

Service Name

Amazon Managed Grafana

Service Overview

Amazon Managed Grafana is a fully managed and secure data visualization service that enables users to instantly query, correlate, and visualize operational metrics, logs, and traces from multiple sources. It simplifies the deployment, operation, and scaling of Grafana, a popular open-source data visualization tool. Users create logically isolated Grafana servers called workspaces to build dashboards and visualizations without managing underlying infrastructure. The service handles provisioning, scaling, maintenance, and provides built-in security features including single sign-on, data access control, and audit reporting for corporate governance compliance.

Key Use Cases

- **Cloud Infrastructure Monitoring:** Monitor AWS resource utilization, cost analysis, and performance metrics across multi-account environments
- **Application Performance Management:** Create application-specific dashboards for request latency, error rates, and user experience metrics
- **Security Operations:** Display security events in dedicated dashboards for rapid incident response and investigation
- **Operational Observability:** Centralize monitoring data from multiple AWS services like CloudWatch, X-Ray, and OpenSearch Service
- **DevOps and Team Collaboration:** Share interactive dashboards across teams with role-based access control

Features

- **Unified Observability:** Visualize and correlate data across multiple data sources with pre-built panels and dashboards
- **Multi-Account Access:** Secure access to AWS data across multiple accounts and regions using AWS Organizations integration
- **Grafana Alerting:** Robust alerting system with centralized alerting information and multiple alert instances from single rules
- **Team Collaboration:** Easy dashboard sharing with user authentication, authorization, and team-based access control
- **Plugin Management:** Install, update, and manage Grafana community plugins and Enterprise plugins for extended data source support
- **VPC Integration:** Connect to private data sources in VPCs without exposing traffic to the internet

- **Enterprise Security:** Built-in security with SAML 2.0 and AWS IAM Identity Center integration, encryption at rest and in transit

Value Proposition

Amazon Managed Grafana eliminates the operational burden of managing Grafana infrastructure while providing enterprise-grade security and scalability. It offers automatic scaling, high availability, automated version updates, and security patching:

- The service provides superior visualization capabilities compared to CloudWatch with advanced widgets, supports data sources beyond AWS services, and enables separate access management from AWS accounts
- Integration with AWS Organizations allows seamless multi-account data access, while the extensive plugin ecosystem supports diverse data sources including third-party and open-source tools
- The pay-per-active-user pricing model with a 90-day free trial makes it cost-effective for teams of all sizes

Service Integration

Amazon Managed Grafana natively integrates with key AWS observability and data services including Amazon CloudWatch for metrics and logs, Amazon OpenSearch Service for search analytics, AWS X-Ray for distributed tracing, AWS IoT SiteWise for industrial data, Amazon Timestream for time-series data, and Amazon Managed Service for Prometheus for container metrics. It leverages AWS IAM Identity Center and AWS Organizations for authentication and multi-account access management:

- The service uses AWS CloudFormation StackSets for cross-account permission provisioning and integrates with Amazon SNS for alert notifications
- Additional integrations include Amazon Athena for data queries, Amazon RDS for database connections, and AWS VPC for private network access to data sources

Onboarding and Offboarding

Customers begin by creating a workspace in the Amazon Managed Grafana console, selecting authentication methods (AWS IAM Identity Center or SAML), and choosing service-managed permissions for simplified setup. The service automatically provisions necessary IAM roles and policies when AWS data sources are selected:

- Users can enable up to 5 workspaces per region initially
- Setup requires the AWSGrafanaAccountAdministrator policy for workspace creation
- After workspace creation, users sign into the Grafana console to configure data sources using the AWS Data Sources plugin, create dashboards, and manage team access

- The service provides getting started tutorials and pre-built dashboard templates to accelerate initial configuration and time-to-value

Getting Started Guide: <https://docs.aws.amazon.com/grafana/latest/userguide/getting-started-with-AMG.html>

Data Removal

When deleting an Amazon Managed Grafana workspace, all associated configuration data including dashboards, data source configurations, alerts, and snapshots are permanently removed. Users must navigate to the Amazon Managed Grafana console, select the workspace, and choose Delete with confirmation requiring the workspace name. The service provides API endpoints for programmatic deletion. Note that deleting a workspace does not automatically remove associated IAM roles, which should be cleaned up separately to maintain security best practices.

Backup/Restore and Disaster Recovery

Amazon Managed Grafana provides built-in high availability and automatic recovery capabilities. The service offers snapshot functionality through the Snapshot API for dashboard backups. Snapshots can be stored locally within the workspace or externally on external servers. However, the service does not provide traditional backup and restore capabilities for entire workspaces. Data persistence relies on the managed infrastructure's durability, with dashboards and configurations stored securely in the AWS managed environment with encryption at rest.

Backup Capabilities

Amazon Managed Grafana supports dashboard snapshots through the Snapshot API, allowing users to create point-in-time backups of dashboard configurations and data. Snapshots can be saved locally or externally with configurable expiration times:

- The service does not integrate with AWS Backup for automated backup strategies
- Users can export dashboard configurations using Grafana APIs and Terraform for infrastructure-as-code backup approaches

Disaster Recovery

Amazon Managed Grafana provides high availability within regions through automatic scaling and recovery mechanisms. The service does not integrate with AWS Elastic Disaster Recovery:

- For cross-region disaster recovery, customers must manually recreate workspaces and restore configurations in alternate regions
- The service's managed nature ensures infrastructure-level resilience, but application-level disaster recovery requires manual planning and implementation

Recovery Objectives

Amazon Managed Grafana helps achieve low RTO objectives through its highly available managed infrastructure with automatic failover and recovery. The service provides instant workspace provisioning and rapid dashboard restoration from snapshots. However, RPO objectives depend on manual backup strategies using snapshot APIs or configuration exports. Customers can minimize data loss by implementing regular dashboard exports and maintaining infrastructure-as-code definitions for workspace configurations.

Service Constraints

Service Quotas:

https://docs.aws.amazon.com/grafana/latest/userguide/AMG_quotas.html

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

Technical Requirements

Service Documentation: <https://docs.aws.amazon.com/grafana/latest/userguide/what-is-Amazon-Managed-Service-Grafana.html>

User Guide: <https://docs.aws.amazon.com/grafana/latest/userguide/getting-started-with-AMG.html>

API Reference:

<https://docs.aws.amazon.com/grafana/latest/APIReference/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/grafana/pricing/>

Cost Optimization

Amazon Managed Grafana offers a 90-day free trial with up to 5 free users per account to minimize initial costs. The pay-per-active-user pricing model charges only for users who access the workspace within 24 hours, not provisioned users:

- API requests are free, helping reduce costs for automated workflows
- Customers can optimize costs by using Viewer licenses (\$5/month) instead of Editor licenses (\$9/month) where appropriate, managing user access patterns to minimize active user counts, and leveraging the free tier for small teams
- Multiple workspaces allow cost segregation between environments

Savings Considerations

Key cost savings include eliminating infrastructure management overhead compared to self-hosted Grafana deployments, reducing operational costs through automatic scaling and maintenance, and avoiding upfront commitments with pay-as-you-use pricing. The service eliminates costs for server provisioning, security patching, version updates, and high availability setup:

- Enterprise plugin licensing provides cost-effective access to premium data sources compared to separate vendor contracts
- Organizations can achieve economies of scale by centralizing monitoring across multiple AWS accounts while maintaining granular access control and cost allocation