

Locking Down ColdFusion

Pete Freitag, Foundeo Inc.

foundeo
inc.

Who am I?

- Over 10 years working with ColdFusion
- Owner of Foundeo Inc a ColdFusion consulting & Products company
- Author, Blogger, and Twitterer?

Today's Agenda

- Security Concepts Applied
- Secure Installation Tips
 - Windows 2008 / IIS 7
 - RedHat EL 5.3 / Apache 2.2
- Secure Configuration Tips

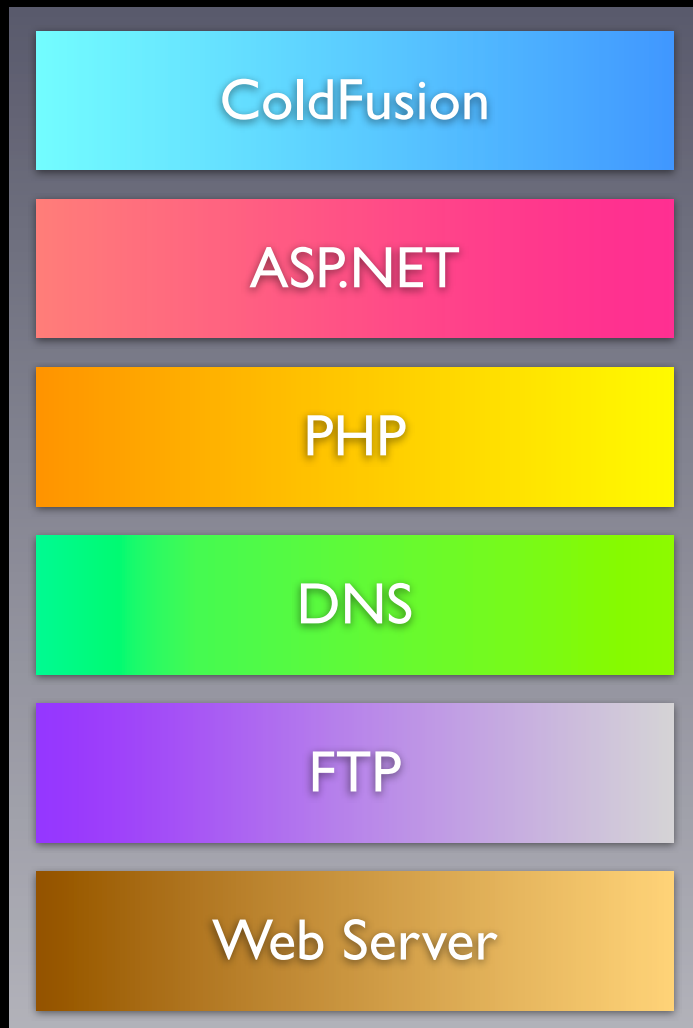
Disclaimer

- It's simply not possible to cover everything there is to know and do to setup a secure ColdFusion server in this 1 hour session.
 - I'll point you to resources as we go

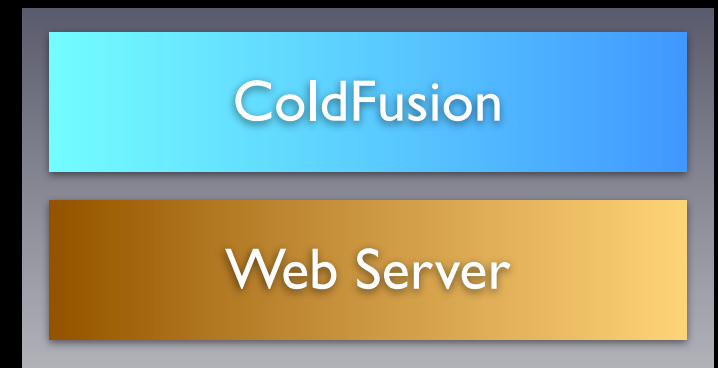
CF9 Lockdown Guide

- This presentation is based on the ColdFusion 9 Lockdown Guide I wrote for Adobe:
 - http://www.adobe.com/products/coldfusion/whitepapers/pdf/91025512_cf9_lockdownguide_wp_ue.pdf
 - <http://bit.ly/cf9secure>

Reduce Attack Surface



vs.



Defense in Depth

- A layered approach to security.
- Reduces the risk of vulnerabilities in one of the levels.

Network Firewall

Web App Firewall

Web Server Rules

Application Server Rule

Your Source Code

Database Controls

Defense in Depth Example

- Web App has read only access to a database.
 - Setup datasource to only allow SELECT
 - Setup sandbox to only allow access to the given datasource
 - Setup database user privileges to only allow SELECT.

Principle of Least Privilege

- Grant the minimum amount of permission necessary to do the job.



Defaults

- Changing defaults doesn't necessarily make you more secure, but it does make automated attacks less likely to succeed.

Logging

- Important for monitoring & forensics.
- Regulations & Requirements
 - Example: PCI requires you to retain logs for at least one year.

Before You Install

- Create 3 Partitions:
 - OS
 - ColdFusion
 - Web Assets

Install OS

- Install with minimal components
- Refer to security guides for installing and configuring OS:
 - NSA Security Configuration Guides:
 - http://www.nsa.gov/ia/guidance/security_configuration_guides/
 - Microsoft Security Compliance Manager
 - <http://www.microsoft.com/downloads/details.aspx?FamilyID=5534bee1-3cad-4bf0-b92b-a8e545573a3e&displaylang=en>

SELinux

- ColdFusion can run under Security Enhanced Linux with a little effort.
- Install with SELinux Enforcing mode on
- SELinux allows programs (such as apache) to run in their own sandboxed security domains.

