AWS Leitfaden zur Entscheidungsfindung

Auswahl eines AWS Kryptografiedienstes

Auswahl eines AWS Kryptografiedienstes: AWS Leitfaden zur Entscheidungsfindung

Table of Contents

Auswahl eines AWS Kryptografiedienstes

Den ersten Schritt machen

Zweck	Finden Sie heraus, welche AWS Kryptografiedienste für Ihr Unternehmen am besten geeignet sind.
Letzte Aktualisierung	31. Januar 2025
Abgedeckte Dienste	• AWS Certificate Manager • AWS CloudHSM • AWS SDK für Datenbankverschlüsselung • AWS Encryption SDK • AWS KMS • AWS Private CA • AWS Secrets Manager
Verwandte Leitfäden	Auswahl von AWS Sicherheits-, Identitäts- und Governance-Diensten

Einführung

Kryptografie ist ein Eckpfeiler der Sicherheit beim Cloud Computing und trägt dazu bei, die Vertraulichkeit, Integrität und Authentizität von Daten zu gewährleisten. In einer Cloud-Umgebung können sensible Daten öffentliche Netzwerke durchqueren und sich in einer gemeinsam genutzten Infrastruktur befinden. Daher sind robuste kryptografische Maßnahmen für den Schutz vor unbefugtem Zugriff oder Manipulation unerlässlich.

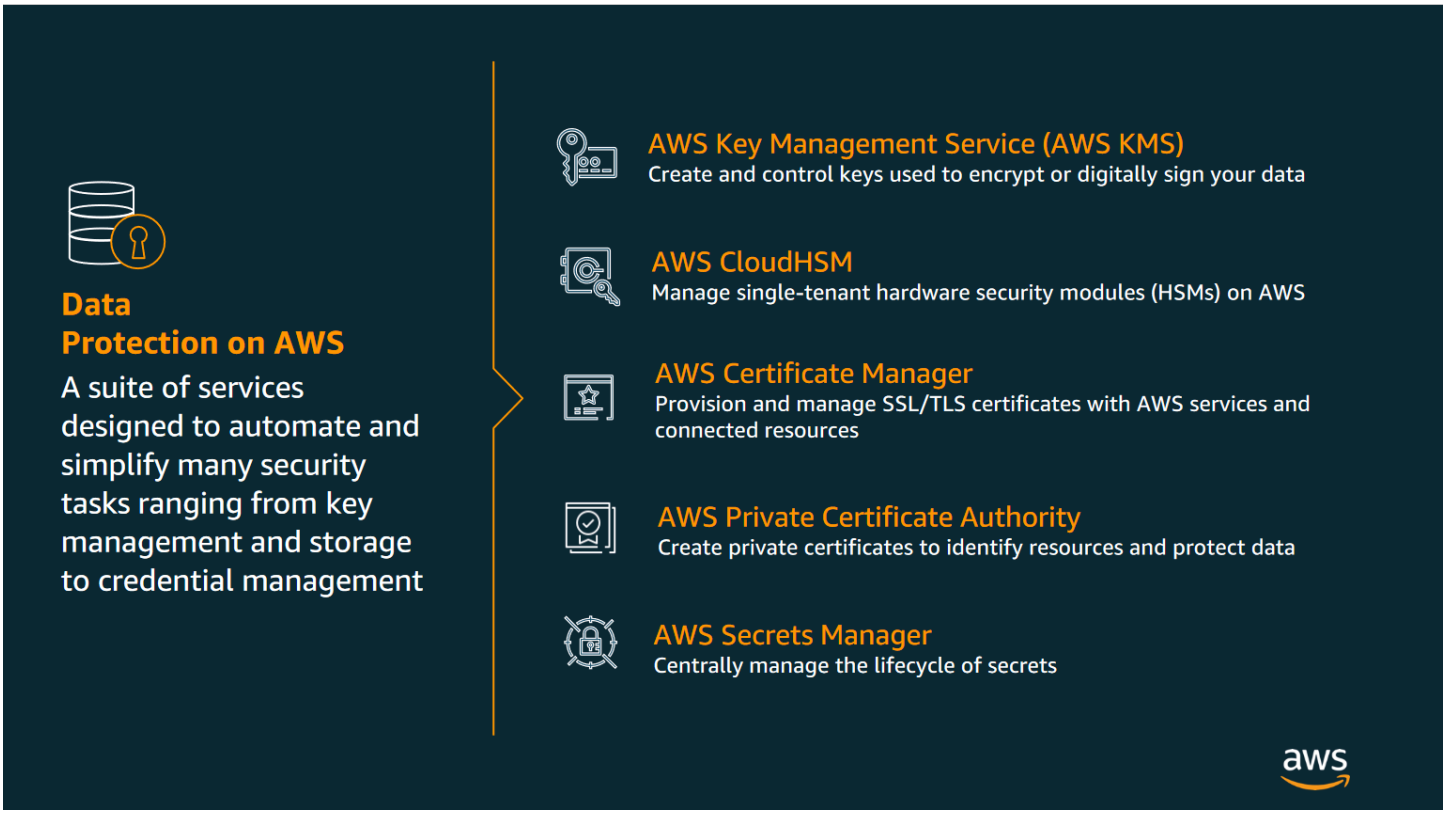
AWS bietet eine umfassende Palette von kryptografischen Diensten zur Sicherung von Daten, zur Verwaltung von Verschlüsselungsschlüsseln und zum Schutz vertraulicher Informationen. Dazu gehören AWS Key Management Service (KMS) für die zentrale Schlüsselverwaltung, AWS CloudHSM für PKCS11 Anwendungen und spezielle Hardware-Sicherheitsmodule sowie AWS Encryption SDK für die clientseitige Verschlüsselung. AWS Secrets Manager ist ein Dienst, mit dem Sie vertrauliche Informationen wie Datenbankanmeldedaten, API-Schlüssel und andere Geheimnisse

