups are displayed when adding users to a policy. To enter an individual user, you must know the user login and enter it in the Enter User box. A list of all possible individual users, which could easily number in the thousands, would be a very impractical means of adding individual users to a policy.

The users you have added to the security policy are now subject to the rules that you have also defined and added to the policy.

Implementing User Security

The User Security feature allows ColdFusion developers to authenticate users and match protected resources with authorized users. User Security consists of several parts:

- The **Security Context** defines the scope, or the security domain, of protected resources.
- **Rules** define access permissions for a particular resource.

- **Policies** match rules to users and user groups. They protect ColdFusion resources and explicitly allow access to users.
- **User Directories** can be NT Domains or LDAP servers.

To implement runtime user security for applications, you use the ColdFusion Administrator to set up the security server, create a security context for your application, and set up rules and policies that match secured resources with authorized users. See "Setting Up a Security Server" on page 125 for details on setting up the security server.

After the security framework is in place, you use the CFAUTHENTICATE tag in individual application pages (or the `Application.cfm` file) to authenticate users. The IsAuthenticated and IsAuthorized functions enable developers to offer or deny access based on the established security policies. See the ../../CFML_Language_Reference/contents.htm*CFML Language Reference*/a for more information on IsAuthenticated and IsAuthorized.

Implementing Server Sandbox Security

ColdFusion Server Enterprise edition supports server sandbox security for hosted sites. This security feature, controlled by the ColdFusion administrator of a hosted site, offers runtime security based on directory access at a hosted site.

Sandbox security is enforced by the ColdFusion Server, using the path location established for the security sandbox in the ColdFusion Administrator. When Server Sandbox security is turned on, ColdFusion Server will throw a security exception if a developer attempts to use tags or resource types that aren't authorized in the Sandbox.

To enable server sandbox security:

1. Open the ColdFusion Administrator and choose Advanced Security.
2. Select the Use Security Sandbox Settings check box. Then click the Security Sandboxes button.
3. Enter a fully qualified path (using forward slashes) as a location for the Security Sandbox, and click Add to register the sandbox.
4. Enter an existing security context for the sandbox.
5. Enter a username and password for the sandbox user. This user must be a member of an already registered user directory.

Note If both user security and server sandbox security are enabled, sandbox security takes precedence.

About Securing ColdFusion Resources

ColdFusion Advanced Security allows you to secure the following resource types:

- Applications
- CFML tags
- Verity collections
- Components such as a CFApplet, CFX, or CFOBJECT Class name
- CustomTag
- DataSources
- Files
- UserObjects

Securing one of these resource types means defining a set of rules that identify the resource and, in the case of CFML tags, for example, the set of actions you want to secure. With a rule defined, you then associate the rule with a user or group.

There are several contexts in which security comes into play:

- At runtime: With a security context defined, ColdFusion developers can build authentication logic into application pages using the CFAUTHENTICATE tag. See ../../Developing_Web_Apps/contents.htm*Developing Web Applications with ColdFusion*/a.
- From ColdFusion Studio: ColdFusion Studio users are authenticated and their access to files and data sources authorized before they can edit files or manipulate data sources.
- Pages and functions in the ColdFusion Administrator: Since the Administrator is the locus of all security management functions, as well as data source, performance, and scheduling, you may need to define rules to authenticate users before they access individual Administrator pages.
- The sandbox: In a hosted environment, ColdFusion applications are secured on a directory level allowing the hosting ISP to partition access to application pages and resources.

Securing Resources

The process of securing ColdFusion resources is essentially the same for all resource types, with minor variances based on different resource types.

It's important to understand that you do not need to explicitly define rules for every single ColdFusion resource type. Instead, by defining a rule for a particular type, you are saying 'I want ColdFusion to authorize access to this resource by this person.' Since rules are only enforced when associated with users and groups in a security policy, you only need rules to define exceptions to default behavior.

In summary, you follow these steps.