User Accounts

- ColdFusion runs under the System account on Windows.
- Create user accounts for ColdFusion and the web server to operate under.

User Accounts

- Remove unnecessary permissions and default groups.
- On Windows
 - Deny Terminal Services Access
- On Linux
 - Shell: `/sbin/nologin` *
 - Add to `/etc/nologin`

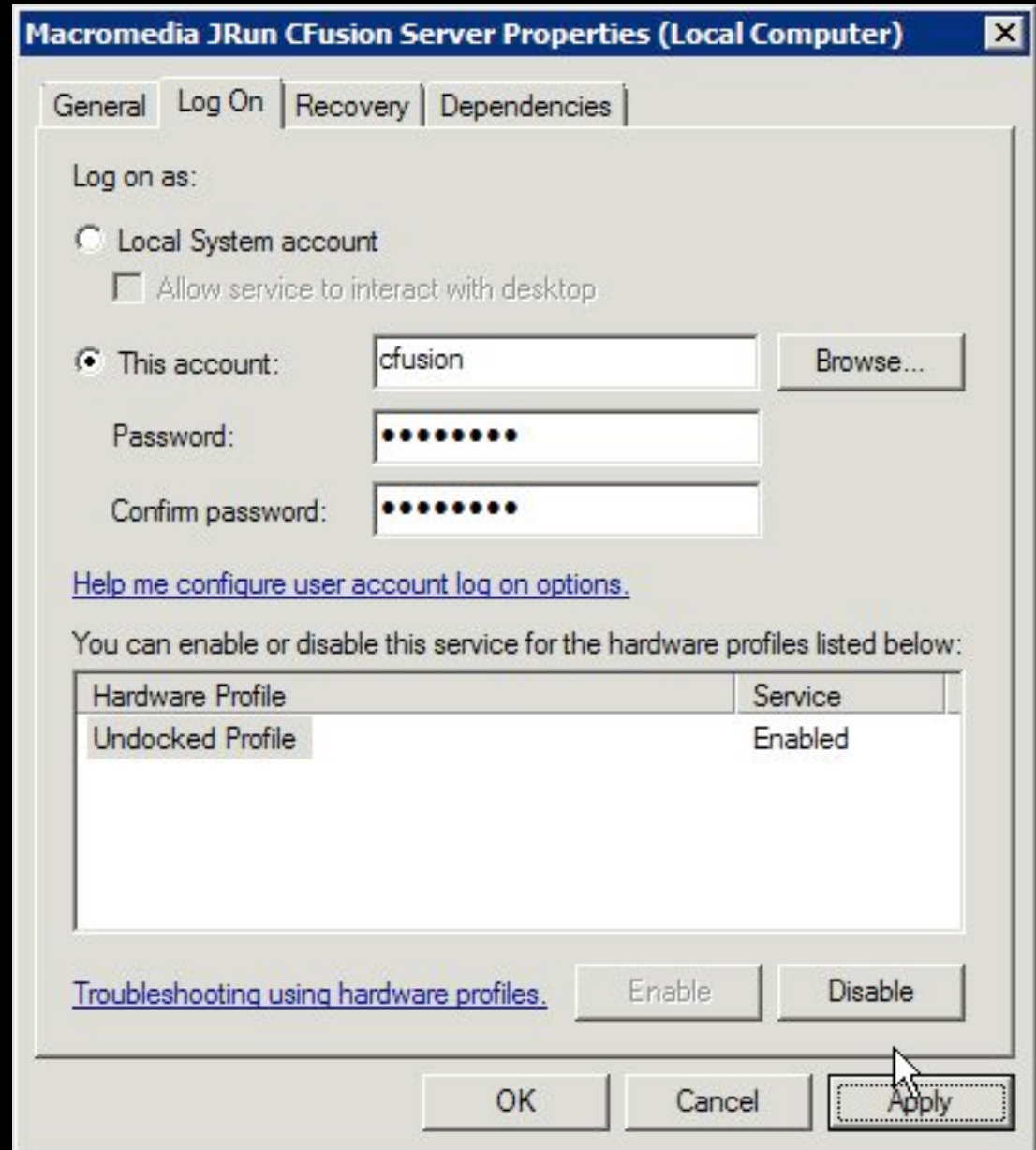
* Requires modifying the cf startup script

ColdFusion User

Directory	Read	Write
ColdFusion Root	Y	Yes many sub directories require write (logs, etc)
Web Root	Y	As needed

Run ColdFusion As

1. Services
2. Right Click
3. Log On tab
4. Enter Credentials



Run ColdFusion As...

- On Linux
 - The ColdFusion installer will prompt you for a user name to run ColdFusion as.

Web Server User Permissions

- The web server user will need file system permissions to the lib/wsconfig directory under your ColdFusion installation.

Apache User

- Found in the Apache conf file: httpd.conf
 - User apache
 - Group apache
 - Some installations will use the account: *nobody* but it's better to use a dedicated account.

