Implementation Guide

Digital Evidence Archive

Digital Evidence Archive: Implementation Guide

Table of Contents

Overview

Digital Evidence Archive on AWS (DEA) is a solution that enables investigative units to store and manage digital evidence through Amazon Simple Storage Service (Amazon S3) and Amazon DynamoDB. DEA provides a web user interface (UI) that investigators and other law enforcement personnel can use to create and update cases and associated digital evidence. DEA uses Amazon S3 Intelligent-Tiering to dynamically change the storage class used for digital evidence based on how often users access them, which reduces costs incurred when using DEA.

With DEA, law enforcement customers can optimize their total cost of ownership by reducing management of multiple storage repositories, reliance on physical devices such as USBs and hard drives, and operational costs associated with running a local data center.

DEA maintains file integrity, hashing, encryption, and audit logging to help customers meet requirements of the Criminal Justice Information Services (CJIS) Security Policy. There are no additional charges or upfront commitments required to use DEA. You only pay for AWS services used in your DEA deployment, such as Amazon Simple Storage Service pricing. DEA integrates with your external identity provider, allowing agencies to use their existing single sign-on (SSO) configuration. This solution can also support non-standard AWS partitions, including the AWS GovCloud (US) Regions.

This implementation guide provides an overview of the Digital Evidence Archive on AWS solution, its reference architecture and components, considerations for planning the deployment, and configuration steps for deploying the Digital Evidence Archive solution to the Amazon Web Services (AWS) Cloud.

Use this navigation table to quickly find answers to these questions:

If you want to . . .	**Read . . .**
Know the cost for running this solution.	Cost
Understand the security considerations for this solution.	Security
Know how to plan for quotas for this solution.	Quotas

If you want to . . .	Read . . .
Know which AWS Regions are supported for this solution.	Supported AWS Regions
View or download the AWS CloudFormation template included in this solution to automatically deploy the infrastructure resources (the “stack”) for this solution.	AWS CloudFormation template

This guide is intended for solutions architects, business decision makers, DevOps engineers, data scientists, and cloud professionals who want to implement Digital Evidence Archive on AWS in their environment.

⚠ **Important**

This open source AWS Solution is subject to additional notices. For more information on your customer responsibility, see Notices.

Features and benefits

The Digital Evidence Archive on AWS solution provides the following features:

Easy-to-use web UI for law enforcement

A simple web UI for investigative units to manage their data in one place, without needing to use the AWS Management Console. No cloud knowledge is required to leverage the scale, elasticity, and automation capabilities of AWS through this solution.

Cost optimization with pay-as-you-go pricing

You only pay for the storage and compute services used within this solution. By default, Digital Evidence Archive uses Amazon Simple Storage Service Intelligent-Tiering to store data cost-efficiently.

Data integrity and compliance

Data within Digital Evidence Archive is encrypted. Comprehensive audit logs can be generated at the file, user, case, and system level. Access controls allow permissions to be granted on an as-needed basis. Files are hashed upon upload and can be validated to verify evidence has not been changed from its original form so users can maintain chain of custody.

Integration with Service Catalog AppRegistry and AWS Systems Manager Application Manager

This solution includes a Service Catalog AppRegistry resource to register the solution’s CloudFormation template and its underlying resources as an application in both Service Catalog AppRegistry and AWS Systems Manager Application Manager. With this integration, you can centrally manage the solution’s resources.

Use cases

Digital Evidence Management

Law enforcement agencies struggle to store and manage an ever-increasing amount of digital evidence produced during operations and investigations. AWS and its partners build solutions for managing, storing, and analyzing digital evidence. The solutions are secure, cost-effective, and scalable to meet agencies' growing needs. By managing evidence in the cloud, maintaining compliance, preserving data integrity and the chain of custody, managing the lifecycle of evidence is easier than ever.

Concepts and definitions

This section describes key concepts and defines terminology specific to this solution:

Case Audit Log

A CSV file used to track changes made to cases created in Digital Evidence Archive.

Case Manager

An administrative user persona within Digital Evidence Archive.

Case Member

A non-admin user persona that classifies someone as being involved in a case.

Case Owner

A user persona that classifies someone as being responsible for a case.

Destination location

When performing a mass data ingestion, the destination location is the DEA dataset's location to which AWS DataSync transfers data.

Digital evidence

Digitally formatted evidence contained for a forensic case. Examples of this evidence type are photos, files, and other digital content.

Source location

When performing a mass data ingestion, the source location is the storage system or source from which AWS DataSync transfers data.

For a general reference of AWS terms, see the AWS glossary in the AWS General Reference.