

Service Name

AWS AppFabric

Service Overview

AWS AppFabric is a fully managed service that quickly connects software-as-a-service (SaaS) applications across organizations to enhance security and increase productivity. It consists of two facets: AppFabric for security, which aggregates and normalizes audit logs from SaaS applications into a central repository using the Open Cybersecurity Schema Framework (OCSF), enabling IT and security teams to manage and secure applications using a standard schema; and AppFabric for productivity (preview), which leverages generative AI powered by Amazon Bedrock to enable employees to complete everyday tasks faster by automating task management and generating insights across their SaaS productivity applications. The service eliminates the need for custom code development and maintenance to connect applications.

Key Use Cases

- Use case 1: Security observability enhancement - Aggregating and normalizing audit logs from multiple SaaS applications to provide centralized security monitoring, standardized alerts, and improved incident response capabilities
- Use case 2: User access management - Quickly managing and auditing employee access across connected SaaS applications, enabling IT teams to see who has access to what applications through a single interface
- Use case 3: AI-powered productivity enhancement - Using generative AI to automatically facilitate tasks across applications, generate insights, prepare for meetings, and prioritize daily work activities

Features

- **Normalized Audit Logs:** Automatically normalizes SaaS application audit logs using the Open Cybersecurity Schema Framework (OCSF) into standardized formats (JSON or Apache Parquet)
- **Enriched Audit Logs:** Automatically enriches audit log data with user email addresses and additional context like IP addresses and user agent strings for comprehensive analysis
- **User Access Management:** Enables quick search and management of employee access across connected applications using corporate email addresses
- **Generative AI Assistant:** Powered by Amazon Bedrock, provides AI-driven insights and actions across applications with cross-app context
- **No-Code Integration:** Connects multiple SaaS applications without requiring custom code development or maintenance

- **Data Encryption:** Encrypts data at rest using AWS KMS keys and in transit using TLS 1.2 with AWS Signature V4

Value Proposition

AWS AppFabric provides unique value by eliminating the complexity and cost of building custom integrations between SaaS applications. It reduces operational costs by removing the need for custom code development and maintenance while automatically providing normalized audit logs in near real-time (every 2 minutes):

- The service offers enhanced security observability through standardized OCSF schema, enabling common security policies and standardized alerts across multiple applications
- AppFabric's generative AI capabilities powered by Amazon Bedrock provide cross-application insights and automation that competitors cannot match
- The service supports over 20 popular SaaS applications including Microsoft 365, Google Workspace, Slack, Zoom, and Salesforce, with compatibility for leading security tools like Splunk, Rapid7, and Netskope
- Organizations benefit from faster incident response times through enriched audit logs with user email addresses and reduced security blind spots across their SaaS portfolio

Service Integration

AWS AppFabric integrates deeply with several core AWS services to deliver its functionality. Primary integrations include Amazon S3 for storing aggregated audit log data, Amazon Kinesis Data Firehose for streaming normalized data to security tools and destinations, and AWS Key Management Service (KMS) for encryption of data at rest and customer-managed keys:

- The service leverages Amazon Bedrock to power its generative AI capabilities for productivity features
- AppFabric works with Amazon Security Lake to improve security posture by delivering OCSF-normalized data in Apache Parquet format
- Additional integrations include AWS CloudTrail for API and user activity logging, Amazon CloudWatch for metrics and monitoring, and AWS IAM for access control and service-linked roles
- The service also supports integration with Amazon Athena for querying audit log data and Amazon QuickSight for visualization and business intelligence dashboards

Onboarding and Offboarding

Customers get started with AppFabric by first creating an AWS account and navigating to the AppFabric console in supported regions (US East N. Virginia, Asia Pacific Tokyo, or Europe Ireland):

- The process begins with creating an app bundle, which serves as a container for app authorizations and ingestions
- During setup, customers configure encryption using either AWS-owned keys or customer-managed KMS keys
- Next, they authorize applications by providing necessary credentials like tenant IDs, client secrets, or personal access tokens for each SaaS application
- After authorization, customers set up audit log ingestions to specify destinations (Amazon S3 or Kinesis Data Firehose) for normalized data
- The user access tool can then be configured for employee access management
- AppFabric provides step-by-step guidance in the console and comprehensive documentation
- The service offers a 30-day free tier for the first two applications to facilitate proof-of-concept deployments

Getting Started Guide:

<https://docs.aws.amazon.com/appfabric/latest/adminguide/getting-started-security.html>

Data Removal

When offboarding from AppFabric, customers can remove their data by deleting app bundles, which permanently removes all associated metadata. Audit log data stored in customer-owned Amazon S3 buckets or delivered through Kinesis Data Firehose remains under customer control and must be deleted separately according to their data retention policies. AppFabric automatically retires issued grants on customer-managed KMS keys when app bundles are deleted. Intermediate S3 buckets used for temporary data processing are automatically deleted after 30 days using lifecycle policies. Customers should also revoke application authorizations and remove AppFabric access from their SaaS applications.

