COALESCE SOLUTIONS

We are Coalesce —

a technology solutions provider and systems integrator.

We bring clarity to Adobe ColdFusion-centered projects and accelerate Cloud based businesses.

Hardened Adobe ColdFusion on Linux AMIs

Contents

The release notes are furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by Coalesce Solutions, LLC or Adobe Systems Incorporated. Coalesce Solutions, LLC and Adobe Systems Incorporated assume no responsibility or liability for any errors or inaccuracies that may appear in the informational content contained in this document.

Getting Started

After launching the AMI on an EC2 Instance, if you have network access to the instance over port 22, connect to it using a Secure Shell (SSH) client by right clicking the instance in the EC2 console and selecting Connect. SSH into the instance with the username "ec2-user" on Amazon Linux and "ubuntu" on Ubuntu with the KeyPair you associated with the instance. Alternatively, you can connect using Session Manager instead of using an SSH client.

If you have allowed your IP address to connect (see the cfsetup example in "Example Configuration Commands" below), access the ColdFusion Administrator by visiting *http://<server ip>:8500/CFIDE/administrator* and log in with the password: TempAdmin$1

INSTALLATION NOTES

Server

- Hardened based on the [CIS Benchmark for Linux] (specifically the benchmark for the Operating System on the AMI)
- Swap memory (1gb) enabled to help prevent the kernel from killing services when out of memory

Adobe ColdFusion

General

- ColdFusion installation path:
  - 2021 Release - /opt/cf2021cloud
  - 2023 Release - /opt/cf2023cloud
- ColdFusion service account: cf_svc
- cfsetup alias "cfusion" is configured for instance located in cfusion path
- JRE DNS Caching TTL Set to 15 seconds
- JRE Min Heap 256m, Max Heap 1024m, Max Metaspace 192m
- ColdFusion Tomcat is listening on port 8500
- Hardened using the Lockdown guide:
  - 2021 Release - Adobe ColdFusion 2021 Lockdown Guide
  - 2023 Release - Adobe ColdFusion 2023 Lockdown Guide

Updates/Hotfixes Applied

- ColdFusion Updates applied as new AMIs are released
- ColdFusion packages installed: adminapi, administrator
- All CFPM Packages are downloaded and updated as of each release and can be installed offline without accessing an external server

Apache

- ColdFusion is connected to both an HTTP (port 80) and HTTPS (port 443) virtual hosts
- Web root path: /srv/www
- Access and Error Logs path: /var/log/httpd/
- Access logs include the x-forwarded-for original client IP for when server is behind a load balancer

Programs Installed

- Amazon CloudWatch Agent (pre-configured to send some logs to CloudWatch)
- Java JDK
- MySQL Connector/J
- Amazon CloudWatch Agent
- AWS CodeDeploy Agent
- AWS CLI 2
- AWS SSM Agent

CONFIGURATION NOTES

Further Hardening Recommendations (not an exhaustive list):

a) Change the ColdFusion Administrator Password
b) Install Antivirus software
c) Install File Integrity Monitoring software
d) Install Intrusion Detection / Prevention software and/or service
e) Install SSL Certificate and Deploy the website as SSL
f) Change the Tomcat secret and associated connector
g) Change the PMT monitoring secret
h) Enable the ColdFusion Sandbox as appropriate for each application
i) Enable the secure settings within the ColdFusion Administrator
j) Remove the cf_scripts* virtual directory if you are not using any of its components
k) Launch as part of a Launch Template to Encrypt all EBS volumes
l) Add more logs to be sent to CloudWatch. Add adm group ownership to log files to grant cwagent permission to read files. See CloudWatch Config File Details for more information.

Example Configuration Commands

- Install ColdFusion Packages:
  ```
  /opt/cf<release>cloud/cfusion/bin/cfpm.sh install awss3,document,zip
  ```
- Change ColdFusion settings using cfsetup (cd into `/opt/cf<release>cloud/config/cfsetup/`):
  ```
  ./cfsetup/cfsetup.sh set security allowedIPForAdmin=172.16.*.* cfusion
  ./cfsetup.sh set Runtime CFCLimit=50 cfusion
  ./cfsetup.sh set mail server=your-smtp.server.com cfusion
  ```
- Change ColdFusion Administrator Password:
  ```
  ./cfsetup.sh set security adminPassword=newpwd cfusion
  ```

IMPORTANT: The reader is strongly encouraged to test all recommendations on an isolated test environment before deploying into production. CFSetup.sh settings require CF Service restart to become effective.

Hardening Scan Results

Topic	Id	Title	Result	Coalesce Notes
AWS Linux 2023	2.1.2	Ensure chrony is configured	fail	AWS defaults to internal time pools with chrony. False negative.
AWS Linux 2023	2.2.8	Ensure a web server is not installed	fail	Apache is required and installed.
AWS Linux 2023	5.1.3	Ensure all logfiles have appropriate permissions and ownership	fail	Immediately upon new log files getting created, they have extra read permissions
AWS Linux 2023	6.2.2	Ensure /etc/shadow password fields are not empty	fail	No user account have empty passwords other than ec2-user