Service Name

AWS Secrets Manager

Service Overview

AWS Secrets Manager is a fully managed service that helps manage, retrieve, and rotate database credentials, application credentials, OAuth tokens, API keys, and other secrets throughout their lifecycles. The service eliminates the need to hard-code credentials in application source code, reducing the risk of compromise. Secrets Manager encrypts secrets at rest using AWS KMS and secures transmission over TLS. It enables automatic rotation of secrets, replacing long-term credentials with short-term ones, and allows applications to retrieve credentials dynamically at runtime through API calls.

Key Use Cases

- Database credential management: Store and automatically rotate credentials for Amazon RDS, DocumentDB, Redshift, and other database services without disrupting applications
- Application security: Replace hard-coded API keys, OAuth tokens, and application credentials with dynamic retrieval from Secrets Manager
- Third-party SaaS integration: Manage and automatically rotate credentials for external services like Salesforce, Snowflake, and other SaaS providers
- Multi-region disaster recovery: Replicate secrets across multiple AWS regions for business continuity and low-latency access
- Compliance and auditing: Meet regulatory requirements with comprehensive logging, monitoring, and fine-grained access controls for sensitive credentials

Features

- **Automatic Rotation**: Schedule-based or on-demand rotation of secrets without disrupting applications, with built-in support for AWS services and third-party providers
- **Encryption**: End-to-end encryption at rest using AWS KMS keys and in transit using TLS, with support for customer-managed keys
- **Cross-Region Replication**: Automatic replication of secrets to multiple AWS regions for disaster recovery and cross-regional redundancy
- **Fine-Grained Access Control**: Integration with IAM for granular permissions, resource-based policies, and support for attribute-based access control
- **Managed External Secrets**: Lambda-free managed rotation for third-party SaaS providers with predefined secret formats and integrated partner ecosystem
- **Comprehensive Auditing**: Complete logging through AWS CloudTrail, monitoring via CloudWatch, and integration with security services like GuardDuty

- **Caching Support**: Built-in caching libraries and Lambda extensions to improve performance and reduce costs when retrieving secrets
- **Batch Operations**: Ability to retrieve multiple secrets in a single API call for improved efficiency in applications

Value Proposition

AWS Secrets Manager provides a comprehensive, fully managed solution for secret management that eliminates operational overhead while enhancing security. Unlike hard-coding credentials or manual rotation processes, Secrets Manager offers automatic rotation, enterprise-grade encryption, and seamless integration with AWS services:

- Key differentiators include Lambda-free managed rotation for third-party services, cross-region replication for disaster recovery, fine-grained access controls, and comprehensive auditing capabilities
- The service's pay-as-you-go pricing model with no setup fees, combined with built-in caching support and high API rate limits, makes it cost-effective for applications of any scale while meeting strict compliance requirements

Service Integration

AWS Secrets Manager integrates deeply with core AWS services to provide seamless credential management. Primary integrations include Amazon RDS, DocumentDB, and Redshift for automatic database credential rotation; AWS Lambda for secret retrieval through extensions and Powertools; Amazon EKS for Pod Identity integration; and AWS IAM for access control:

- The service works with AWS KMS for encryption key management, CloudTrail for audit logging, CloudWatch for monitoring, and GuardDuty for security threat detection
- Additional integrations span compute services like ECS and App Runner, data services like Athena and EMR, and developer tools like CodeBuild, enabling centralized secret management across the entire AWS ecosystem

Onboarding and Offboarding

Getting started with AWS Secrets Manager involves creating secrets through the AWS console, CLI, or SDKs, with built-in tutorials for common scenarios like moving hard-coded credentials and setting up database rotation. Users need the SecretsManagerReadWrite managed policy and can begin with tutorials for hardcoded secrets migration, database credential management, or rotation setup:

- The service offers multiple secret types including database credentials, API keys, and OAuth tokens, with managed external secrets available for supported partners
- Applications integrate by replacing hard-coded credentials with API calls to retrieve secrets dynamically, utilizing caching libraries for performance optimization

Getting Started Guide:
https://docs.aws.amazon.com/secretsmanager/latest/userguide/intro.html

Data Removal

Secret deletion in AWS Secrets Manager includes a configurable recovery window (7-30 days) during which secrets can be restored before permanent deletion. Customers can delete secrets immediately by setting the recovery window to zero, though this prevents restoration. The DeleteSecret API operation removes all secret versions and metadata. When offboarding, replicated secrets across regions must be deleted separately. CloudTrail logs capture all deletion activities for audit purposes.