IIS App Pool User

- Microsoft does not recommend changing the run as account for the *World Wide Web Publishing Service*.
 - Instead you can modify the *Identity* (the user) that each IIS Application Pool Runs As.
 - Application Pools > Actions > Set Application Pool Defaults > Process Model > Identity

File Auditing

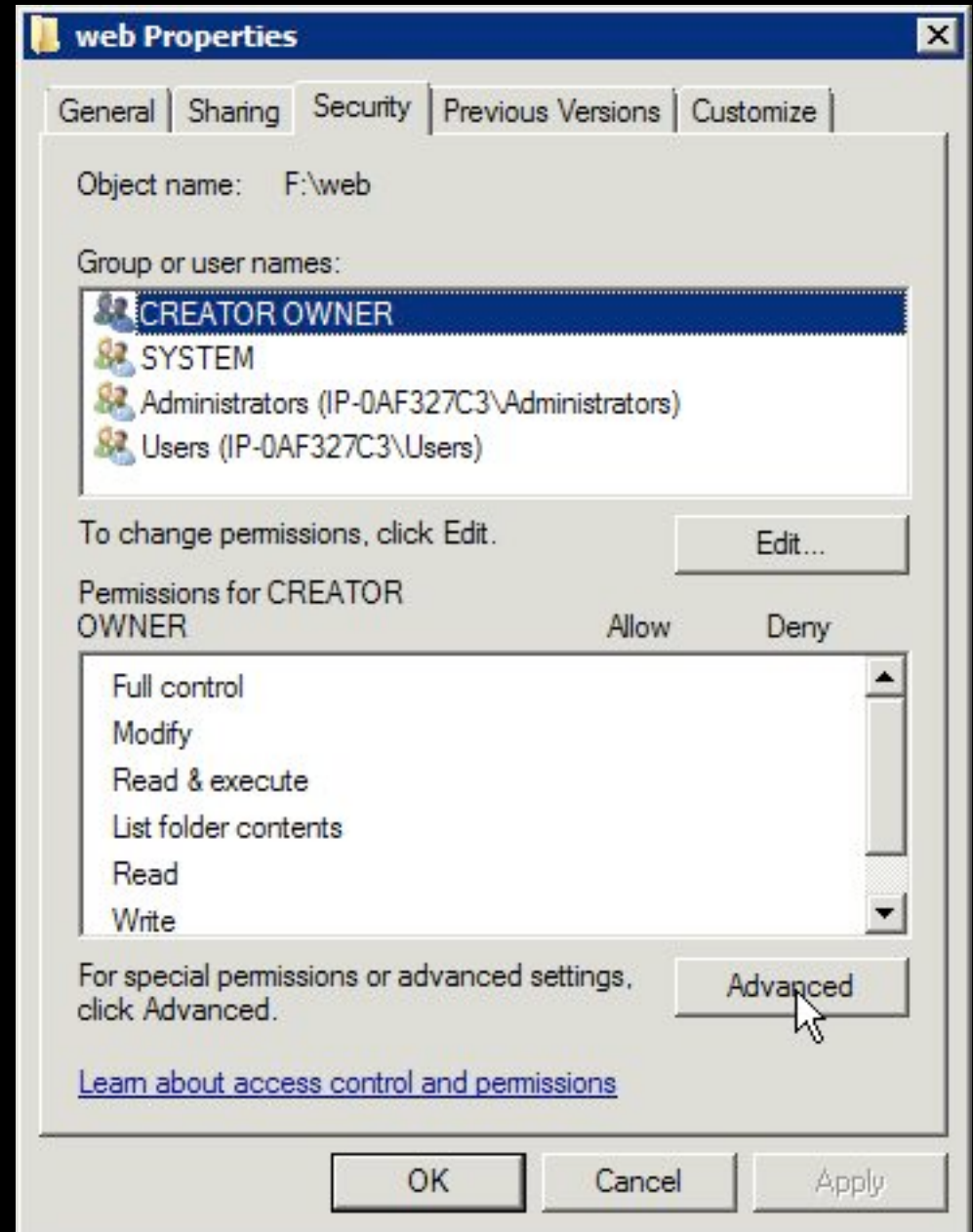
- Modern Operating Systems allow you to log successful or failed file access attempts.
 - Be careful logging all successful file operations, can quickly fill logs.
 - Successful deletes are a good idea though.
 - Log all failed accesses (read, write, delete, etc).

Linux File Auditing

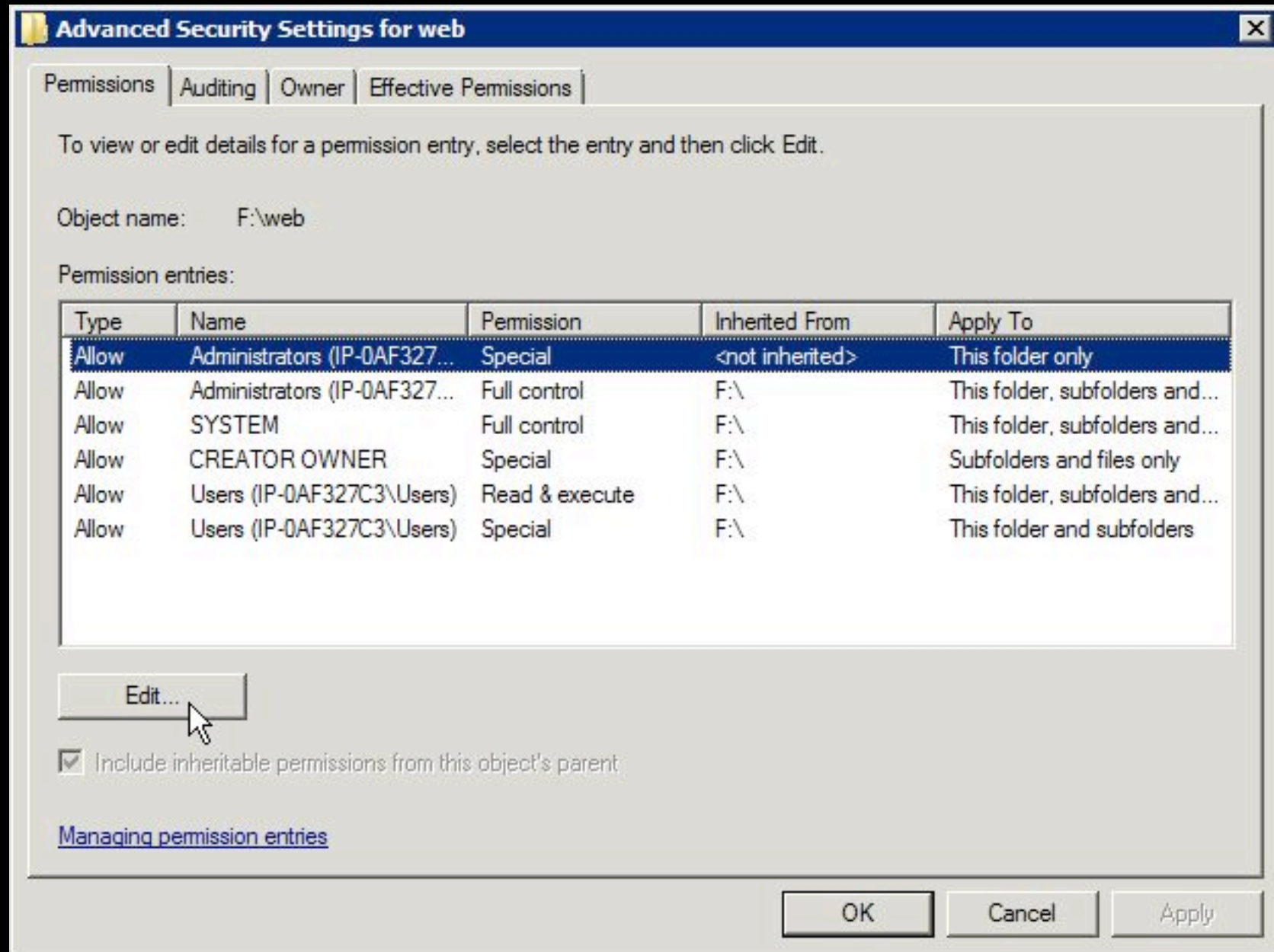
- Use **auditd** for Linux (Linux Kernel 2.6+)
 - Config stored in: /etc/audit.rules
 - **auditctl** - modify rules
 - **aureport** - reports logs
 - **aureport** - search logs

