Empfohlene Sicherheitskontrollen für die Implementierung von AWS CAF-Sicherheitsfunktionen

AWS Präskriptive Leitlinien

AWS Präskriptive Leitlinien: Empfohlene Sicherheitskontrollen für die Implementierung von AWS CAF-Sicherheitsfunktionen

Table of Contents

Einführung 1
Identitäts- und Zugriffskontrollen 3
Root-Benutzeraktivität 3
Zugriffsschlüssel für den Root-Benutzer 4
MFA für den Root-Benutzer 4
IAM Best Practices 5
Das geringste Privileg 6
Leitplanken auf Workload-Ebene 6
IAM-Zugriffsschlüssel rotieren 7
Extern gemeinsam genutzte Ressourcen 8
Kontrollen für Protokollierung und Überwachung 9
CloudTrail Wanderweg mit mehreren Regionen 9
Dienst- und Anwendungsprotokollierung 10
Zentralisierte Protokollierung 11
Zugriff auf CloudTrail Protokolldateien 11
Benachrichtigungen für Sicherheitsgruppen oder Änderungen der Netzwerk-ACL 12
Benachrichtigungen für CloudWatch Alarme 12
Kontrollen der Infrastruktur 14
CloudFront Standard-Stammobjekte 14
Anwendungscode scannen 15
Erstellen Sie Netzwerkschichten 15
Verwenden Sie nur autorisierte Ports 16
Öffentlicher Zugriff auf Systems Manager Manager-Dokumente 16
Öffentlicher Zugriff auf Lambda-Funktionen 17
Aktualisieren Sie die Standardsicherheitsgruppe 17
Suchen Sie nach Sicherheitslücken und Netzwerkgefährdungen 18
Einrichten AWS WAF 19
Erweiterter Schutz vor S-Angriffen DDo 20
Kontrollieren des Netzwerkverkehrs 20
Datenkontrollen 22
Klassifizieren Sie Daten auf Workload-Ebene 22
Richten Sie Kontrollen für jede Datenklassifizierungsebene ein 23
Daten im Ruhezustand verschlüsseln 24
Verschlüsseln Sie Daten während der Übertragung 25

Öffentlicher Zugriff auf Amazon EBS-Snapshots 25
Öffentlicher Zugriff auf Amazon RDS-Snapshots 26
Öffentlicher Zugriff auf Amazon RDS, Amazon Redshift und Ressourcen AWS DMS 26
Öffentlicher Zugriff auf S3-Buckets 27
MFA zum Löschen von S3-Bucket-Daten erforderlich 28
OpenSearch Servicedomänen in VPCs 28
Benachrichtigungen für das Löschen von KMS-Schlüsseln 29
Öffentlicher Zugriff auf KMS-Schlüssel 29
Listener verwenden sichere Protokolle 30
Empfehlungen zur Reaktion auf Vorfälle 32
Plan zur Reaktion auf Vorfälle 32
Runbooks und Playbooks 33
Ereignisgesteuerte Automatisierung 33
Support Prozess 34
Benachrichtigungen für Sicherheitsereignisse 35
Nächste Schritte 36
Dokumentverlauf 37
Glossar 38
..... 38
A 39
B 42
C 44
D 48
E 52
F 54
G 56
H 57
I 59
L 62
M 63
O 67
P 70
Q 73
R 74
S 77
T 81

U 83
V 83
W 84
Z 85
..... lxxxvi

Empfohlene Sicherheitskontrollen für die Implementierung AWS von CAF-Sicherheitsfunktionen

Rishi Singla und Rovan Omar, Amazon Web Services ()AWS

November 2023 (Dokumentverlauf)

Sicherheit hat bei oberste Priorität. AWS Um Ihren Betrieb zu entlasten, tragen Sie gemeinsam die Verantwortung für Cloud-Sicherheit und Compliance AWS. AWS ist verantwortlich für die Sicherheit der Cloud, d. h. für den Schutz der Infrastruktur, auf der die in der Cloud angebotenen Dienste ausgeführt werden AWS Cloud. Sie sind verantwortlich für die Sicherheit in der Cloud, z. B. für Ihre Daten und Anwendungen. Dieser Leitfaden enthält Sicherheitskontrollen, die Ihnen helfen können, Ihren Sicherheitsaufgaben in der nachzukommen AWS Cloud.

Das AWS Cloud Adoption Framework (AWS CAF) bietet bewährte Methoden, mit denen Sie Ihre Cloud-Bereitschaft verbessern können. AWS CAF unterteilt diese Best Practices in sechs Perspektiven: Unternehmen, Mitarbeiter, Unternehmensführung, Plattform, Sicherheit und Betrieb. Dieser Leitfaden konzentriert sich auf die folgenden Funktionen aus Sicht der Sicherheit:

- Identitäts- und Zugriffsmanagement — Verwalten Sie die Identitäten von Menschen und Maschinen und deren Berechtigungen in großem Umfang.
- Bedrohungserkennung — Konfigurieren Sie Protokollierung und Überwachung, um potenzielle Sicherheitsfehler, Bedrohungen oder unerwartetes Verhalten zu erkennen und zu untersuchen.
- Schutz der Infrastruktur — Schützen Sie Systeme und Dienste vor unbeabsichtigtem oder unbefugtem Zugriff und potenziellen Sicherheitslücken.
- Schutz von Daten — Kategorisieren Sie Daten nach Vertraulichkeitsstufen. Sorgen Sie für Transparenz und Kontrolle über Daten und darüber, wie sie in Ihrem Unternehmen abgerufen und verwendet werden.
- Reaktion auf Vorfälle — Richten Sie Mechanismen ein, um auf Sicherheitsvorfälle zu reagieren und ihre potenziellen Auswirkungen zu mindern.

Das Versäumnis, präventive, detektive und reaktionsschnelle Sicherheitskontrollen für diese AWS CAF-Sicherheitsfunktionen zu implementieren, kann ein kritisches Risiko für Ihre Cloud-Umgebung darstellen und Ihren Geschäftsbetrieb unterbrechen. Die Implementierung der Sicherheitskontrollen in diesem Leitfaden kann Ihrem Unternehmen helfen, seine Cloud-Umgebung zu schützen.

> **Note**
>
> AWS bietet Dienste, Tools und Frameworks, die Ihnen helfen können, sicher in der zu arbeiten AWS Cloud. Dieser Leitfaden entspricht dem AWS Well-Architected Framework, dem AWS Cloud Adoption Framework (AWS CAF), der AWS Security Reference Architecture (AWS SRA) und anderen Sicherheitsempfehlungen, die von veröffentlicht wurden, und ergänzt diese. AWS Die Kontrollen in diesem Leitfaden umfassen nicht alle Überlegungen zur Cloud-Sicherheit, und dieser Leitfaden soll diese Frameworks nicht ersetzen.

Empfehlungen zur Sicherheitskontrolle für die Identitäts- und Zugriffsverwaltung

Sie können Identitäten in AWS einer externen Identitätsquelle erstellen oder eine Verbindung herstellen. Mithilfe von AWS Identity and Access Management (IAM-) Richtlinien gewähren Sie Benutzern die erforderlichen Berechtigungen, damit sie auf AWS Ressourcen und integrierte Anwendungen zugreifen oder diese verwalten können. Ein effektives Identitäts- und Zugriffsmanagement hilft zu überprüfen, ob die richtigen Personen und Maschinen unter den richtigen Bedingungen Zugriff auf die richtigen Ressourcen haben. Das AWS Well-Architected Framework bietet bewährte Methoden für die Verwaltung von Identitäten und deren Berechtigungen. Beispiele für bewährte Verfahren sind die Verwendung eines zentralen Identitätsanbieters und die Verwendung starker Anmeldemechanismen wie Multi-Faktor-Authentifizierung (MFA). Die Sicherheitskontrollen in diesem Abschnitt können Ihnen bei der Implementierung dieser bewährten Methoden helfen.