First, specify ColdFusion resource types:

1. You define a security context using the Administrator, Advanced Security pages.

Part of defining a security context is specifying the resource types you want to secure. You can select multiple resource types.

2. With your resource types selected, make sure you click the Apply button. Then click the Rules button.

Define rules for each resource type:

1. From the Edit Security Context page, click the Rules button.
2. Define a rule by entering the name of the rule you want and selecting the resource type from the list box. If the resource type you want is not listed in the list box, go back and edit the security context definition to include the resource type you want.

Create a new security policy:

1. From the Edit Security Context page, click the Policies button.
2. Enter a policy name that gives some indication of its purpose, such as WebTeam1, and click the Add button.
3. In the New Security Policy page, enter a description of the policy and click Add. ColdFusion returns you to the Resource Policies page for the current security context.
4. Click the name of the policy you just created. ColdFusion opens the Edit Security Policy page.

Associate users with the security context:

1. At the Edit Security Policy page, you can change the name or description of the current policy. To associate users with this policy, click the Users button. ColdFusion opens the Users page for the current policy.
2. If necessary, select a User Directory and click the Add/Remove button to open the Add/Remove Users page.
3. Based on the user directory you chose, you'll see a list of available users on the left of the list control and a list of current users on the right. To add users to the current policy select the users you want and click the left arrow button.
4. Click the Back button to return to the Users page for the current policy. If you click the Back button one more time, you return to the Edit Security Policy page for the current policy where you can click the Map button to view a schematic of the current security structure.

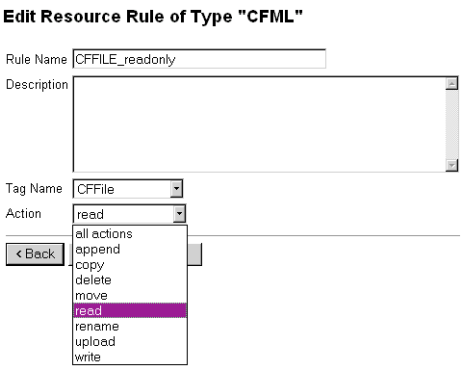
Securing CFML Tags

You secure CFML tags by first selecting CFML as a resource type when defining a security context. Then, when you open the Resource Rules page, ColdFusion offers CFML as a valid resource type for which you can define rules.

To secure a CFML tag:

1. Make sure in your security context, that you have enabled security for the CFML resource type.
2. On the Security context page, click Rules. The Resource Rules page appears for the current security context.
3. Enter a rule name, and in the Resource Type list box, select CFML. Click Add when you're ready.
4. On the Edit Resource Rule page, enter a description for the new rule.
5. In the Tag Name list box, select the tag you want to define in the rule. The rule you are defining here forces ColdFusion to authorize the execution of the tag before executing it. If you do not select CFML as a secured resource type, all tags will execute without prior authorization.
6. If applicable, select the action you want to add to the rule and click Apply.

Use this page to define a rule for specific tags or tag actions that are the exception. For example, in the following example, the READ action of the CFFILE tag is being explicitly defined so that, once this rule is associated with a particular user or group, ColdFusion will authorize the execution of this tag only when the associated user attempts to process a page containing this tag.



Note To protect all of a tag's individual actions, select the **all actions** option in the Action list box.

Securing Custom Tags

This release includes support for sandbox security for Custom Tags. To avoid name conflicts, you can register custom tags on the Advanced Security page of the ColdFusion Administrator. Select both the Use Advanced Security setting and the Use Sandbox Security Settings box. When you add rules to protect Custom Tags, enter the full path (using forward slashes) of each custom tag you want to secure, in the Custom Tag box on the New Resource Rule of Type "Custom Tag" page. Then click Add.

Viewing a Map of your Security Framework

ColdFusion Advanced security has its complexities. One utility you can use to get the big picture is the Map option available on the Advanced Security page. To view a map of your currently defined security framework, click the Map button. The resulting map depicts the hierarchical nature of your security structure showing exactly how the various components fit together.

Index

D

E