Windows Advanced Security

1. Right Click on a Directory
2. Select the Security Tab
3. Click Advanced



Windows File Permissions



The screenshot shows the 'Advanced Security Settings for web' dialog box. The 'Permissions' tab is active. The object name is 'F:\web'. A table lists permission entries for various users, including Administrators and Users. An 'Edit...' button is highlighted with a mouse cursor. A checkbox for 'Include inheritable permissions from this object's parent' is checked. At the bottom, there are 'OK', 'Cancel', and 'Apply' buttons.

Permissions | Auditing | Owner | Effective Permissions

To view or edit details for a permission entry, select the entry and then click Edit.

Object name: F:\web

Permission entries:

Type	Name	Permission	Inherited From	Apply To
Allow	Administrators (IP-0AF327...	Special	<not inherited>	This folder only
Allow	Administrators (IP-0AF327...	Full control	F:\	This folder, subfolders and...
Allow	SYSTEM	Full control	F:\	This folder, subfolders and...
Allow	CREATOR OWNER	Special	F:\	Subfolders and files only
Allow	Users (IP-0AF327C3\Users)	Read & execute	F:\	This folder, subfolders and...
Allow	Users (IP-0AF327C3\Users)	Special	F:\	This folder and subfolders

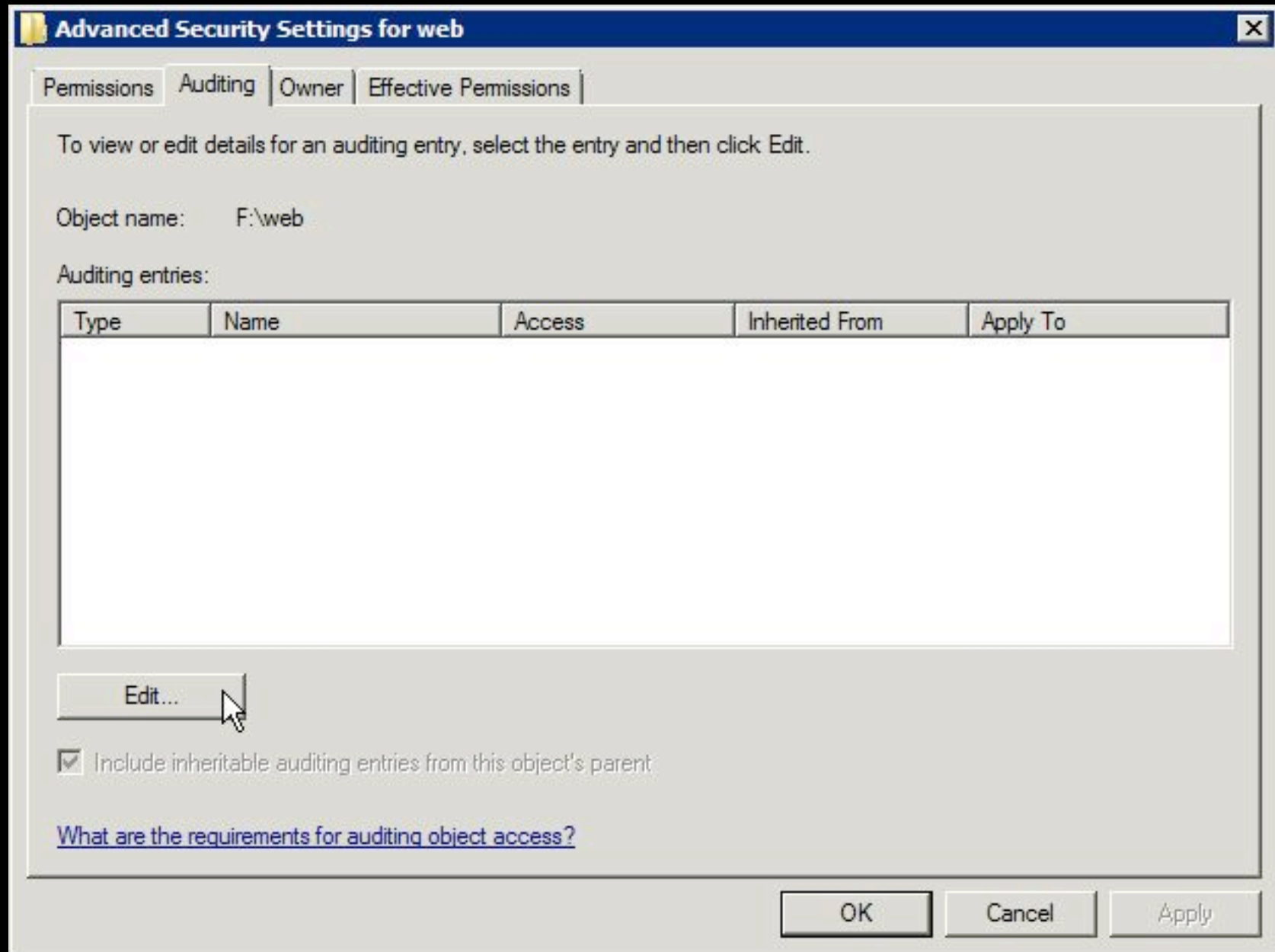
Edit...