Steuerelemente in diesem Abschnitt:

- Überwachen und konfigurieren Sie Benachrichtigungen für Root-Benutzeraktivitäten
- Keine Zugriffsschlüssel für den Root-Benutzer erstellen
- MFA für den Root-Benutzer aktivieren
- Folgen Sie den bewährten Sicherheitsmethoden für IAM
- Gewähren Sie Berechtigungen mit den geringsten Rechten
- Definieren Sie Richtlinien für Berechtigungen auf Workload-Ebene
- Wechseln Sie die IAM-Zugriffsschlüssel in regelmäßigen Abständen
- Identifizieren Sie Ressourcen, die mit einer externen Entität gemeinsam genutzt werden

Überwachen und konfigurieren Sie Benachrichtigungen für Root-Benutzeraktivitäten

Wenn Sie zum ersten Mal eine erstellen AWS-Konto, beginnen Sie mit einer einzigen Anmeldeidentität, dem so genannten Root-Benutzer. Standardmäßig hat der Root-Benutzer vollen Zugriff auf alle AWS-Services Ressourcen im Konto. Sie sollten den Root-Benutzer genau kontrollieren und überwachen und ihn nur für Aufgaben verwenden, für die Root-Benutzeranmeldedaten erforderlich sind.

Weitere Informationen finden Sie in den folgenden Ressourcen:

- Gewähren Sie den Zugriff mit den geringsten Rechten im Well-Architected Framework AWS
- Überwachen Sie die IAM-Root-Benutzeraktivitäten in Prescriptive Guidance AWS

Keine Zugriffsschlüssel für den Root-Benutzer erstellen

Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. Die Deaktivierung des programmatischen Zugriffs auf den Root-Benutzer trägt dazu bei, das Risiko einer versehentlichen Offenlegung der Benutzeranmeldeinformationen und der damit verbundenen Beeinträchtigung der Cloud-Umgebung zu verringern. Wir empfehlen Ihnen, IAM-Rollen als temporäre Anmeldeinformationen für den Zugriff auf Ihre Ressourcen zu erstellen und zu verwenden. AWS-Konten

Weitere Informationen finden Sie in den folgenden Ressourcen:

- Der IAM-Root-Benutzerzugriffsschlüssel sollte in der Dokumentation nicht enthalten sein AWS Security Hub CSPM
- Löschen der Zugriffsschlüssel für den Root-Benutzer in der IAM-Dokumentation
- IAM-Rollen in der IAM-Dokumentation

MFA für den Root-Benutzer aktivieren

Wir empfehlen, mehrere Geräte mit Multi-Faktor-Authentifizierung (MFA) für AWS-Konto Root-Benutzer und IAM-Benutzer zu aktivieren. Dies erhöht die Sicherheitslatte AWS-Konten und kann die Zugriffsverwaltung vereinfachen. Da es sich bei einem Root-Benutzer um einen Benutzer mit hohen Rechten handelt, der privilegierte Aktionen ausführen kann, ist es wichtig, MFA für den Root-Benutzer vorzuschreiben. Sie können ein Hardware-MFA-Gerät verwenden, das einen numerischen Code auf der Grundlage des Time-Based One-Time Password (TOTP) -Algorithmus, eines FIDO-Hardwaresicherheitsschlüssels oder einer virtuellen Authentifikatoranwendung generiert.

Im Jahr 2024 wird MFA erforderlich sein, um auf den Root-Benutzer eines beliebigen AWS-Konto Benutzers zuzugreifen. Weitere Informationen finden Sie im AWS Sicherheitsblog unter Secure by Design: AWS zur Verbesserung der MFA-Anforderungen im Jahr 2024. Wir empfehlen Ihnen dringend, diese Sicherheitspraxis auszuweiten und MFA für alle Benutzertypen in Ihren AWS Umgebungen vorzuschreiben.

Wenn möglich, empfehlen wir, ein Hardware-MFA-Gerät für den Root-Benutzer zu verwenden. Eine virtuelle MFA bietet möglicherweise nicht das gleiche Sicherheitsniveau wie ein Hardware-MFA-Gerät. Sie können Virtual MFA verwenden, während Sie auf die Genehmigung oder Lieferung des Hardwarekaufs warten.

In Situationen, in denen Sie Hunderte von Konten verwalten AWS Organizations, ist es je nach Risikobereitschaft Ihres Unternehmens möglicherweise nicht skalierbar, hardwarebasiertes MFA für den Root-Benutzer jedes Kontos in einer Organisationseinheit (OU) zu verwenden. In diesem Fall können Sie ein Konto in der Organisationseinheit auswählen, das als Verwaltungskonto für die Organisationseinheit fungiert, und dann den Root-Benutzer für die anderen Konten in dieser Organisationseinheit deaktivieren. Standardmäßig hat das OU-Verwaltungskonto keinen Zugriff auf die anderen Konten. Wenn Sie den kontenübergreifenden Zugriff im Voraus einrichten, können Sie im Notfall vom OU-Verwaltungskonto aus auf die anderen Konten zugreifen. Um den kontenübergreifenden Zugriff einzurichten, erstellen Sie eine IAM-Rolle im Mitgliedskonto und definieren Richtlinien, sodass nur der Root-Benutzer im OU-Verwaltungskonto diese Rolle übernehmen kann. Weitere Informationen finden Sie in der IAM-Dokumentation unter Tutorial: Delegieren des Zugriffs AWS-Konten mithilfe von IAM-Rollen.

Wir empfehlen, dass Sie mehrere MFA-Geräte für Ihre Root-Benutzeranmeldedaten aktivieren. Sie können bis zu acht MFA-Geräte beliebiger Kombination registrieren.

Weitere Informationen finden Sie in den folgenden Ressourcen:

- Aktivierung eines Hardware-TOTP-Tokens in der IAM-Dokumentation
- Aktivierung eines Geräts mit virtueller Multifaktor-Authentifizierung (MFA) in der IAM-Dokumentation
- Aktivierung eines FIDO-Sicherheitsschlüssels in der IAM-Dokumentation
- Schützen Sie Ihre Root-Benutzeranmeldung mit Multi-Faktor-Authentifizierung (MFA) in der IAM-Dokumentation

Folgen Sie den bewährten Sicherheitsmethoden für IAM

Die IAM-Dokumentation enthält eine Liste mit bewährten Methoden, die Ihnen helfen sollen, Ihre AWS-Konten Ressourcen zu schützen. Sie enthält Empfehlungen für die Konfiguration von Zugriff und Berechtigungen nach dem Prinzip der geringsten Rechte. Zu den bewährten Methoden für die IAM-Sicherheit gehören beispielsweise die Konfiguration eines Identitätsverbunds, die Anforderung von MFA und die Verwendung temporärer Anmeldeinformationen.

Weitere Informationen finden Sie in den folgenden Ressourcen:

- Bewährte Sicherheitsmethoden in IAM finden Sie in der IAM-Dokumentation
- Verwendung temporärer Anmeldeinformationen mit AWS Ressourcen in der IAM-Dokumentation

Gewähren Sie Berechtigungen mit den geringsten Rechten

Bei den geringsten Rechten werden nur die Berechtigungen erteilt, die zur Ausführung einer Aufgabe erforderlich sind. Dazu definieren Sie die Aktionen, die für bestimmte Ressourcen unter bestimmten Bedingungen ausgeführt werden können.

Die attributebasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen auf der Grundlage von Attributen, wie z. B. ihren Tags, definiert werden. Sie können Gruppen-, Identitäts- und Ressourcenattribute verwenden, um Berechtigungen dynamisch und skalierbar zu definieren, anstatt Berechtigungen für einzelne Benutzer zu definieren. Sie können ABAC beispielsweise verwenden, um einer Gruppe von Entwicklern den Zugriff nur auf Ressourcen zu ermöglichen, denen ein bestimmtes Tag mit ihrem Projekt verknüpft ist.

Weitere Informationen finden Sie in den folgenden Ressourcen:

- Wenden Sie in der IAM-Dokumentation Berechtigungen mit den geringsten Rechten an
- Wozu dient ABAC in der IAM-Dokumentation AWS

Definieren Sie Richtlinien für Berechtigungen auf Workload-Ebene

Es hat sich bewährt, eine Strategie für mehrere Konten zu verwenden, da sie Flexibilität bei der Definition von Leitplanken auf Workload-Ebene bietet. Die AWS Security Reference Architecture bietet verbindliche Anleitungen zur Strukturierung Ihrer Konten. Diese Konten werden als Organisation in verwaltet AWS Organizations, und die Konten sind in Organisationseinheiten gruppiert () OUs.