Backup/Restore and Disaster Recovery

AppFabric does not provide built-in backup and disaster recovery capabilities as it is a data aggregation and normalization service. The service relies on the underlying AWS infrastructure's resilience and availability. Customer audit log data is stored in Amazon S3 or streamed through Kinesis Data Firehose to customer-specified destinations, where standard AWS service backup and recovery features apply. AppFabric metadata and configurations are managed by AWS, and customers should document their app bundle configurations, authorizations, and ingestion settings for disaster recovery planning purposes.

Backup Capabilities

AppFabric does not have native backup capabilities as it functions as a data processing and aggregation service. The service does not store long-term customer data that would require backup:

- Audit log data flows through AppFabric to customer-specified destinations (Amazon S3 or Kinesis Data Firehose), where customers can implement their own backup strategies using AWS Backup or S3 versioning and replication features
- AppFabric configurations and authorizations should be documented and can be recreated as needed

Disaster Recovery

AppFabric does not directly support AWS Elastic Disaster Recovery as it is not a compute-intensive service requiring replication of instances or volumes. The service operates across multiple AWS regions (US East N:

- Virginia, Asia Pacific Tokyo, Europe Ireland) with AWS-managed high availability
- Customers should implement disaster recovery strategies for their audit log destinations in Amazon S3 or Kinesis Data Firehose using cross-region replication, backup policies, and documentation of AppFabric configurations for recreation in alternate regions if needed

Recovery Objectives

AppFabric helps customers meet RPO and RTO objectives by providing continuous audit log ingestion every two minutes, minimizing data loss in security monitoring scenarios. The service's near real-time data processing reduces the recovery point objective for security incident detection and response. However, since AppFabric is a data processing service without persistent storage, traditional RPO/RTO metrics are less applicable. Customers achieve their recovery objectives through the underlying AWS infrastructure's availability and by implementing appropriate backup and recovery strategies for their chosen data destinations.

Service Constraints

Service Quotas: <https://docs.aws.amazon.com/appfabric/latest/adminguide/limits.html>

FAQ: <https://aws.amazon.com/appfabric/faqs/>

Technical Requirements

Service Documentation:

<https://docs.aws.amazon.com/appfabric/latest/adminguide/what-is-appfabric.html>

User Guide: <https://docs.aws.amazon.com/appfabric/latest/adminguide/getting-started-security.html>

API Reference: <https://docs.aws.amazon.com/appfabric/latest/api/Welcome.html>

Pricing Overview

Please see the AWS UK G Cloud 15 Pricing Document accompanying this service in the Digital Marketplace.

Public Pricing: <https://aws.amazon.com/appfabric/pricing/>

Cost Optimization

AppFabric offers several cost optimization strategies specific to SaaS security management. The service eliminates the need for custom integration development and maintenance costs, providing significant operational savings:

- Customers benefit from a pay-as-you-go pricing model at \$3 per user per month with volume discounts available for organizations with over 2,000 users
- The 30-day free tier for the first two applications allows for cost-effective proof-of-concept testing
- Organizations can optimize costs by carefully selecting which applications to connect based on security priorities
- Data storage costs can be managed by implementing appropriate S3 lifecycle policies and choosing between JSON and more storage-efficient Apache Parquet formats
- The user access feature pricing is per-search rather than per-user, allowing cost control based on actual usage patterns

Savings Considerations

The primary cost savings from AppFabric come from eliminating the need to build and maintain custom integrations between SaaS applications, which can cost hundreds of thousands of dollars in development and ongoing maintenance. Organizations save on security analyst time through normalized, enriched audit logs that accelerate incident response and reduce investigation time:

- The centralized user access management reduces IT overhead for access auditing and compliance reporting across multiple applications
- By providing standardized OCSF schema, AppFabric reduces the complexity and cost of security tool implementations and maintenance
- The generative AI productivity features can significantly reduce time spent on routine tasks like meeting preparation and task prioritization
- Volume pricing discounts and the ability to start with a subset of applications allow organizations to scale cost-effectively based on demonstrated value and ROI