Include inheritable permissions from this object's parent

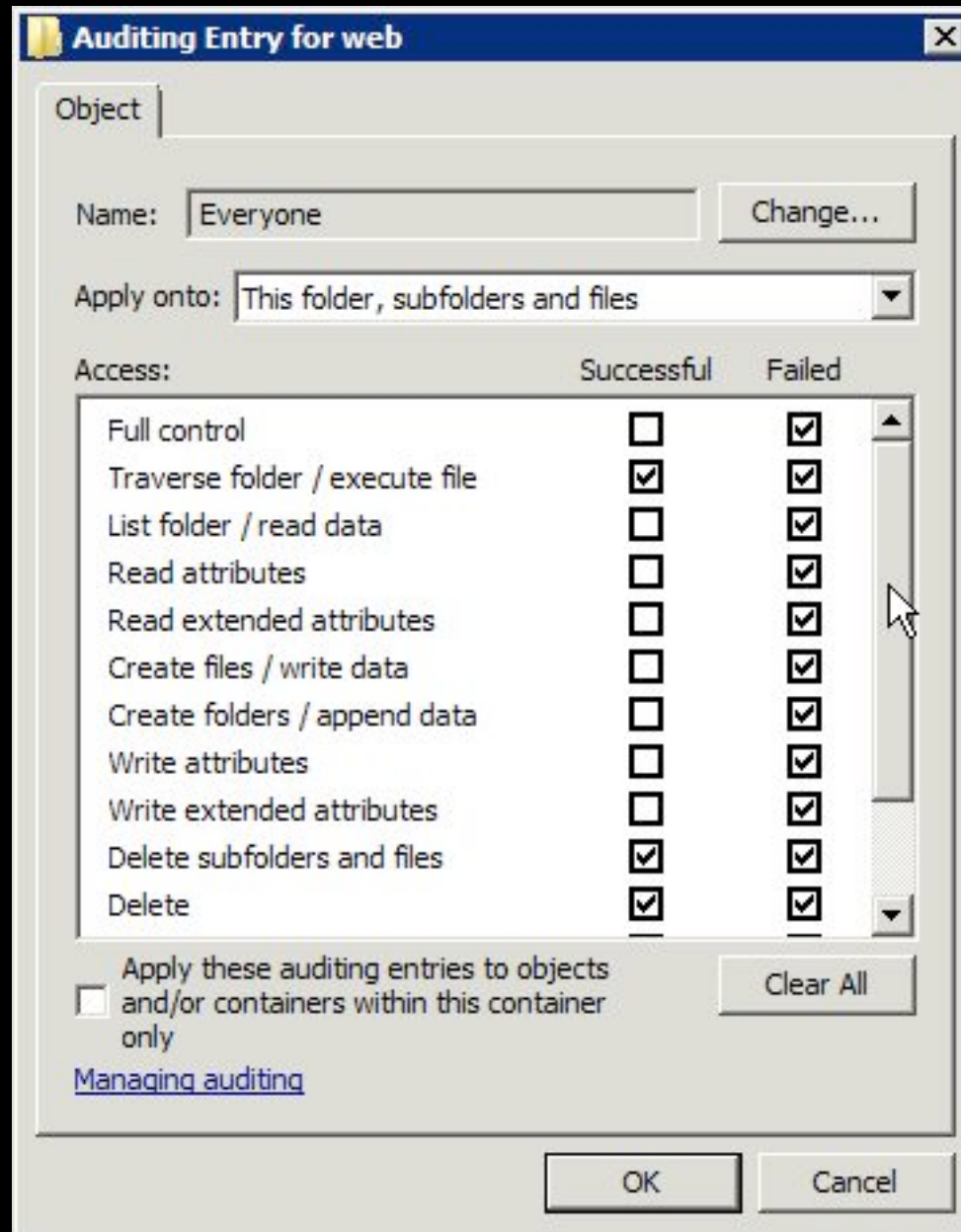
[Managing permission entries](#)