AWS-Services, kann Ihnen beispielsweise dabei helfen AWS Control Tower, die Kontrollen innerhalb einer Organisation zentral zu verwalten. Wir empfehlen Ihnen, für jedes Konto oder jede Organisationseinheit innerhalb der Organisation einen klaren Zweck zu definieren und die Kontrollen entsprechend diesem Zweck anzuwenden. AWS Control Tower implementiert präventive, detektive und proaktive Kontrollen, die Ihnen helfen, die Ressourcen zu verwalten und die Einhaltung der

Vorschriften zu überwachen. Eine präventive Kontrolle soll verhindern, dass ein Ereignis eintritt. Eine detektive Kontrolle ist darauf ausgelegt, ein Ereignis zu erkennen, zu protokollieren und zu warnen, nachdem ein Ereignis eingetreten ist. Eine proaktive Kontrolle soll den Einsatz nicht richtlinienkonformer Ressourcen verhindern, indem Ressourcen gescannt werden, bevor sie bereitgestellt werden.

Weitere Informationen finden Sie in den folgenden Ressourcen:

- Separate Workloads mithilfe von Konten im AWS Well-Architected Framework
- AWS Sicherheitsreferenzarchitektur (AWS SRA) in präskriptiven Leitlinien AWS
- Informationen zu den Kontrollen finden Sie in der Dokumentation AWS Control Tower AWS Control Tower
- Die Implementierung von Sicherheitskontrollen ist AWS in den AWS vorgeschriebenen Leitlinien enthalten
- Verwenden Sie im Sicherheitsblog Richtlinien zur Servicekontrolle, um Zugangsberechtigungen für alle Konten in Ihrem AWS Unternehmen festzulegen AWS

Wechseln Sie die IAM-Zugriffsschlüssel in regelmäßigen Abständen

Es hat sich bewährt, die Zugriffsschlüssel für Anwendungsfälle zu aktualisieren, für die langfristige Anmeldeinformationen erforderlich sind. Wir empfehlen, die Zugangsschlüssel alle 90 Tage oder weniger zu wechseln. Durch die Rotation der Zugangsschlüssel wird das Risiko verringert, dass ein Zugriffsschlüssel verwendet wird, der mit einem kompromittierten oder gekündigten Konto verknüpft ist. Außerdem wird der Zugriff durch die Verwendung eines alten Schlüssels verhindert, der möglicherweise verloren gegangen, kompromittiert oder gestohlen wurde. Aktualisieren Sie Anwendungen immer, nachdem Sie die Zugriffstasten gedreht haben.

Weitere Informationen finden Sie in den folgenden Ressourcen:

- Aktualisieren Sie die Zugriffsschlüssel bei Bedarf für Anwendungsfälle, für die langfristige Anmeldeinformationen erforderlich sind, in der IAM-Dokumentation
- Wechseln Sie die IAM-Benutzerzugriffsschlüssel automatisch nach Bedarf mit AWS Organizations und AWS Secrets Manager in AWS Prescriptive Guidance
- Aktualisierung der Zugriffsschlüssel in der IAM-Dokumentation

Identifizieren Sie Ressourcen, die mit einer externen Entität gemeinsam genutzt werden

Eine externe Entität ist eine Ressource, eine Anwendung, ein Dienst oder ein Benutzer außerhalb Ihrer AWS Organisation, z. B. ein anderer, ein Root-Benutzer AWS-Konten, ein IAM-Benutzer oder eine IAM-Rolle, ein Verbundbenutzer, ein oder ein AWS-Service anonymer (oder nicht authentifizierter) Benutzer. Es ist eine bewährte Sicherheitsmethode, IAM Access Analyzer zu verwenden, um die Ressourcen in Ihrer Organisation und in Ihren Konten zu identifizieren, wie z. B. Amazon Simple Storage Service (Amazon S3) -Buckets oder IAM-Rollen, die mit einer externen Entität gemeinsam genutzt werden. Auf diese Weise können Sie den unbeabsichtigten Zugriff auf Ressourcen und Daten identifizieren, der ein Sicherheitsrisiko darstellt.

Weitere Informationen finden Sie in den folgenden Ressourcen:

- Überprüfen Sie den öffentlichen und kontoübergreifenden Zugriff auf Ressourcen mit IAM Access Analyzer in der IAM-Dokumentation
- Analysieren Sie den öffentlichen und kontoübergreifenden Zugriff im AWS Well-Architected Framework
- Verwendung AWS Identity and Access Management Access Analyzer in der IAM-Dokumentation

Empfehlungen zur Sicherheitskontrolle für die Protokollierung und Überwachung

Protokollierung und Überwachung sind wichtige Aspekte der Bedrohungserkennung. Die Erkennung von Bedrohungen ist eine der sicherheitstechnischen Funktionen des AWS Cloud Adoption Framework (AWS CAF). Mithilfe von Protokolldaten kann Ihr Unternehmen Ihre Umgebung überwachen, um potenzielle Sicherheitsfehlkonfigurationen, Bedrohungen und unerwartetes Verhalten zu verstehen und zu identifizieren. Das Verständnis potenzieller Bedrohungen kann Ihrem Unternehmen dabei helfen, Sicherheitskontrollen zu priorisieren, und eine effektive Bedrohungserkennung kann Ihnen helfen, schneller auf Bedrohungen zu reagieren.

Kontrollen in diesem Abschnitt:

- Konfigurieren Sie mindestens einen Trail mit mehreren Regionen in CloudTrail
- Konfigurieren Sie die Protokollierung auf Dienst- und Anwendungsebene
- Richten Sie einen zentralen Ort für die Analyse von Protokollen und die Reaktion auf Sicherheitsereignisse ein
- Verhindern Sie unbefugten Zugriff auf S3-Buckets, die CloudTrail Protokolldateien enthalten
- Konfigurieren Sie Warnmeldungen für Änderungen an Sicherheitsgruppen oder im Netzwerk ACLs
- Konfigurieren Sie Alarme für CloudWatch Alarme, die in den ALARM-Status wechseln

Konfigurieren Sie mindestens einen Trail mit mehreren Regionen in CloudTrail

AWS CloudTrailhilft Ihnen bei der Prüfung der Unternehmensführung, der Einhaltung von Vorschriften und der betrieblichen Risiken Ihres AWS-Konto. Von einem Benutzer, einer Rolle oder einem ausgeführte Aktionen AWS-Service werden als Ereignisse in aufgezeichnet CloudTrail. Zu den Ereignissen gehören Aktionen AWS-Managementkonsole, die in den Bereichen, AWS Command Line Interface (AWS CLI) und AWS SDKs und ausgeführt wurden APIs. Dieser Ereignisverlauf hilft Ihnen dabei, Ihren Sicherheitsstatus zu analysieren, Ressourcenänderungen nachzuverfolgen und die Einhaltung von Vorschriften zu überprüfen.

Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS-Konto System müssen Sie einen Trail erstellen. Jeder Trail sollte so konfiguriert sein, dass alle Ereignisse protokolliert werden AWS-

Regionen. Indem Sie alle Ereignisse protokollieren AWS-Regionen, stellen Sie sicher, dass alle Ereignisse, die in Ihrem Bereich auftreten, protokolliert AWS-Konto werden, unabhängig davon, in welchem AWS-Region Bereich sie aufgetreten sind. Ein regionsübergreifender Trail stellt sicher, dass globale Serviceereignisse protokolliert werden.

Weitere Informationen finden Sie in den folgenden Ressourcen:

- CloudTrail In der Dokumentation finden Sie bewährte Sicherheitsmethoden CloudTrail
- Umwandlung eines Pfads, der für eine Region gilt, so dass er für alle Regionen in der CloudTrail Dokumentation gilt
- Aktivierung und Deaktivierung der globalen Protokollierung von Serviceereignissen in der Dokumentation CloudTrail

Konfigurieren Sie die Protokollierung auf Dienst- und Anwendungsebene

Das AWS Well-Architected Framework empfiehlt, Sicherheitsereignisprotokolle von Diensten und Anwendungen aufzubewahren. Dies ist ein grundlegendes Sicherheitsprinzip für Prüfungen, Untersuchungen und betriebliche Anwendungsfälle. Die Aufbewahrung von Service- und Anwendungsprotokollen ist eine allgemeine Sicherheitsanforderung, die sich nach den Standards, Richtlinien und Verfahren für Governance, Risiko und Compliance (GRC) richtet.