während ihres gesamten Lebenszyklus sicher speichern, verwalten und abrufen können. AWS Certificate Manager (ACM) vereinfacht den Prozess der Bereitstellung, Verwaltung und Bereitstellung von öffentlich vertrauenswürdigen Transport Layer Security (TLS) -Zertifikaten zur Verwendung mit. AWS-Services Mit dem AWS Private Certificate Authority (PCA) können Sie x509-Zertifikate für Ihre internen Ressourcen generieren und verteilen.

Der Leitfaden soll Ihnen bei der Auswahl der AWS Kryptografiedienste und -tools helfen, die für Ihre Bedürfnisse und Ihr Unternehmen am besten geeignet sind.

Das folgende Video ist ein zweiminütiger Abschnitt einer Präsentation, in der bewährte Methoden für die Kryptografie vorgestellt werden.

Verstehen



Die Auswahl der richtigen AWS Kryptografiedienste hängt von Ihrem spezifischen Anwendungsfall, Ihren Datensicherheitsanforderungen, Compliance-Verpflichtungen und betrieblichen Präferenzen ab, wie in den folgenden Tabellen dargestellt.

Key management

Wenn Sie Verschlüsselungsschlüssel sicher verwalten müssen, sollten Sie den AWS Key Management Service (KMS) in Betracht ziehen. Es ermöglicht Ihnen, kryptografische Schlüssel, die in andere AWS-Services integriert sind, zu erstellen, zu rotieren und zu verwalten. KMS verwendet FIPS-validierte Daten HSMs , um Sie bei der Erfüllung von Compliance-Anforderungen zu unterstützen und sicherzustellen, dass die Implementierung der von KMS offengelegten kryptografischen Primitiven korrekt ist. Einige Anwendungen erfordern bestimmte kryptografische Funktionen oder Anwendungsschnittstellen, die nur mit einem herkömmlichen HSM verfügbar sind, und stellen spezielle Hardware-Sicherheitsmodule (HSMs) in der Cloud AWS CloudHSM bereit, sodass Sie die volle Kontrolle über Ihre kryptografischen Schlüssel und Operationen haben.

Data encryption

Für die Verschlüsselung sensibler Daten wie Kundendaten oder geistiges Eigentum AWS KMS ist es eng in AWS Speicher-, Datenbank- und Messaging-Dienste (z. B. S3, RDS oder EBS) integriert. Wenn Sie eine clientseitige Verschlüsselung benötigen, AWS Encryption SDK handelt es sich um eine Open-Source-Bibliothek, mit der Sie Daten in Ihrer Anwendung einfach verschlüsseln können, bevor sie an die Cloud gesendet werden.