OK Cancel Apply

Windows Auditing



Windows File Auditing



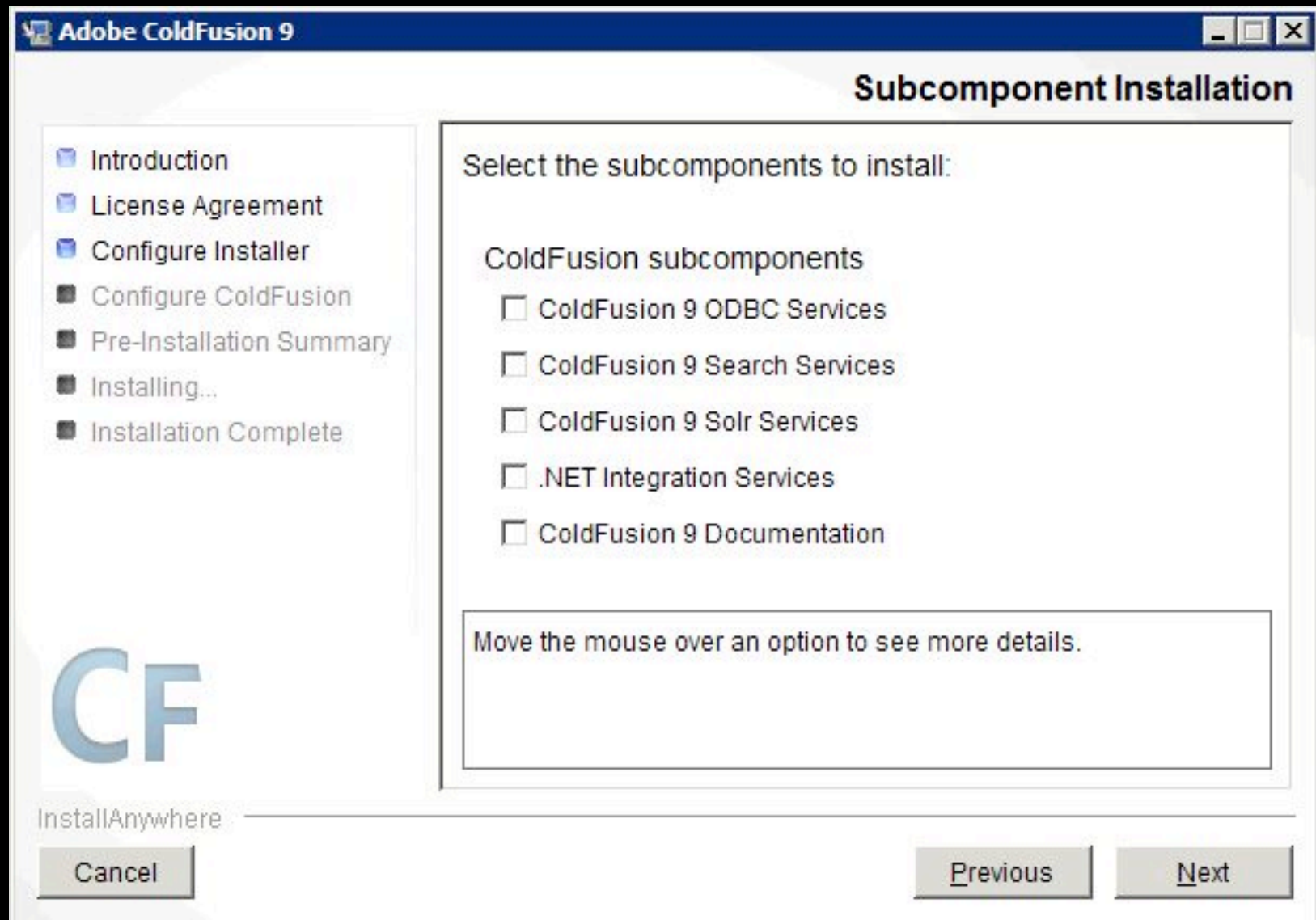
Create a ColdFusion Administrator Site

- The ColdFusion Administrator Should not be exposed to the public.
- Setup a dedicated web site on the web server.
- Listen on localhost only or a internal lan address
- Require SSL.
- Use a Web Server Password to allow Auditing.

