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 Windows 2022 AMIs

coalescesolutions.com | **+1 (901) 567-8300** | **info@coalescesolutions.com**

Contents

Getting Started

After launching the AMI on an EC2 Instance, RDP into the instance with the username "Administrator" and the generated password.

Access the ColdFusion Administrator by visiting http://localhost:8500/CFIDE/administrator and log in with the password: TempAdmin$1

INSTALLATION NOTES

Server

- **An EBS volume was added to the image for the IIS Logs and Web Root and mounted as the W drive**
- **The Guest account is renamed**
- **Hardened based on the CIS Benchmark for Azure Compute Microsoft Windows Server 2022 version 1.0.0. (Azure benchmark was used due to the fact that the settings also apply to other cloud environments and the non-Azure benchmarks include not-applicable domain and user settings)**

Adobe ColdFusion

General

- **ColdFusion installation path:**
  - **2021 Release - C:\cf2021cloud**
  - **2023 Release - C:\cf2023cloud**
- **ColdFusion service account: .\cfservice**
- **cfsetup alias "cfusion" is configured for instance located at c:\cf2021cloud\cfusion**
- **JRE DNS Caching TTL Set to 15 seconds**
- **JRE Min Heap 256m, Max Heap 1024m, Max Metaspace 192m**
- **Java args include coldfusion.xml.allowPathCharacters=true**
- **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**

IIS

- **ColdFusion Connector is attached to the "Default Web Site" in IIS**
- **Web root path: W:\wwwroot**
- **IIS Logs path: W:\IISLogs**
- **Hardened based on the CIS Microsoft IIS 10 Benchmark Level 1 version 1.2.0**

Programs Installed

- Microsoft Application Request Routing 3.0 (x64)
- Microsoft Visual C++ Redistributable
- 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) Configure CloudWatch log delivery
f) Disable WinRM
g) Bind the IIS Site to a hostname instead of a blank value
h) Install SSL Certificate and Deploy the website as SSL
i) Change the Tomcat secret and associated connector
j) Change the PMT monitoring secret
k) Enable the ColdFusion Sandbox as appropriate for each application
l) Change IIS's Request Filtering setting for Allow Unlisted to "false" and enter in the applicable file extensions for each application. Currently this is set up with a blacklist collection of extensions.
m) Enable the secure settings within the ColdFusion Administrator
n) Remove the cf_scripts* virtual directory if you are not using any of its components
o) Launch as part of a Launch Template to Encrypt all EBS volumes

Example Configuration Commands

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

  (echo password=thenewpassword && echo rdspassword= && echo encrypted=false) >
  C:\cf<release>cloud\cfusion\lib\password.properties
  ```

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

Hardening Scan Results

Topic	Id	Title	Result	Coalesce Notes
IIS	1.1	(L1) Ensure web content is on non-system partition	manual	Confirmed to be in place
IIS	1.2	(L1) Ensure 'host headers' are on all sites	fail	To be completed after deployment due using final host name
IIS	1.7	(L1) Ensure WebDav feature is disabled	manual	Confirmed to be in place
IIS	2.1	(L1) Ensure 'global authorization rule' is set to restrict access	manual	Confirmed to be in place
IIS	2.2	(L1) Ensure access to sensitive site features is restricted to authenticated principals only	manual	Confirmed to be in place
IIS	2.3	(L1) Ensure 'forms authentication' require SSL	manual	To be completed after deployment, if utilizing IIS authentication
IIS	2.5	(L1) Ensure 'cookie protection mode' is configured for forms authentication	manual	To be completed after deployment, if utilizing IIS authentication
IIS	2.6	(L1) Ensure transport layer security for 'basic authentication' is configured	manual	Confirmed to be in place
IIS	2.7	(L1) Ensure 'passwordFormat' is not set to clear	manual	To be completed after deployment, if utilizing IIS authentication
IIS	3.1	(L1) Ensure 'deployment method retail' is set	manual	Confirmed to be in place
IIS	3.4	(L1) Ensure IIS HTTP detailed errors are hidden from displaying remotely	manual	Confirmed to be in place
IIS	3.7	(L1) Ensure 'cookies' are set with HttpOnly attribute	manual	Confirmed to be in place
IIS	3.9	(L1) Ensure 'MachineKey validation method - .Net 4.5' is configured	manual	Confirmed to be in place
IIS	3.10	(L1) Ensure global .NET trust level is configured	manual	Confirmed to be in place
IIS	4.6	(L1) Ensure 'HTTP Trace Method' is disabled	manual	Confirmed to be in place
IIS	4.7	(L1) Ensure Unlisted File Extensions are not allowed	fail	To be completed after deployment, once each application's actual file extensions are understood
IIS	4.8	(L1) Ensure Handler is not granted Write and Script/Execute	manual	Confirmed to be in place
IIS	4.11	(L1) Ensure 'Dynamic IP Address Restrictions' is enabled	manual	Confirmed to be in place
IIS	5.1	(L1) Ensure Default IIS web log location is moved	manual	Confirmed to be in place

Topic	Id	Title	Result	Coalesce Notes
IIS	5.2	(L1) Ensure Advanced IIS logging is enabled	manual	Confirmed to be in place
IIS	5.3	(L1) Ensure 'ETW Logging' is enabled	manual	Confirmed to be in place
IIS	6.1	(L1) Ensure FTP requests are encrypted	manual	Confirmed to be in place
IIS	6.2	(L1) Ensure FTP Logon attempt restrictions is enabled	manual	Confirmed to be in place
Windows	2.2.6	(L1) Ensure 'Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE'	fail	Required for a server running IIS
Windows	2.2.28	(L1) Ensure 'Generate security audits' is set to 'LOCAL SERVICE, NETWORK SERVICE'	fail	Required for a server running IIS
Windows	2.2.41	(L1) Ensure 'Replace a process level token' is set to 'LOCAL SERVICE, NETWORK SERVICE'	fail	Required for a server running IIS
Windows	2.3.1.4	(L1) Configure 'Accounts: Rename administrator account'	fail	AWS Marketplace requires Administrator to be named as such