YazamTech

YazamTech Content Disarm and Reconstruction (CDR) solutions

Usage Instructions

Overview

This product is deployed via AWS CloudFormation to a Windows EC2 instance. The customer selects an existing VPC Subnet and an existing Security Group to control inbound access.

Resources created by this template

- Creates: EC2 instance and its EBS root volume (size controlled by RootVolumeSize).
- Uses: customer-selected SubnetId and ExistingSecurityGroupId.
- Does not create: S3 buckets, IAM roles/policies, or KMS keys.

CloudFormation template access (S3)

- The CloudFormation template is hosted at a public Amazon S3 URL for retrieval by CloudFormation.
- The deployed stack does not create or use any customer S3 buckets.

1. Launch with CloudFormation

1.1. Initial launch settings

1.1.1. Keep Version set to latest/stable (unless instructed otherwise).

1.1.2. Select the appropriate AWS Region based on customer requirements.

1.1.3. Click Launch with CloudFormation.

1.2. Create stack – Template preparation

1.2.1. Ensure Choose an existing template is selected.

1.2.2. The template source is automatically set to Amazon S3 URL.

1.2.3. Click Next.

1.3. Specify stack details

1.3.1. Provide the following parameters:

1.3.1.1. StackName: clear and identifiable name.

1.3.1.2. AMI ID: leave the default value from the template.

1.3.1.3. SubnetId: select the relevant subnet in the customer's VPC.

1.3.1.4. ExistingSecurityGroupId: select an existing Security Group (see Networking section).

1.3.1.5. InstanceType: use the recommended default unless otherwise required.

1.3.1.6. KeyName (EC2 Key Pair): select an EC2 key pair (used to retrieve/decrypt the initial Windows Administrator password if RDP access is required).

1.3.1.7. RootVolumeSize: define disk size in GB.

1.3.2. Click Next.

1.4. Configure stack options

1.4.1. No changes required (Tags, Permissions, etc.).

1.4.2. Leave defaults and click Next.

1.5. Review and create

1.5.1. Review settings, with emphasis on Region, Subnet, Security Group, and Instance Type.

1.5.2. Click Submit.

2. Deployment validation / Health checks (step-by-step)

2.1. In CloudFormation, verify the stack status is CREATE_COMPLETE.

2.2. In EC2, confirm the instance is in Running state.

2.3. In the EC2 console, select the instance and confirm that all EC2 status checks are passing (System + Instance, and if shown, Attached EBS).

2.4. Verify application reachability (see Access section below).

3. Networking / Security Group

3.1. This deployment does NOT create or modify Security Groups.

3.2. You must select an existing Security Group (ExistingSecurityGroupId) to control inbound access.

3.3. Configure inbound rules on the selected Security Group as follows:

3.3.1. TCP 80, 443, 8008 (Process / Media / API / Directories)

3.3.2. TCP 25 (SMTP) only if email/SMTP is required

3.4. Security recommendation: restrict inbound access to trusted source IP ranges (avoid 0.0.0.0/0), especially during initial setup.

3.5. Windows Firewall

Ensure the same required ports are allowed on the Windows instance firewall according to your organization policy.

4. Optional: RDP access (Windows)

4.1. In the EC2 console, select the instance created by the CloudFormation stack and click Connect.

4.2. In the RDP client section, download the RDP file (RDP client) and use it to start the Remote Desktop connection.

4.3. In the same Connect/RDP client screen, click Get Windows password.

4.4. Upload the private key file (.pem) that matches the selected KeyName to decrypt the initial Administrator password.

4.5. Connect via RDP to the instance Public DNS/IP using the decrypted Administrator password.

Security note: If RDP is required, allow TCP 3389 in the selected Security Group from trusted IPs only.

5. Accessing the management interface (HTTP → HTTPS)

5.1. Initial access to the management interface is over HTTP:

http://%client_Dns%/management/home

5.2. Replace %client_Dns% with your DNS address.

5.3. After uploading a valid TLS/SSL certificate in the management UI (see Section 6.2), the system switches to HTTPS:

https://%client_Dns%/management/home

Recommendation: upload the certificate immediately after first login and restrict inbound access to trusted IPs during setup.