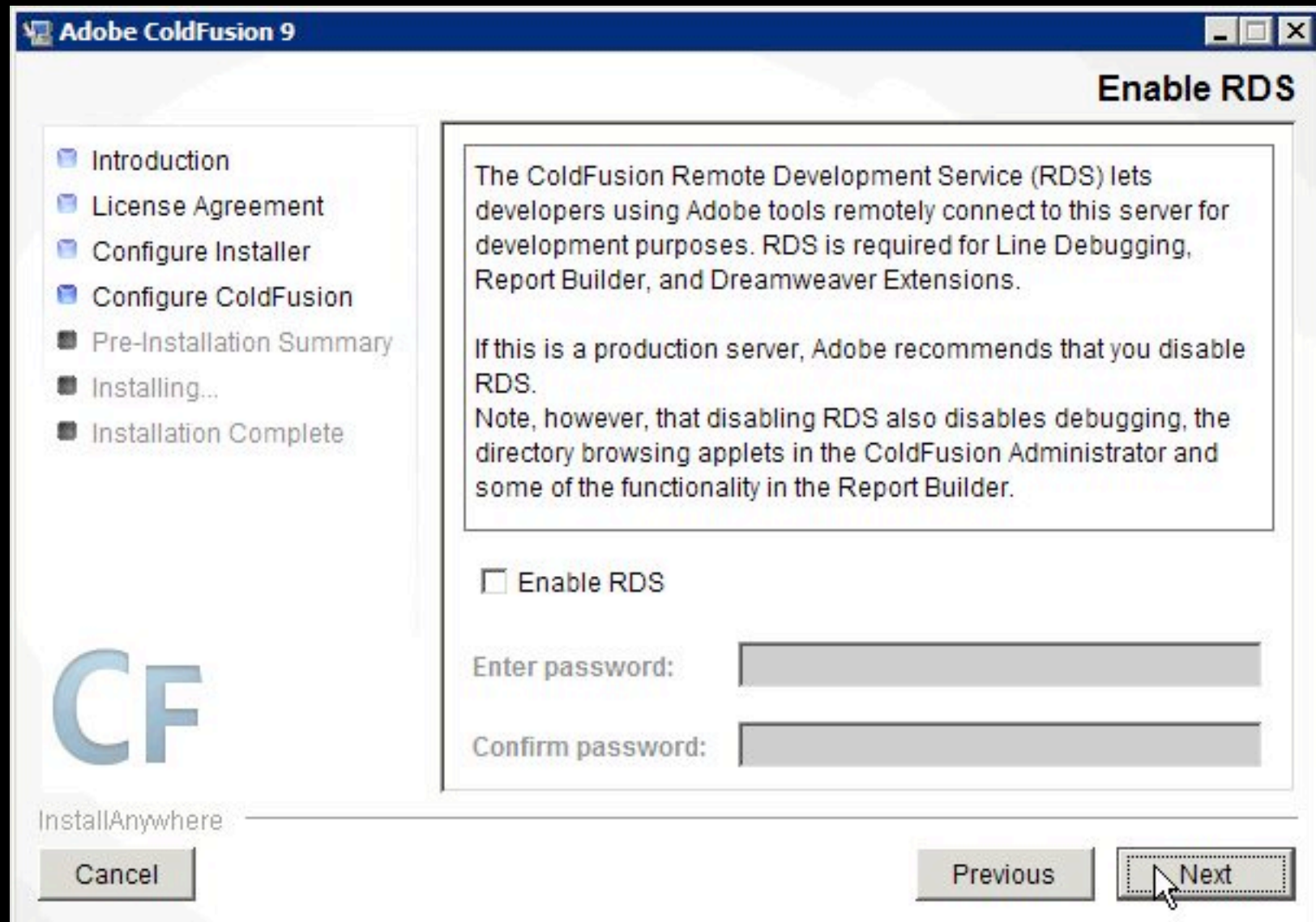
Install ColdFusion



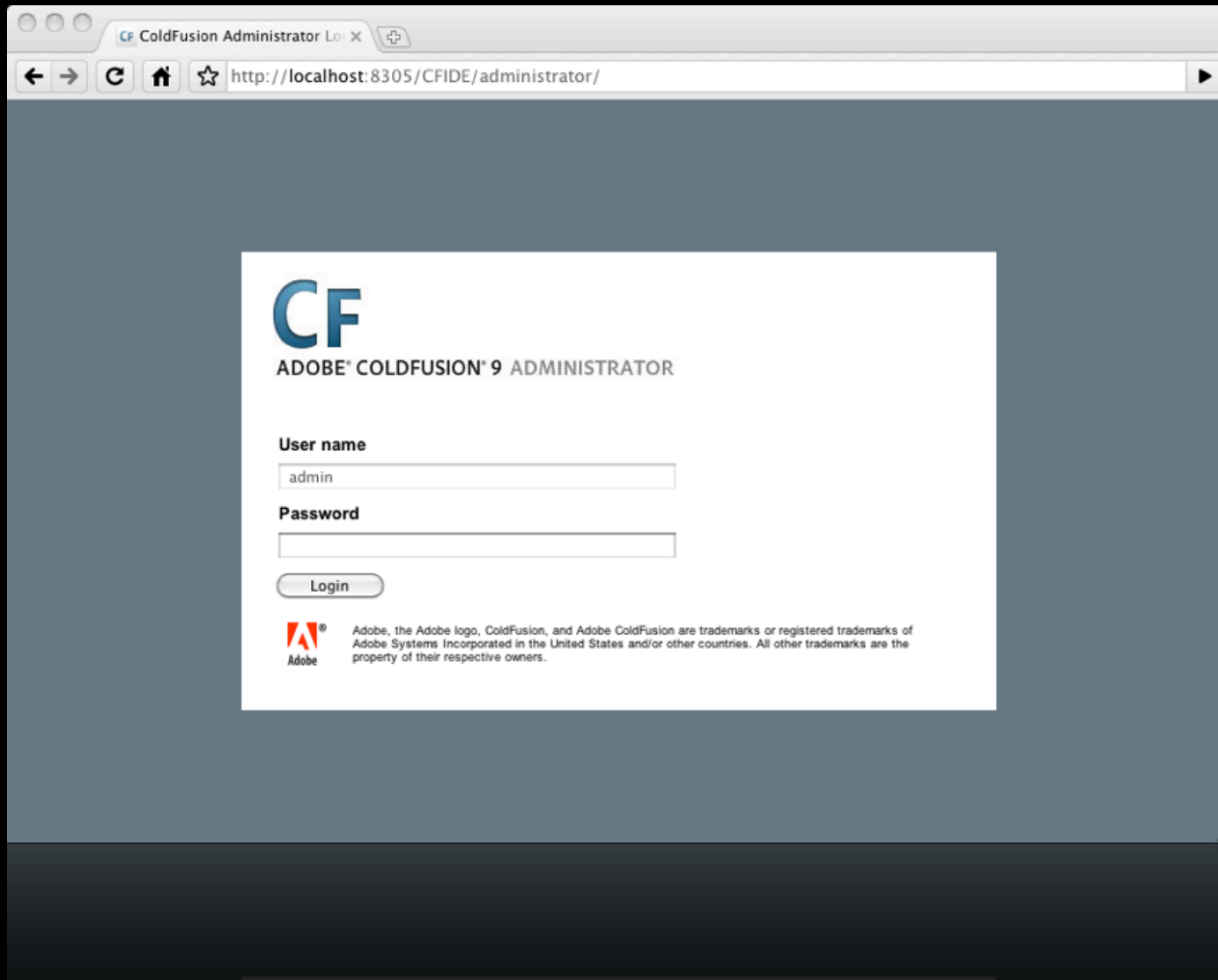
Don't Install Everything



No RDS on Production



ColdFusion Administrator



Sandbox Security

- Restricts what your CFML can access:
 - Tags
 - Functions
 - Datasources
 - File Access
 - Network