Secure communications

Um Daten bei der Übertragung zu schützen, vereinfacht AWS Certificate Manager (ACM) die Verwaltung öffentlich vertrauenswürdiger TLS-Zertifikate. Verwenden Sie es, um die Identität Ihrer mit dem Internet verbundenen Anwendungen zu bestätigen und die Verschlüsselung der Kommunikation zwischen Ihren Anwendungen, Benutzern und Cloud-Diensten zu erleichtern, ohne sich Gedanken über Zertifikatserneuerungen machen zu müssen. Für interne Anwendungen können Sie AWS Private Certificate Authority (PCA) verwenden, um x509-Zertifikate für Ihre internen Ressourcen, einschließlich Clients und Server, zu generieren und zu verteilen.

Secrets and credentials management

Für das sichere Speichern und Abrufen von Anwendungsgeheimnissen wie Datenbankanmeldedaten, API-Schlüsseln oder Zertifikaten sollten Sie Folgendes in Betracht ziehen. AWS Secrets Manager Es bietet eine automatisierte Rotation von Geheimnissen und detaillierte Zugriffskontrollen. Alternativ ist AWS Systems Manager Parameter Store eine kostengünstigere Option für die Verwaltung nicht sensibler Konfigurationen und kann in diese integriert werden. AWS Secrets Manager

Compliance and auditing

Beachten Sie bei der Einhaltung gesetzlicher Vorschriften die Einhaltung der Verschlüsselungsstandards AWS KMS und tragen Sie AWS CloudHSM dazu bei, dass diese eingehalten werden. AWS Artifact ist ein Self-Service-Portal, das On-Demand-Zugriff AWS auf Sicherheits- und Compliance-Berichte wie ISO-Zertifizierungen und SOC-Berichte sowie die Möglichkeit bietet, Vereinbarungen wie den Business Associate Addendum (BAA) zu überprüfen und zu akzeptieren. Sie können auch Dienste wie AWS Config, und verwenden AWS Security Hub, AWS Audit Manager um die Einhaltung der Vorschriften zu überwachen und die entsprechenden Artefakte für Ihren eigenen Gebrauch oder für die Nutzung durch Ihre Stakeholder zu erstellen.

Beachten Sie bei der Auswahl zwischen AWS Kryptografiediensten die folgenden Anforderungen.

Anforderung	Service
Geringer Aufwand, vollständig verwaltet	AWS KMS oder AWS Secrets Manager
Erfordern spezielle Anwendungsschnittstellen oder kryptografische Algorithmen, die von KMS nicht unterstützt werden	AWS CloudHSM
Encrypting/decrypting Daten in Ihren Anwendungen	AWS Encryption SDK
Vereinfachtes öffentliches TLS-Zertifikatsmanagement	AWS Certificate Manager
Verwaltung von Secrets	AWS Secrets Manager

Indem Sie Ihre Anforderungen an diese Optionen anpassen, können Sie kryptografische Lösungen implementieren, die auf Ihre Sicherheits- und Betriebsanforderungen zugeschnitten sind.

Überlegen Sie

Die Wahl des richtigen AWS Kryptografiedienstes setzt voraus, dass Sie Ihre spezifischen Sicherheits-, Betriebs- und Compliance-Anforderungen verstehen. AWS bietet eine Vielzahl von

kryptografischen Diensten, die jeweils für unterschiedliche Anwendungsfälle konzipiert sind, von der Schlüsselverwaltung über Datenverschlüsselung bis hin zu sicherer Kommunikation. Um eine fundierte Entscheidung zu treffen, sollten Sie Ihre Anforderungen anhand mehrerer kritischer Kriterien bewerten, darunter Ihr Anwendungsfall, Ihre Kontroll- und Flexibilitätsanforderungen, Compliance-Verpflichtungen, Kostenüberlegungen und die Integration mit AWS-Services. Diese Kriterien helfen Ihnen dabei, Ihre Wahl an den Sicherheitszielen und betrieblichen Abläufen Ihres Unternehmens auszurichten.

Use case

Überlegen Sie, wofür Sie den Kryptografiedienst benötigen: Datenverschlüsselung, Schlüsselverwaltung, sichere Kommunikation oder Geheimnisverwaltung. Er AWS KMS eignet sich beispielsweise ideal für integrierte Verschlüsselung und AWS CloudHSM eignet sich gleichzeitig für Unternehmen AWS-Services, die bestimmte kryptografische Funktionen, Anwendungsschnittstellen oder ein einheitliches HSM benötigen, was häufig auf strenge Richtlinien oder spezifische Anwendungsanforderungen zurückzuführen ist. Die Klärung des Zwecks stellt sicher, dass Sie einen Service auswählen, der Ihren Anforderungen entspricht, wodurch sowohl die Funktionalität als auch die Kosten optimiert werden.