Sicherheitsteams verlassen sich auf Protokolle und Suchtools, um potenzielle interessante Ereignisse zu entdecken, die auf unbefugte Aktivitäten oder unbeabsichtigte Änderungen hinweisen könnten. Sie können die Protokollierung je nach Anwendungsfall für verschiedene Dienste aktivieren. Sie können beispielsweise den Amazon S3 S3-Bucket-Zugriff, AWS WAF Web-ACL-Verkehr, Amazon API Gateway Gateway-Verkehr auf Netzwerkebene oder CloudFront Amazon-Verteilungen protokollieren.

Weitere Informationen finden Sie in den folgenden Ressourcen:

- Streamen Sie Amazon CloudWatch Logs zur Prüfung und Analyse auf ein zentrales Konto im AWS Architektur-Blog
- Konfigurieren Sie die Dienst- und Anwendungsprotokollierung im AWS Well-Architected Framework

Richten Sie einen zentralen Ort für die Analyse von Protokollen und die Reaktion auf Sicherheitsereignisse ein

Die manuelle Analyse von Protokollen und die Verarbeitung von Informationen reichen nicht aus, um mit der Menge an Informationen Schritt zu halten, die mit komplexen Architekturen einhergeht. Analyse und Berichterstattung allein ermöglichen es nicht, Ereignisse rechtzeitig der richtigen Ressource zuzuweisen. Das AWS Well-Architected Framework empfiehlt, dass Sie AWS Sicherheitsereignisse und -ergebnisse in ein Benachrichtigungs- und Workflowsystem integrieren, z. B. in ein Ticket-, Bug- oder SIEM-System (Security Information and Event Management). Diese Systeme unterstützen Sie bei der Zuweisung, Weiterleitung und Verwaltung von Sicherheitsereignissen.

Weitere Informationen finden Sie in den folgenden Ressourcen:

- Analysieren Sie Protokolle, Ergebnisse und Metriken zentral im AWS Well-Architected Framework
- Analysieren Sie Sicherheit, Compliance und betriebliche Aktivitäten mithilfe von CloudTrail Amazon Athena im AWS Sicherheits-Blog
- AWS Partner, die im AWS Partnerportfolio Dienste zur Erkennung und Abwehr von Bedrohungen anbieten

Verhindern Sie unbefugten Zugriff auf S3-Buckets, die CloudTrail Protokolldateien enthalten

Standardmäßig werden CloudTrail Protokolldateien in Amazon S3 S3-Buckets gespeichert. Es ist eine bewährte Sicherheitsmethode, um unbefugten Zugriff auf Amazon S3 S3-Buckets zu verhindern, die CloudTrail Protokolldateien enthalten. Auf diese Weise können Sie die Integrität, Vollständigkeit und Verfügbarkeit dieser Protokolle aufrechterhalten, was für forensische Zwecke und Prüfzwecke von entscheidender Bedeutung ist. Wenn Sie Datenereignisse für S3-Buckets protokollieren möchten, die CloudTrail Protokolldateien enthalten, können Sie zu diesem Zweck einen CloudTrail Trail erstellen.

Weitere Informationen finden Sie in den folgenden Ressourcen:

- Konfiguration der Einstellungen zum Blockieren des öffentlichen Zugriffs für Ihre S3-Buckets in der Amazon S3 S3-Dokumentation
- CloudTrail Bewährte Methoden zur präventiven Sicherheit in der Dokumentation CloudTrail

- Erstellung einer Spur in der Dokumentation CloudTrail

Konfigurieren Sie Warnmeldungen für Änderungen an Sicherheitsgruppen oder im Netzwerk ACLs

Eine Sicherheitsgruppe in Amazon Virtual Private Cloud (Amazon VPC) kontrolliert den Datenverkehr, der die Ressourcen erreichen und verlassen darf, mit denen er verknüpft ist. Eine Network Access Control List (ACL) erlaubt oder verweigert bestimmten eingehenden oder ausgehenden Verkehr auf der Subnetzebene der VPC. Diese Ressourcen sind für die Verwaltung des Zugriffs in Ihrer Umgebung von entscheidender Bedeutung. AWS

Erstellen und konfigurieren Sie einen CloudWatch Amazon-Alarm, der Sie benachrichtigt, wenn sich die Konfiguration einer Sicherheitsgruppe oder Netzwerk-ACL ändert. Konfigurieren Sie diesen Alarm so, dass Sie jedes Mal benachrichtigt werden, wenn ein AWS API-Aufruf zur Aktualisierung von Sicherheitsgruppen ausgeführt wird. Sie können auch Dienste wie Amazon EventBridge und verwenden AWS Config, um automatisch auf diese Art von Sicherheitsereignissen zu reagieren.

Weitere Informationen finden Sie in den folgenden Ressourcen:

- Automatisches Zurücksetzen und Erhalten von Benachrichtigungen über Änderungen an Ihren Amazon VPC-Sicherheitsgruppen im AWS Sicherheits-Blog
- Verwendung von CloudWatch Amazon-Alarmen in der CloudWatch Dokumentation
- Implementieren Sie umsetzbare Sicherheitsereignisse im AWS Well-Architected Framework
- Automatisieren Sie die Reaktion auf Ereignisse im AWS Well-Architected Framework

Konfigurieren Sie Alarme für CloudWatch Alarme, die in den ALARM-Status wechseln

In können Sie angeben CloudWatch, welche Aktionen ein Alarm ausführt, wenn er seinen Status zwischen den `INSUFFICIENT_DATA` Zuständen `OKALARM`, und ändert. Die häufigste Art von Alarmaktion besteht darin, eine oder mehrere Personen zu benachrichtigen, indem eine Nachricht an ein Amazon Simple Notification Service (Amazon SNS) -Thema gesendet wird. Sie können auch Alarme konfigurieren, die ausgelöst werden sollen OpsItemsoder in AWS Systems Manager denen Vorfälle auftreten.

Wir empfehlen Ihnen, Alarmaktionen zu aktivieren, um automatisch zu warnen, wenn eine überwachte Metrik den definierten Schwellenwert überschreitet. Durch die Überwachung von Alarmen können Sie ungewöhnliche Aktivitäten erkennen und schnell auf Sicherheits- und Betriebsprobleme reagieren.

Weitere Informationen finden Sie in den folgenden Ressourcen:

- Implementieren Sie umsetzbare Sicherheitsereignisse im AWS Well-Architected Framework
- Alarmaktionen in der Dokumentation CloudWatch

Empfehlungen zur Sicherheitskontrolle zum Schutz der Infrastruktur

Der Schutz der Infrastruktur ist ein wichtiger Bestandteil jedes Sicherheitsprogramms. Es umfasst Kontrollmethoden, mit denen Sie Ihre Netzwerke und Rechenressourcen schützen können. Beispiele für Infrastrukturschutz sind Vertrauensgrenzen, ein defense-in-depth Ansatz, Sicherheitsverstärkung, Patch-Management sowie Betriebssystemauthentifizierung und -autorisierung. Weitere Informationen finden Sie unter Infrastrukturschutz im AWS Well-Architected Framework. Die Sicherheitskontrollen in diesem Abschnitt können Ihnen bei der Implementierung von Best Practices für den Infrastrukturschutz helfen.