6. Management configuration and client installation

6.1. Admin user setup

6.1.1. Define the credentials for the Admin user who will manage the system (Logs, Policies, etc.).

6.1.2. Enter Username and Password, then click Save.

6.1.3. Go to the Options tab.

6.1.4. Configure the Email Gateway (SMTP) (required for receiving 2FA emails/codes).

6.1.5. Enable Two-Factor Authentication (2FA) for the Admin account (recommended)).

6.2. DNS and SSL certificate configuration

6.2.1. DNS: enter your registered DNS address.

6.2.2. Private Key: enter the password for your private key.

6.2.3. Certificate: upload your certificate file. The certificate subject must match the DNS address provided.

6.2.4. Click Save. The system will switch to HTTPS.

6.3. API user creation & init script download

6.3.1. Create an API User (low-privileged deployment user, cannot manage policies).

6.3.2. Click Download Init Script to download the installation package.

6.3.3. Clarification: the init script contains the base installation only and does not include specific client-side configurations or policies.

6.4. Pilot installation

6.4.1. Extract the ZIP file (contains a cmd and an .exe).

6.4.2. Run the cmd via Command Prompt with admin permission on a pilot machine.

6.4.3. After pilot validation, apply required configurations in the pilot machine, then export an updated script for organization-wide deployment.

7. Sensitive data locations (Windows)

7.1. The product stores customer/application data locally on the Windows instance at:

7.1.1. C:\ProgramData\yazam\data\

7.1.2. SQLite database file: stored under the same folder (e.g., *.db)

7.1.3. User accounts file (JSON): C:\ProgramData\yazam\data\users.json

7.2. Credentials / password storage

7.2.1. User passwords are not stored in plaintext. Passwords are stored as a one-way hash (non-reversible).

7.2.2. If a user forgets a password, an administrator must reset the password via the management interface under Option Tab.

8. Encryption configuration

8.1. In transit: management access is HTTP initially and becomes HTTPS after the customer uploads a valid TLS/SSL certificate.

8.2. At rest (local files): application data (SQLite DB files and user accounts JSON) stored under C:\ProgramData\yazam\data\ is not encrypted by the application by default.

8.3. Optional at-rest protection: customers may enable disk-level encryption according to their AWS/Windows policies (for example, EBS encryption and/or Windows BitLocker) to protect data stored on the instance.

9. Cryptographic material & rotation requirements

9.1. TLS/SSL certificate: rotate/replace periodically (recommended every 6–12 months or per organization policy) by uploading a new certificate in the management UI and verifying HTTPS access.

9.2. Admin/API credentials: rotate periodically (recommended every 60–90 days) and reset immediately if compromise is suspected.

10. Backup & recovery (SQLite + users JSON)

10.1. Backup

10.1.1. Stop the application (Windows Service / application process), then back up the entire folder:

C:\ProgramData\yazam\data\

(includes SQLite .db files and the users JSON file)

10.2. Recovery

10.2.1. Stop the application → restore the folder contents to the same path → start the application → verify login and operation.

11. Monitoring / troubleshooting

11.1. Verify CloudFormation stack is CREATE_COMPLETE and EC2 status checks are passing

11.2. Verify the management UI loads at http://%client_Dns%/management/home (or https://... after certificate upload).

11.3. Verify required inbound ports are allowed on the selected Security Group and Windows Firewall.

11.4. Review data/logs under C:\ProgramData\yazam\data\ as needed for troubleshooting.

12. AWS service quotas (Service Quotas guidance)

If stack creation fails, check AWS Service Quotas for the target region and request increases if needed (common quotas: EC2 vCPU/instances, EBS volumes/snapshots, Elastic IPs, network interfaces).

13. Pricing notes

Costs include the selected EC2 instance type and EBS root volume size. Additional AWS charges may apply for standard items such as data transfer.

14. IAM roles / policies and keys

14.1. This product does not create IAM roles or IAM policies via CloudFormation.

14.2. This product does not create KMS keys via CloudFormation.

14.3. The product does not require customers to provide static AWS access keys.

15. Uninstall / cleanup

To remove the deployment, delete the CloudFormation stack. Ensure you have backed up required data from C:\ProgramData\yazam\data\ before deletion.