Control and flexibility

Beurteilen Sie, wie viel Kontrolle Sie über Ihre kryptografischen Operationen benötigen. Managed Services wie ein Multi-Tenant-HSM AWS KMS bieten Benutzerfreundlichkeit bei minimalem Verwaltungsaufwand und behalten gleichzeitig die volle Kontrolle über Ihr Schlüsselmaterial. Im Gegensatz dazu AWS CloudHSM bietet es ein Single-Tenant-Modell für spezifische Anwendungs-, Kryptografie- oder Compliance-Anforderungen.

Compliance requirements

Wenn Sie in einer regulierten Branche tätig sind, stellen Sie sicher, dass der Service Standards wie GDPR, PCI DSS oder HIPAA entspricht. AWS KMS und AWS CloudHSM sind beide nach FIPS 140-2 Level 3 zertifiziert. Wenn Sie einen Service auswählen, der Ihre Anforderungen nicht erfüllt, können Sie das Vertrauen aufrechterhalten und potenzielle rechtliche oder finanzielle Sanktionen vermeiden.

Cost considerations

Vergleichen Sie Ihr Budget mit dem Preismodell des Services. AWS KMS ist für allgemeine Verschlüsselungsanforderungen kostengünstig, AWS CloudHSM verursacht aber aufgrund der speziellen Hardware höhere Kosten. Wenn Sie die Auswirkungen auf die Kosten verstehen, können Sie Ihre Sicherheitsausgaben optimieren.

Integration with AWS ecosystem

Wenn Sie viel nutzen AWS-Services, sollten Sie einer Kryptografielösung wie ACM Priorität einräumen, die sich nahtlos in S3, RDS AWS KMS oder Lambda integrieren lässt. Dies sorgt für reibungslosere Arbeitsabläufe und reduziert den Entwicklungsaufwand. Integrationsfunktionen können die betriebliche Effizienz erheblich verbessern.

Klicken Sie auf

Die Auswahl des richtigen AWS Kryptografiedienstes setzt voraus, dass Sie Ihre spezifischen Sicherheits-, Betriebs- und Compliance-Anforderungen verstehen. AWS bietet eine Vielzahl von kryptografischen Diensten, die jeweils für unterschiedliche Anwendungsfälle konzipiert sind, von der Schlüsselverwaltung über Datenverschlüsselung bis hin zu sicherer Kommunikation. Um eine fundierte Entscheidung zu treffen, sollten Sie Ihre Anforderungen anhand mehrerer kritischer Kriterien bewerten, darunter Ihr Anwendungsfall, Ihre Kontroll- und Flexibilitätsanforderungen, Compliance-Verpflichtungen, Kostenüberlegungen und die Integration mit AWS-Services. Diese Kriterien helfen Ihnen dabei, Ihre Wahl an den Sicherheitszielen und betrieblichen Abläufen Ihres Unternehmens auszurichten.

Ziel-Anwendungsfall	Wann würden Sie es verwenden?	Empfohlener Service
Schlüsselverwaltung	Um kryptografische Schlüssel, die in andere integriert sind, sicher zu erstellen, zu rotieren und zu verwalten AWS-Services	AWS KMS
Schlüsselverwaltung	Für spezifische Anwendungsintegrationen oder kryptografische Primitive	AWS CloudHSM
Datenverschlüsselung	Um eine clientseitige Verschlüsselung zu implementieren, um sensible Daten wie Kundendaten oder geistiges Eigentum zu schützen.	AWS Encryption SDK AWS SDK zur Datenbankverschlüsselung

Ziel-Anwendungsfall	Wann würden Sie es verwenden?	Empfohlener Service
Sichere Kommunikationen	Um Daten während der Übertragung zu schützen und die Verwaltung von SSL/TLS Zertifikaten zu vereinfachen.	AWS Certificate Manager AWS Private CA
Verwaltung von Geheimnissen und Anmeldeinformationen	Zum sicheren Speichern und Abrufen von Anwendung sgeheimnissen wie Datenbank anmeldedaten, API-Schlüsseln oder Zertifikaten.	AWS Secrets Manager AWS Parameter Store

Verwenden Sie

Sie sollten jetzt genau wissen, was die einzelnen AWS Kryptografiedienste tun und welche für Sie geeignet sein könnten.