Steuerelemente in diesem Abschnitt:

- Geben Sie Standard-Stammobjekte für CloudFront Distributionen an
- Scannen Sie den Anwendungscode, um häufig auftretende Sicherheitsprobleme zu identifizieren
- Erstellen Sie Netzwerkschichten mithilfe von dedizierten VPCs Netzen und Subnetzen
- Beschränken Sie den eingehenden Datenverkehr auf nur autorisierte Ports
- Sperren Sie den öffentlichen Zugriff auf Systems Manager Manager-Dokumente
- Blockieren Sie den öffentlichen Zugriff auf Lambda-Funktionen
- Beschränken Sie eingehenden und ausgehenden Datenverkehr in der Standardsicherheitsgruppe
- Suchen Sie nach Software-Sicherheitslücken und unbeabsichtigter Netzwerkgefährdung
- Einrichten AWS WAF
- Konfigurieren Sie erweiterte Schutzmaßnahmen gegen S-Angriffe DDo
- Verwenden Sie einen defense-in-depth Ansatz zur Steuerung des Netzwerkverkehrs

Geben Sie Standard-Stammobjekte für CloudFront Distributionen an

Amazon CloudFront beschleunigt die Verteilung Ihrer Webinhalte, indem es sie über ein weltweites Netzwerk von Rechenzentren bereitstellt, was die Latenz senkt und die Leistung verbessert. Wenn Sie kein Standardstammobjekt definieren, werden Anfragen für den Stamm Ihrer Verteilung an Ihren Ursprungs-Server weitergeleitet. Wenn Sie einen Amazon Simple Storage Service (Amazon S3) -

Ursprung verwenden, gibt die Anfrage möglicherweise eine Liste der Inhalte in Ihrem S3-Bucket oder eine Liste der privaten Inhalte Ihres Ursprungs zurück. Durch die Angabe eines Standard-Root-Objekts können Sie vermeiden, dass der Inhalt Ihrer Distribution offengelegt wird.

Weitere Informationen finden Sie in den folgenden Ressourcen:

- Die Angabe eines Standard-Stammobjekts in der Dokumentation CloudFront

Scannen Sie den Anwendungscode, um häufig auftretende Sicherheitsprobleme zu identifizieren

Das AWS Well-Architected Framework empfiehlt, Bibliotheken und Abhängigkeiten auf Probleme und Fehler zu überprüfen. Es gibt viele Tools zur Quellcode-Analyse, mit denen Sie Quellcode scannen können. Amazon CodeGuru kann beispielsweise in Java unseren Python Anwendungen nach häufigen Sicherheitsproblemen suchen und Empfehlungen zur Behebung geben.

Weitere Informationen finden Sie in den folgenden Ressourcen:

- CodeGuru Dokumentation
- Tools zur Quellcode-Analyse auf der OWASP Foundation Website
- Führen Sie das Schwachstellenmanagement im AWS Well-Architected Framework durch

Erstellen Sie Netzwerkschichten mithilfe von dedizierten VPCs Netzen und Subnetzen

Das AWS Well-Architected Framework empfiehlt, Komponenten mit gemeinsamen Sensitivitätsanforderungen in Schichten zu gruppieren. Dadurch wird das potenzielle Ausmaß der Auswirkungen eines unbefugten Zugriffs minimiert. Beispielsweise sollte ein Datenbankcluster, der keinen Internetzugang benötigt, in einem privaten Subnetz seiner VPC platziert werden, um sicherzustellen, dass es keine Route zum oder vom Internet gibt.

AWS bietet viele Dienste, mit denen Sie die Erreichbarkeit für die Öffentlichkeit testen und ermitteln können. Reachability Analyzer ist beispielsweise ein Tool zur Konfigurationsanalyse, mit dem Sie die Konnektivität zwischen Quell- und Zielressourcen in Ihrem testen können. VPCs Außerdem kann Network Access Analyzer Ihnen helfen, unbeabsichtigte Netzwerkzugriffe auf Ressourcen zu identifizieren.

Weitere Informationen finden Sie in den folgenden Ressourcen:

- Erstellen Sie Netzwerkschichten im AWS Well-Architected Framework
- Dokumentation zu Reachability Analyzer
- Dokumentation zu Network Access Analyzer
- Erstellen Sie ein Subnetz in der Amazon Virtual Private Cloud (Amazon VPC) -Dokumentation

Beschränken Sie den eingehenden Datenverkehr auf nur autorisierte Ports

Uneingeschränkter Zugriff, z. B. Datenverkehr von der `0.0.0.0/0` Quell-IP-Adresse, erhöht das Risiko für böswillige Aktivitäten wie Hacking- denial-of-service (DoS-) Angriffe und Datenverlust. Sicherheitsgruppen ermöglichen eine statusorientierte Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen. AWS Keine Sicherheitsgruppe sollte uneingeschränkten Zugriff auf eingehende Zugriffe auf bekannte Ports wie SSH und Windows Remote Desktop Protocol (RDP) zulassen. Lassen Sie für eingehenden Datenverkehr in Ihren Sicherheitsgruppen nur TCP- oder UDP-Verbindungen an autorisierten Ports zu. Um eine Verbindung zu Amazon Elastic Compute Cloud (Amazon EC2) -Instances herzustellen, verwenden Sie Session Manager oder Run Command anstelle von direktem SSH- oder RDP-Zugriff.

Weitere Informationen finden Sie in den folgenden Ressourcen:

- Arbeiten Sie mit Sicherheitsgruppen in der EC2 Amazon-Dokumentation
- Steuern Sie den Datenverkehr zu Ihren AWS Ressourcen mithilfe von Sicherheitsgruppen in der Amazon VPC-Dokumentation

Sperren Sie den öffentlichen Zugriff auf Systems Manager Manager-Dokumente

Sofern Ihr Anwendungsfall nicht erfordert, dass die öffentliche Freigabe aktiviert ist, empfehlen die AWS Systems Manager bewährten Methoden, die öffentliche Freigabe für Systems Manager Manager-Dokumente zu blockieren. Das öffentliche Teilen kann zu unbeabsichtigtem Zugriff auf Dokumente führen. Ein öffentliches Systems Manager Manager-Dokument kann wertvolle und vertrauliche Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Weitere Informationen finden Sie in den folgenden Ressourcen:

- Bewährte Methoden für gemeinsam genutzte Systems Manager Manager-Dokumente in der Systems Manager Manager-Dokumentation
- Ändern Sie die Berechtigungen für ein gemeinsam genutztes Systems Manager Manager-Dokument in der Systems Manager Manager-Dokumentation

Blockieren Sie den öffentlichen Zugriff auf Lambda-Funktionen

AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne dass Sie Server bereitstellen oder verwalten müssen. Lambda-Funktionen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf den Funktionscode ermöglichen könnte.

Wir empfehlen Ihnen, ressourcenbasierte Richtlinien für Lambda-Funktionen zu konfigurieren, um den Zugriff von außerhalb Ihres Kontos zu verweigern. Sie können dies erreichen, indem Sie Berechtigungen entfernen oder der Anweisung die `AWS:SourceAccount` Bedingung hinzufügen, die den Zugriff gewährt. Sie können ressourcenbasierte Richtlinien für Lambda-Funktionen über die Lambda-API oder () aktualisieren. AWS Command Line Interface AWS CLI

Wir empfehlen außerdem, dass Sie die [Lambda.1] Lambda-Funktionsrichtlinien aktivieren, um die öffentliche Zugriffskontrolle in zu verbieten. AWS Security Hub CSPM Dieses Steuerelement bestätigt, dass ressourcenbasierte Richtlinien für Lambda-Funktionen den öffentlichen Zugriff verbieten.

Weitere Informationen finden Sie in den folgenden Ressourcen:

- AWS Lambda Kontrollen in der Security Hub CSPM-Dokumentation
- Verwendung ressourcenbasierter Richtlinien für Lambda in der Lambda-Dokumentation
- Ressourcen und Bedingungen für Lambda-Aktionen in der Lambda-Dokumentation

Beschränken Sie eingehenden und ausgehenden Datenverkehr in der Standardsicherheitsgruppe

Wenn Sie bei der Bereitstellung einer AWS Ressource keine benutzerdefinierte Sicherheitsgruppe zuordnen, wird die Ressource der Standardsicherheitsgruppe der VPC zugeordnet. Die Standardregeln für diese Sicherheitsgruppe lassen den gesamten eingehenden Verkehr von allen

Ressourcen zu, die dieser Sicherheitsgruppe zugewiesen sind, und sie lassen den gesamten ausgehenden IPv4 Verkehr und Datenverkehr zu. IPv6 Dies kann unbeabsichtigten Datenverkehr zur Ressource ermöglichen.

AWS empfiehlt, die Standardsicherheitsgruppe nicht zu verwenden. Erstellen Sie stattdessen benutzerdefinierte Sicherheitsgruppen für bestimmte Ressourcen oder Ressourcengruppen.