Backup/Restore and Disaster Recovery

AWS Secrets Manager provides automatic cross-region replication for disaster recovery, maintaining synchronized copies of secrets and their metadata across multiple regions. Replicated secrets have the same ARN with region-specific endpoints and support automatic rotation propagation. The service maintains versioned secrets with labeled versions (AWSCURRENT, AWSPREVIOUS, AWSPENDING) enabling rollback capabilities. Secret replication improves workload resilience and supports low-latency access requirements across geographic regions.

Backup Capabilities

Secrets Manager implements versioning as its backup mechanism, maintaining multiple versions of each secret with staging labels. The service automatically retains previous secret versions during rotation and allows manual version management:

- Cross-region replication serves as geographic backup, with replicas maintaining independent versions while staying synchronized with the primary secret
- The service does not integrate with AWS Backup as traditional backup is replaced by versioning and replication features

Disaster Recovery

While AWS Secrets Manager doesn't directly integrate with AWS Elastic Disaster Recovery, it provides essential disaster recovery capabilities through cross-region replication and high availability design. Replicated secrets automatically synchronize across regions, enabling applications to failover seamlessly:

- The service's regional endpoints ensure continued access during regional impairments
- Multi-AZ deployment and 99.95% SLA provide resilience within regions, while cross-region replication supports broader disaster recovery strategies

Recovery Objectives

AWS Secrets Manager helps achieve low RPO and RTO objectives through cross-region replication with near real-time synchronization, eliminating data loss during regional failures. The service's high availability design with 99.95% SLA and multi-AZ deployment minimizes downtime. Cached secret retrieval and high API rate limits (10,000 requests/second for GetSecretValue) ensure rapid secret access during recovery scenarios. Automatic rotation ensures secrets remain current even during extended outages.

Service Constraints

Service Quotas:
https://docs.aws.amazon.com/secretsmanager/latest/userguide/reference_limits.html

FAQ: https://aws.amazon.com/secrets-manager/faqs/

Technical Requirements

Service Documentation:
https://docs.aws.amazon.com/secretsmanager/latest/userguide/intro.html

User Guide: https://docs.aws.amazon.com/secretsmanager/latest/userguide/intro.html

API Reference:
https://docs.aws.amazon.com/secretsmanager/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/secrets-manager/pricing/

Cost Optimization

AWS Secrets Manager offers several cost optimization strategies: utilize the free tier for new customers with $200 credits; implement caching to reduce API calls and associated costs; use cost allocation tags to track and allocate secret usage across business units; consider secret consolidation where appropriate to reduce per-secret monthly charges; leverage managed rotation to eliminate Lambda function costs for supported services; and monitor unused secrets for deletion. The pay-as-you-go model charges $0.40 per secret per month plus $0.05 per 10,000 API calls, making cost tracking granular and predictable.

Savings Considerations

Primary cost savings come from eliminating manual credential management overhead and reducing security incident risks. Automated rotation eliminates operational costs of manual updates and application deployments:

- Cross-region replication reduces disaster recovery complexity compared to custom solutions
- Managed external secrets eliminate Lambda function development and maintenance costs
- Caching reduces API call costs significantly for high-frequency applications
- Cost allocation tags enable precise chargeback to business units, improving cost accountability
- The service's integration with AWS services reduces development time and operational complexity, delivering substantial indirect cost savings through improved operational efficiency