Um herauszufinden, wie die einzelnen verfügbaren AWS Kryptografiedienste verwendet werden können, und mehr über sie zu erfahren, haben wir einen Weg bereitgestellt, um zu untersuchen, wie die einzelnen Dienste funktionieren. In den folgenden Abschnitten finden Sie Links zu ausführlicher Dokumentation, praktischen Tutorials und anderen Ressourcen, die Ihnen den Einstieg erleichtern.

AWS Certificate Manager

- Fangen Sie an mit AWS Certificate Manager

  Beginnen Sie mit der Nutzung AWS Certificate Manager, einschließlich der Arbeit mit öffentlichen und privaten Zertifikaten.

  Den Leitfaden erkunden
- Bewährte Methoden für AWS Certificate Manager

  Lesen Sie sich die Empfehlungen durch, die Ihnen helfen können, sie AWS Certificate Manager effektiver zu nutzen.

  Den Leitfaden erkunden

- AWS Certificate Manager Häufig gestellte Fragen

  Auf der FAQ-Seite AWS Certificate Manager (ACM) finden Sie detaillierte Antworten auf häufig gestellte Fragen zu den Funktionen, Fähigkeiten und der Verwendung von ACM. Es behandelt Themen wie die Arten von Zertifikaten, die ACM verwaltet, die Integration mit anderen AWS-Services Zertifikaten und Anleitungen zur Bereitstellung und Verwaltung von Zertifikaten. SSL/TLS

  Erkunden Sie die FAQs

AWS CloudHSM

- Fangen Sie an mit AWS CloudHSM

  Erfahren Sie, wie Sie einen Cluster erstellen, initialisieren und aktivieren in AWS CloudHSM. Nachdem Sie diese Verfahren abgeschlossen haben, können Sie Benutzer verwalten, Cluster verwalten und die integrierten Software-Bibliotheken zur Durchführung kryptografischer Operationen nutzen.

  Den Leitfaden erkunden

- Bewährte Methoden für AWS CloudHSM

  Informieren Sie sich über bewährte Methoden für die Verwaltung und Überwachung Ihres AWS CloudHSM Clusters.

  Den Leitfaden erkunden

- AWS CloudHSM Preisgestaltung

  Weitere Informationen zur Preisgestaltung finden Sie auf der Seite mit den AWS CloudHSM Preisen. Für die Nutzung AWS CloudHSM fallen keine Vorabkosten an. Mit zahlen Sie für jedes HSM AWS CloudHSM, das Sie starten, eine Stundengebühr, bis Sie das HSM kündigen. Dieser Leitfaden enthält den Stundensatz für jede AWS Region.

  Erkunden Sie die Preisseite

- AWS CloudHSM Häufig gestellte Fragen

  Auf der AWS CloudHSM FAQ-Seite finden Sie ausführliche Antworten auf häufig gestellte Fragen AWS CloudHSM zu Funktionen, Preisen, Bereitstellung, Sicherheit, Compliance, Leistung und Integration mit Drittanbieteranwendungen.

Erkunden Sie die FAQs

AWS Encryption SDK

- Fangen Sie an mit dem AWS Encryption SDK

  Erfahren Sie, wie Sie das AWS Encryption SDK mit verwenden AWS KMS.

  Den Leitfaden erkunden

- Bewährte Methoden für AWS Encryption SDK

  Auf der Seite mit den AWS Encryption SDK bewährten Methoden finden Sie Anleitungen zur effektiven Nutzung der AWS Encryption SDK zur Sicherung Ihrer Daten. Die Einhaltung dieser bewährten Methoden trägt dazu bei, die Vertraulichkeit und Integrität Ihrer verschlüsselten Daten zu gewährleisten.

  Den Leitfaden erkunden

- AWS Encryption SDK Häufig gestellte Fragen

  Auf der AWS Encryption SDK FAQ-Seite finden Sie Antworten auf häufig gestellte Fragen zu den AWS Encryption SDK Funktionen, unterstützten Programmiersprachen und bewährten Methoden für die Implementierung.

  Erkunden Sie die häufig gestellten Fragen

AWS Database Encryption SDK

- Beginnen Sie mit dem AWS Database Encryption SDK

  Erfahren Sie, wie Sie das AWS Database Encryption SDK mit verwenden AWS KMS.

  Den Leitfaden erkunden

- Konfigurieren Sie das AWS Database Encryption SDK

  Erfahren Sie, wie Sie das AWS Database Encryption SDK konfigurieren, einschließlich der Auswahl einer Programmiersprache und der Auswahl von Wrapping-Schlüsseln.