Da die Standardsicherheitsgruppe nicht gelöscht werden kann, empfehlen wir, die Standardsicherheitsgruppenregeln zu ändern, um den eingehenden und ausgehenden Datenverkehr einzuschränken. Beachten Sie bei der Konfiguration von Sicherheitsgruppenregeln das Prinzip der geringsten Rechte.

Wir empfehlen außerdem, die [EC2.2] VPC-Standardsicherheitsgruppen sollten keine Kontrolle des eingehenden oder ausgehenden Datenverkehrs in Security Hub CSPM zulassen. Dieses Steuerelement bestätigt, dass die Standardsicherheitsgruppe einer VPC eingehenden und ausgehenden Datenverkehr ablehnt.

Weitere Informationen finden Sie in den folgenden Ressourcen:

- Steuern Sie den Datenverkehr zu Ihren AWS Ressourcen mithilfe von Sicherheitsgruppen in der Amazon VPC-Dokumentation
- Standard-Sicherheitsgruppen für Sie VPCs in der Amazon VPC-Dokumentation
- Amazon EC2 Controls in der CSPM-Dokumentation von Security Hub

Suchen Sie nach Software-Sicherheitslücken und unbeabsichtigter Netzwerkgefährdung

Wir empfehlen Ihnen, Amazon Inspector in all Ihren Konten zu aktivieren. Amazon Inspector ist ein Schwachstellen-Management-Service, der Ihre EC2 Amazon-Instances, Container-Images von Amazon Elastic Container Registry (Amazon ECR) und Lambda-Funktionen kontinuierlich auf Softwareschwachstellen und unbeabsichtigte Netzwerkgefährdung überprüft. Es unterstützt auch die eingehende Inspektion von EC2 Amazon-Instances. Wenn Amazon Inspector eine Sicherheitslücke oder einen offenen Netzwerkpfad identifiziert, wird ein Ergebnis generiert, das Sie untersuchen können. Wenn Amazon Inspector und Security Hub CSPM beide in Ihrem Konto eingerichtet sind, sendet Amazon Inspector automatisch Sicherheitsergebnisse zur zentralen Verwaltung an Security Hub CSPM.

Weitere Informationen finden Sie in den folgenden Ressourcen:

- Scannen von Ressourcen mit Amazon Inspector in der Amazon Inspector Inspector-Dokumentation
- Amazon Inspector Deep Inspection für Amazon EC2 in der Amazon Inspector Inspector-Dokumentation
- Scannen EC2 AMIs mit Amazon Inspector im AWS Sicherheitsblog
- Aufbau eines skalierbaren Schwachstellen-Management-Programms auf Basis von AWS AWS Prescriptive Guidance
- Automatisieren Sie den Netzwerkschutz im AWS Well-Architected Framework
- Automatisieren Sie den Computerschutz im AWS Well-Architected Framework

Einrichten AWS WAF

AWS WAFist eine Webanwendungs-Firewall, mit der Sie HTTP- oder HTTPS-Anfragen überwachen und blockieren können, die an Ihre geschützten Webanwendungsressourcen wie Amazon API Gateway APIs, CloudFront Amazon-Distributionen oder Application Load Balancers weitergeleitet werden. Basierend auf den von Ihnen angegebenen Kriterien beantwortet der Service Anfragen entweder mit dem angeforderten Inhalt, mit einem HTTP-403-Statuscode (Verboten) oder mit einer benutzerdefinierten Antwort. AWS WAF kann zum Schutz von Webanwendungen oder APIs vor gängigen Web-Exploits beitragen, die die Verfügbarkeit beeinträchtigen, die Sicherheit gefährden oder übermäßig viele Ressourcen verbrauchen können. Erwägen Sie die Einrichtung AWS WAF AWS-Konten und Verwendung einer Kombination aus AWS verwalteten Regeln, benutzerdefinierten Regeln und Partnerintegrationen, um Ihre Anwendungen vor Angriffen auf Anwendungsebene (Layer 7) zu schützen.

Weitere Informationen finden Sie in den folgenden Ressourcen:

- Erste Schritte AWS WAF in der Dokumentation AWS WAF
- AWS WAF Lieferpartner auf der AWS Website
- Sicherheitsautomatisierungen für AWS WAF in der AWS Solutions Library
- Implementieren Sie Inspektion und Schutz im AWS Well-Architected Framework

Konfigurieren Sie erweiterte Schutzmaßnahmen gegen S-Angriffe DDo

AWS Shieldbietet Schutz vor verteilten Denial-of-Service-Angriffen (DDoS) für AWS Ressourcen auf der Netzwerk- und Transportebene (Schicht 3 und 4) sowie auf der Anwendungsebene (Schicht 7). Dieser Service ist in zwei Optionen verfügbar: AWS Shield Standard und. AWS Shield Advanced Shield Standard schützt automatisch unterstützte AWS Ressourcen ohne zusätzliche Kosten.

Wir empfehlen Ihnen, Shield Advanced zu abonnieren, das erweiterten DDo S-Angriffsschutz für geschützte Ressourcen bietet. Der Schutz, den Sie von Shield Advanced erhalten, hängt von Ihrer Architektur und Ihren Konfigurationsoptionen ab. Erwägen Sie die Implementierung von Shield Advanced-Schutzmaßnahmen für Anwendungen, für die Sie Folgendes benötigen:

- Garantierte Verfügbarkeit für die Benutzer der Anwendung.
- Schneller Zugang zu Experten zur DDo S-Abwehr, falls die Anwendung von einem DDo S-Angriff betroffen ist.
- Kenntnis von AWS, dass die Anwendung von einem DDo S-Angriff betroffen sein könnte, und Benachrichtigung über Angriffe von AWS und Eskalation an Ihre Sicherheits- oder Betriebsteams.
- Vorhersehbarkeit Ihrer Cloud-Kosten, auch wenn sich ein DDo S-Angriff auf Ihre Nutzung von auswirkt. AWS-Services

Weitere Informationen finden Sie in den folgenden Ressourcen:

- AWS Shield Advanced Überblick in der Shield-Dokumentation
- AWS Shield Advanced geschützte Ressourcen in der Shield-Dokumentation
- AWS Shield Advanced Funktionen und Optionen in der Shield-Dokumentation
- Reagieren auf DDo S-Ereignisse in der Shield-Dokumentation
- Implementieren Sie Inspektion und Schutz im AWS Well-Architected Framework

Verwenden Sie einen defense-in-depth Ansatz zur Steuerung des Netzwerkverkehrs

AWS Network Firewall ist ein zustandsbehafteter, verwalteter Dienst zur Netzwerk-Firewall und zur Erkennung und Verhinderung von Eindringlingen für virtuelle private Clouds (VPCs) in der.

AWS Cloud Es hilft Ihnen dabei, wichtige Netzwerkschutzmaßnahmen am Perimeter der VPC bereitzustellen. Dazu gehört das Filtern von Datenverkehr, der zu und von einem Internet-Gateway, NAT-Gateway oder über VPN oder kommt. AWS Direct Connect Die Network Firewall umfasst Funktionen, die zum Schutz vor gängigen Netzwerkbedrohungen beitragen. Die Stateful-Firewall in der Network Firewall kann den Kontext von Verkehrsströmen wie Verbindungen und Protokollen einbeziehen, um Richtlinien durchzusetzen.

Weitere Informationen finden Sie in den folgenden Ressourcen:

- AWS Network Firewall Dokumentation
- Steuern Sie den Verkehr auf allen Ebenen im AWS Well-Architected Framework

Empfehlungen zur Sicherheitskontrolle zum Schutz von Daten

Das AWS Well-Architected Framework unterteilt die bewährten Methoden zum Schutz von Daten in drei Kategorien: Datenklassifizierung, Schutz ruhender Daten und Schutz von Daten bei der Übertragung. Die Sicherheitskontrollen in diesem Abschnitt können Ihnen dabei helfen, bewährte Methoden für den Datenschutz zu implementieren. Diese grundlegenden bewährten Methoden sollten vorhanden sein, bevor Sie Workloads in der Cloud entwerfen. Sie verhindern einen falschen Umgang mit Daten und helfen Ihnen, organisatorische, regulatorische und Compliance-Verpflichtungen zu erfüllen. Verwenden Sie die Sicherheitskontrollen in diesem Abschnitt, um bewährte Methoden für den Datenschutz zu implementieren.