Sandbox Setup

- Very easy to get going with on standalone install (click checkbox).
- Enterprise / Multiserver requires an addition to `jvm.config`
- Enterprise allows multiple sandboxes

Sandbox jvm.config

-Djava.security.manager "-

Djava.security.policy=cf_root/WEB-INF/cfusion/
lib/coldfusion.policy" "-

Djava.security.auth.policy=cf_root/WEB-INF/
cfusion/lib/neo_jaas.policy"

Restricting /CFIDE

- Expose only the necessary files in /CFIDE
- Many of the files can be blocked by the web server but still work within ColdFusion.

What's in /CFIDE

Folder / File	Notes
adminapi/	ColdFusion Admin API, can usually be blocked.
administrator/	CF Admin, should not be public.
AIR/	Adobe Air offline synchronization. BINU
appdeployment/	Used for CAR File Deployment, can be blocked.
classes/	Contains Old CFForm Applets. BINU
componentutils/	CFC Metadata Documentation, should not be public.
debug/	Used when debugging is enabled, should not be public.

BINU = Block if not used

What's in /CFIDE

Folder / File	Notes
images/	Contains 2 image files, should be safe to block.
orm/	ORM Event Handler Interface CFCs. Can be blocked.
portlets/	CF9 Portlet API. BINU
probe.cfm	ColdFusion Probes. BINU
scripts/	JS, CSS, and CFM files used by cf tags. Move to non-default location, or BINU.
ServerManager/	Contains Server Manager AIR app. Can be blocked.
services/	CFAAS Components. BINU
wizards/	Not sure what its for but it has had several vulnerabilities in the past year or so. Block it.

BINU = Block if not used

Blocking /CFIDE

- Apache mod_rewrite
- IIS 7 applicationHost.config file

```
<denyUrlSequences>
  <add sequence="/CFIDE/administrator" />
  <add sequence="/CFIDE/adminapi"/>
  <add sequence="/CFIDE/AIR"/>
  <add sequence="/CFIDE/appdeployment"/>
  <add sequence="/CFIDE/componentutils"/>
  <add sequence="/CFIDE/debug"/>
  <add sequence="/CFIDE/orm"/>
  <add sequence="/CFIDE/portlets"/>
  <add sequence="/CFIDE/probe.cfm"/>
  <add sequence="/CFIDE/scripts"/>
  <add sequence="/CFIDE/services"/>
  <add sequence="/CFIDE/wizards"/>
</denyUrlSequences>
```


IIS 7 Request Filtering

- Take some time to learn about it.
 - Block by URI
 - Block file extension white/black list
 - Limit POST Size, Query String size
 - Limit Verbs (GET, POST, etc)

What's not in /CFIDE

- You might notice that a few other requests are served from /CFIDE but don't have corresponding files. For example:
 - /CFIDE/GraphData.cfm (cfchart)
 - /CFIDE/main/ide.cfm (RDS)

Servlet Mappings

- These mappings are defined in the web.xml file located in the WEB-INF directory.
 - web.xml is part of JEE / J2EE standard

Servlets & Mappings

- Java EE Web Applications consist of Servlets and Servlet Mappings.
 - Servlet - Is the chunk of code that does the processing of the request
 - Servlet Mapping - Simply routes url requests to a Servlet.

Example Servlet Mapping in web.xml

```
<servlet-mapping id="coldfusion_mapping_11">  
  <servlet-name>GraphServlet</servlet-name>  
  <url-pattern>/CFIDE/GraphData.cfm</url-pattern>  
</servlet-mapping>
```

Removing Unused Mappings

- You can remove unused servlet mappings by commenting out the `<servlet-mapping>` tags in web.xml
 - Warning: Keep a backup of the web.xml file certain changes might cause the server not to start. Strict XML.
 - Beware Adobe may not preserve your changes when installing an updater.

Servlet Mappings in CF9

URI Mapping	Servlet	Used For
*.cfm, *.cfml	CfmServlet	Serving cfm files. Don't remove
*.cfc	CFCServlet	Serving Remote CFC Method calls. You can remove this mapping and still use CFCs, you just can't use remote methods.
/CFIDE/GraphData.cfm /CFIDE/GraphData	GraphServlet	CFChart, CFGraph
/flashservices/gateway/*	FlashGateway	BlaseDS for Flash Remoting
/flex2gateway/*	MessageBrokerServlet	Flash Remoting for Flex
*.jws	CFCServlet	Web Services written in java, not typically used by CF developers.

Servlet Mappings in CF9

URI Mapping	Servlet	Used For
*.cfr	CFCServlet	CFReport
/CFFormGateway/*	CFFormGateway	CFForm Flash Forms
/cform-internal/*	CFInternalServlet	CFForm Flash Forms
*.cfswf	CFSwfServlet	CFForm Flash Forms
/CFFileServlet/*	CFFileServlet	Used for serving images from cfimage tag. Also used in cfreport and cfpresentation
/WSRPProducer/*	WSRPProducer	Web Services for Remote Portlets



FuseGuard

Web Application Firewall for ColdFusion
<http://foundeo.com/security/>

foundeo
inc.

Thanks. Questions?
pete@foundeo.com

www.hackmycf.com
www.foundeo.com

foundeo
inc.