  Den Leitfaden erkunden

AWS KMS

- Fangen Sie an mit AWS KMS

  Erfahren Sie, wie Sie KMS-Schlüssel erstellen, einschließlich symmetrischer und asymmetrischer Verschlüsselungsschlüssel.

  Den Leitfaden erkunden
- Bewährte Methoden für AWS KMS

  Erfahren Sie mehr über bewährte Verschlüsselungsmethoden für AWS KMS.

  Den Leitfaden erkunden
- AWS KMS Preisgestaltung

  Auf der Preisseite AWS Key Management Service (KMS) finden Sie Informationen zu den mit der Nutzung verbundenen Kosten AWS KMS, einschließlich Gebühren für Schlüsselspeicher, API-Anfragen und optionale Funktionen wie benutzerdefinierte Schlüsselspeicher.

  Erkunden Sie die Seite mit den Preisen
- AWS KMS Häufig gestellte Fragen

  Auf der Seite mit häufig gestellten Fragen AWS Key Management Service (KMS) finden Sie ausführliche Antworten auf häufig gestellte Fragen AWS KMS zu Funktionen, Sicherheitsmaßnahmen, Abrechnungspraktiken, wichtigen Verwaltungsoptionen und Integration mit anderen AWS-Services.

  Erkunden Sie die FAQs

AWS Private CA

- Bewährte Methoden für AWS Private CA

  Lesen Sie sich die Empfehlungen durch, die Ihnen bei der AWS Private CA effektiven Nutzung helfen können.

  Den Leitfaden erkunden
- Fangen Sie an mit AWS Private CA

  Erfahren Sie, wie Sie eine Root-CA programmgesteuert erstellen und aktivieren.

Den Leitfaden erkunden

- AWS Private CA Preisgestaltung

  Überprüfen Sie die Kosten, die mit dem Betrieb von privaten Zertifikaten CAs und der Ausstellung von privaten Zertifikaten verbunden sind.

  Erkunden Sie die Seite mit den Preisen

- AWS Private CA Häufig gestellte Fragen

  Hier erhalten Sie ausführliche Antworten auf häufig gestellte Fragen AWS Private CA zu Funktionen, Preisen, Bereitstellung, Sicherheit, Compliance, Leistung und Integration mit anderen AWS-Services.

  Erkunden Sie die FAQs

AWS Secrets Manager

- Fangen Sie an mit AWS Secrets Manager

  Erfahre, wie du ein AWS Secrets Manager Geheimnis erstellst.

  Den Leitfaden erkunden

- Bewährte Methoden für AWS Secrets Manager

  Erfahren Sie mehr über bewährte Verfahren, die Sie bei der Verwendung berücksichtigen sollten AWS Secrets Manager.

  Den Leitfaden erkunden

- AWS Secrets Manager Preisgestaltung

  Auf der AWS Secrets Manager Preisseite finden Sie Informationen zu den Kosten, die mit dem sicheren Speichern, Verwalten und Abrufen von Geheimnissen wie Datenbankanmeldeinformationen und API-Schlüsseln verbunden sind.

  Erkunden Sie die Seite mit den Preisen

- AWS Secrets Manager Häufig gestellte Fragen

Auf der AWS Secrets Manager FAQ-Seite finden Sie ausführliche Antworten auf häufig gestellte Fragen AWS Secrets Manager zu Funktionen, Sicherheitsmaßnahmen, Preisen und Integrationsmöglichkeiten.

Erkunden Sie die FAQs

Erkunde

- Forschung und Ressourcen

  Entdecken Sie AWS Blogs, Videos und Tools zur Kryptografie.

  Ressourcen überprüfen
- Videos

  Sehen Sie sich diese Videos aus dem AWS Entwicklerkanal an YouTube , um Ihre Kryptografiestrategie weiterzuentwickeln und zu verfeinern.

  Entdecken Sie Videos zur Kryptografie

Dokumentverlauf

In der folgenden Tabelle werden die wichtigen Änderungen an diesem Entscheidungsleitfaden beschrieben. Für Benachrichtigungen über Aktualisierungen dieses Handbuchs können Sie einen RSS-Feed abonnieren.

Änderung	Beschreibung	Datum
Erste Veröffentlichung	Der Leitfaden wurde zuerst veröffentlicht.	31. Januar 2025

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.