Steuerelemente in diesem Abschnitt:

- Identifizieren und klassifizieren Sie Daten auf Workload-Ebene
- Richten Sie Kontrollen für jede Datenklassifizierungsebene ein
- Daten im Ruhezustand verschlüsseln
- Verschlüsseln Sie Daten während der Übertragung
- Sperren Sie den öffentlichen Zugriff auf Amazon EBS-Snapshots
- Sperren Sie den öffentlichen Zugriff auf Amazon RDS-Snapshots
- Sperren Sie den öffentlichen Zugriff auf Amazon RDS, Amazon Redshift und Ressourcen AWS DMS
- Blockieren Sie den öffentlichen Zugriff auf Amazon S3 S3-Buckets
- MFA zum Löschen von Daten in kritischen Amazon S3 S3-Buckets anfordern
- Amazon OpenSearch Service-Domains in einer VPC konfigurieren
- Konfigurieren Sie Warnmeldungen für das Löschen AWS KMS key
- Sperren Sie den öffentlichen Zugriff auf AWS KMS keys
- Konfigurieren Sie Load Balancer-Listener für die Verwendung sicherer Protokolle

Identifizieren und klassifizieren Sie Daten auf Workload-Ebene

Datenklassifizierung ist ein Prozess zur Identifizierung und Kategorisierung der Daten in Ihrem Netzwerk auf der Grundlage ihrer Kritikalität und Sensitivität. Sie ist eine wichtige Komponente jeder

Strategie für das Management von Cybersecurity-Risiken, da sie Ihnen hilft, die geeigneten Schutz- und Aufbewahrungskontrollen für die Daten zu bestimmen. Durch die Datenklassifizierung wird häufig die Häufigkeit von Datenduplizierungen reduziert. Dadurch können Speicher- und Backup-Kosten gesenkt und Suchvorgänge beschleunigt werden.

Wir empfehlen Ihnen, sich mit der Art und Klassifizierung der Daten, die Ihr Workload verarbeitet, mit den zugehörigen Geschäftsprozessen, dem Speicherort der Daten und dem Eigentümer der Daten vertraut zu machen. Die Datenklassifizierung hilft Workload-Besitzern dabei, Standorte zu identifizieren, an denen vertrauliche Daten gespeichert werden, und zu bestimmen, wie auf diese Daten zugegriffen und sie gemeinsam genutzt werden sollen. Tags sind Schlüssel-Wert-Paare, die als Metadaten für die Organisation der AWS Ressourcen dienen. Tags können dabei helfen, Ressourcen zu verwalten, zu identifizieren, zu organisieren, zu suchen und zu filtern.

Weitere Informationen finden Sie in den folgenden Ressourcen:

- Datenklassifizierung in AWS Whitepapers
- Identifizieren Sie die Daten innerhalb Ihres Workloads im AWS Well-Architected Framework

Richten Sie Kontrollen für jede Datenklassifizierungsebene ein

Definieren Sie Datenschutzkontrollen für jede Klassifizierungsebene. Verwenden Sie beispielsweise empfohlene Kontrollen, um Daten zu sichern, die als öffentlich eingestuft sind, und schützen Sie sensible Daten mit zusätzlichen Kontrollen. Verwenden Sie Mechanismen und Tools, die den direkten Zugriff auf oder die manuelle Verarbeitung von Daten reduzieren oder ganz vermeiden. Die Automatisierung der Datenidentifikation und -klassifizierung reduziert das Risiko von Fehlklassifizierungen, falscher Handhabung, Änderung oder menschlichem Versagen.

Erwägen Sie beispielsweise, Amazon Macie zu verwenden, um Amazon Simple Storage Service (Amazon S3) -Buckets nach sensiblen Daten wie personenbezogenen Daten (PII) zu durchsuchen. Außerdem können Sie die Erkennung von unbeabsichtigtem Datenzugriff automatisieren, indem Sie VPC Flow Logs in Amazon Virtual Private Cloud (Amazon VPC) verwenden.

Weitere Informationen finden Sie in den folgenden Ressourcen:

- Definieren Sie Datenschutzkontrollen im AWS Well-Architected Framework
- Automatisieren Sie die Identifizierung und Klassifizierung im AWS Well-Architected Framework
- AWS Die Referenzarchitektur zum Datenschutz (AWS PRA) in AWS präskriptiven Leitlinien

- Erkennung sensibler Daten mit Amazon Macie in der Macie-Dokumentation
- Protokollierung von IP-Verkehr mithilfe von VPC Flow Logs in der Amazon VPC-Dokumentation
- Gängige Techniken zur Erkennung von PHI- und PII-Daten mithilfe des AWS-Services AWS ForIndustries-Blogs

Daten im Ruhezustand verschlüsseln

Daten im Ruhezustand sind Daten, die sich stationär in Ihrem Netzwerk befinden, z. B. Daten, die sich im Speicher befinden. Die Implementierung von Verschlüsselung und geeigneten Zugriffskontrollen für ruhende Daten trägt dazu bei, das Risiko eines unbefugten Zugriffs zu verringern. Verschlüsselung ist ein Rechenprozess, bei dem Klartextdaten, die für Menschen lesbar sind, in Chiffretext umgewandelt werden. Sie benötigen einen Verschlüsselungsschlüssel, um den Inhalt wieder in Klartext zu entschlüsseln, sodass er verwendet werden kann. In der können Sie AWS Key Management Service (AWS KMS) verwenden AWS Cloud, um kryptografische Schlüssel zu erstellen und zu kontrollieren, die zum Schutz Ihrer Daten beitragen.

Wie unter beschrieben, empfehlen wirRichten Sie Kontrollen für jede Datenklassifizierungsebene ein, eine Richtlinie zu erstellen, die festlegt, welche Art von Daten verschlüsselt werden muss. Geben Sie Kriterien an, nach denen bestimmt wird, welche Daten verschlüsselt und welche Daten mit einer anderen Technik wie Tokenisierung oder Hashing geschützt werden sollen.

Weitere Informationen finden Sie in den folgenden Ressourcen:

- Konfiguration der Standardverschlüsselung in der Amazon S3 S3-Dokumentation
- Standardverschlüsselung für neue EBS-Volumes und Snapshot-Kopien in der Amazon-Dokumentation EC2
- Verschlüsseln von Amazon Aurora Aurora-Ressourcen in der Amazon Aurora Aurora-Dokumentation
- Einführung in die kryptografischen Details von AWS KMS in der Dokumentation AWS KMS
- Erstellung einer unternehmensweiten Verschlüsselungsstrategie für gespeicherte Daten in AWS Prescriptive Guidance
- Erzwingen Sie die Verschlüsselung im Ruhezustand im AWS Well-Architected Framework
- Weitere spezifische AWS-Services Informationen zur Verschlüsselung finden Sie in der AWS Dokumentation zu diesem Dienst

Verschlüsseln Sie Daten während der Übertragung

Daten während der Übertragung sind Daten, die sich aktiv durch Ihr Netzwerk bewegen, z. B. zwischen Netzwerkressourcen. Verschlüsseln Sie alle Daten während der Übertragung mithilfe sicherer TLS-Protokolle und Cipher Suites. Der Netzwerkverkehr zwischen den Ressourcen und dem Internet muss verschlüsselt werden, um unbefugten Zugriff auf die Daten zu verhindern. Verwenden Sie nach Möglichkeit TLS, um den Netzwerkverkehr in Ihrer internen AWS Umgebung zu verschlüsseln.

Weitere Informationen finden Sie in den folgenden Ressourcen:

- HTTPS für die Kommunikation zwischen Zuschauern und CloudFront in der CloudFront Amazon-Dokumentation erforderlich
- AWS PrivateLink -Dokumentation
- Erzwingen Sie die Verschlüsselung bei der Übertragung im AWS Well-Architected Framework
- Weitere spezifische AWS-Services Informationen zur Verschlüsselung finden Sie in der AWS Dokumentation zu diesem Dienst

Sperren Sie den öffentlichen Zugriff auf Amazon EBS-Snapshots

Amazon Elastic Block Store (Amazon EBS) bietet Speichervolumes auf Blockebene zur Verwendung mit Amazon Elastic Compute Cloud (Amazon EC2) -Instances. Sie können die Daten auf Ihren Amazon EBS-Volumes auf Amazon S3 sichern, indem Sie point-in-time Snapshots erstellen. Sie können Snapshots öffentlich mit allen anderen teilen AWS-Konten, oder Sie können sie privat mit einer von Ihnen angegebenen Person AWS-Konten teilen.

Wir empfehlen, Amazon EBS-Snapshots nicht öffentlich zu teilen. Dadurch könnten versehentlich vertrauliche Daten offengelegt werden. Wenn Sie einen Snapshot teilen, gewähren Sie anderen Zugriff auf die Daten im Snapshot. Teilen Sie Snapshots nur mit Personen, denen Sie all diese Daten anvertrauen.

Weitere Informationen finden Sie in den folgenden Ressourcen:

- Einen Schnappschuss in der EC2 Amazon-Dokumentation teilen
- Amazon EBS-Snapshots sollten in der Dokumentation nicht öffentlich wiederherstellbar sein AWS Security Hub CSPM

- ebs-snapshot-public-restorable-schauen Sie in der Dokumentation nach AWS Config

Sperren Sie den öffentlichen Zugriff auf Amazon RDS-Snapshots

Amazon Relational Database Service (Amazon RDS) unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen Datenbank in der. AWS Cloud Amazon RDS erstellt und speichert automatische Backups Ihrer Datenbank-Instance (DB) oder Ihres Multi-AZ-DB-Clusters während des Backup-Fensters Ihrer DB-Instance. Amazon RDS erstellt einen Snapshot für das Speichervolume der DB-Instance, damit die gesamte DB-Instance gesichert wird und nicht nur einzelne Datenbanken. Sie können einen manuellen Snapshot teilen, um den Snapshot zu kopieren oder eine DB-Instance daraus wiederherzustellen.

Wenn Sie einen Snapshot als öffentlich freigeben, stellen Sie sicher, dass keine der Daten im Snapshot privat oder vertraulich ist. Wenn ein Snapshot öffentlich geteilt wird, erhält AWS-Konten jeder Zugriff auf die Daten. Dies kann zu einer unbeabsichtigten Offenlegung der Daten in Ihrer Amazon RDS-Instance führen.

Weitere Informationen finden Sie in den folgenden Ressourcen:

- Einen DB-Snapshot in der Amazon RDS-Dokumentation teilen
- rds-snapshots-public-prohibitedin der AWS Config Dokumentation
- Der RDS-Snapshot sollte in der Security Hub CSPM-Dokumentation privat sein

Sperren Sie den öffentlichen Zugriff auf Amazon RDS, Amazon Redshift und Ressourcen AWS DMS

Sie können Amazon RDS-DB-Instances, Amazon Redshift Redshift-Cluster und AWS Database Migration Service (AWS DMS) Replikations-Instances so konfigurieren, dass sie öffentlich zugänglich sind. Wenn der `publiclyAccessible` Feldwert lautet`true`, sind diese Ressourcen öffentlich zugänglich. Wenn der öffentliche Zugriff gewährt wird, kann dies zu unnötigem Datenverkehr, Datenlecks oder Datenlecks führen. Wir empfehlen, den öffentlichen Zugriff auf diese Ressourcen nicht zuzulassen.

Wir empfehlen, AWS Config Regeln oder Security Hub CSPM-Steuerungen zu aktivieren, um zu erkennen, ob Amazon RDS-DB-Instances, AWS DMS Replikations-Instances oder Amazon Redshift Redshift-Cluster öffentlichen Zugriff zulassen.

> **Note**
>
> Die Einstellungen für den öffentlichen Zugriff für AWS DMS Replikations-Instances können nach der Bereitstellung der Instance nicht geändert werden. Um die Einstellung für den öffentlichen Zugriff zu ändern, löschen Sie die aktuelle Instanz und erstellen Sie sie anschließend neu. Wenn Sie sie neu erstellen, wählen Sie nicht die Option Öffentlich zugänglich aus.

Weitere Informationen finden Sie in den folgenden Ressourcen:

- AWS DMS Replikationsinstanzen sollten in der Security Hub CSPM-Dokumentation nicht öffentlich sein
- RDS-DB-Instances sollten den öffentlichen Zugriff in der Security Hub CSPM-Dokumentation verbieten
- Amazon Redshift Redshift-Cluster sollten den öffentlichen Zugriff in der Security Hub CSPM-Dokumentation verbieten
- rds-instance-public-access-schauen Sie in der Dokumentation nach AWS Config
- dms-replication-not-publicin der Dokumentation AWS Config
- redshift-cluster-public-access-checken Sie in der AWS Config Dokumentation nach
- Ändern einer Amazon RDS-DB-Instance in der Amazon RDS-Dokumentation
- Ändern eines Clusters in der Amazon Redshift Redshift-Dokumentation

Blockieren Sie den öffentlichen Zugriff auf Amazon S3 S3-Buckets

Es ist eine bewährte Sicherheitsmethode von Amazon S3, um sicherzustellen, dass Ihre Buckets nicht öffentlich zugänglich sind. Stellen Sie sicher, dass Ihr Bucket nicht öffentlich ist, sofern Sie nicht ausdrücklich verlangen, dass jemand im Internet in der Lage ist, Ihren Bucket zu lesen oder in ihn zu schreiben. Dies trägt zum Schutz der Integrität und Sicherheit der Daten bei. Sie können AWS Config Regeln und Security Hub CSPM-Steuerungen verwenden, um zu überprüfen, ob Ihre Amazon S3 S3-Buckets dieser Best Practice entsprechen.

Weitere Informationen finden Sie in den folgenden Ressourcen:

- Bewährte Methoden zur Amazon S3 S3-Sicherheit in der Amazon S3 S3-Dokumentation

- Die Einstellung S3 Block Public Access sollte in der Security Hub CSPM-Dokumentation aktiviert sein
- S3-Buckets sollten den öffentlichen Lesezugriff in der Security Hub CSPM-Dokumentation verbieten
- S3-Buckets sollten öffentlichen Schreibzugriff in der Security Hub CSPM-Dokumentation verbieten
- s3-Regel in der Dokumentation bucket-public-read-prohibited AWS Config
- s3- bucket-public-write-prohibited in der AWS Config Dokumentation

MFA zum Löschen von Daten in kritischen Amazon S3 S3-Buckets anfordern

Wenn Sie in Amazon-S3-Buckets mit S3-Versioning arbeiten, können Sie optional eine weitere Sicherheitsebene hinzufügen, indem Sie einen Bucket konfigurieren, um MFA (multi-factor authentication) delete zu aktivieren. In diesem Fall muss der Bucket-Eigentümer zwei Authentifizierungsformen in jede Anforderung aufnehmen, um eine Version zu löschen oder den Versioning-Status des Buckets zu ändern. Wir empfehlen, diese Funktion für Buckets zu aktivieren, die Daten enthalten, die für Ihr Unternehmen von entscheidender Bedeutung sind. Dadurch kann ein versehentliches Löschen von Buckets und Daten verhindert werden.

Weitere Informationen finden Sie in den folgenden Ressourcen:

- Konfiguration von MFA Delete in der Amazon S3 S3-Dokumentation

Amazon OpenSearch Service-Domains in einer VPC konfigurieren

Amazon OpenSearch Service ist ein verwalteter Service, der Sie bei der Bereitstellung, dem Betrieb und der Skalierung von OpenSearch Clustern in der unterstützt AWS Cloud. Amazon OpenSearch Service unterstützt OpenSearch ältere Elasticsearch Open-Source-Software (OSS). Amazon OpenSearch Service-Domains, die in einer VPC bereitgestellt werden, können über das private AWS Netzwerk mit VPC-Ressourcen kommunizieren, ohne das öffentliche Internet durchqueren zu müssen. Diese Konfiguration verbessert Ihre Sicherheitslage, indem sie den Zugriff auf die Daten während der Übertragung einschränkt. Wir empfehlen, dass Sie Amazon OpenSearch Service-Domains nicht an öffentliche Subnetze anhängen und dass die VPC gemäß den Best Practices konfiguriert wird.

Weitere Informationen finden Sie in den folgenden Ressourcen:

- Starten Ihrer Amazon OpenSearch Service-Domains innerhalb einer VPC in der Amazon OpenSearch Service-Dokumentation
- opensearch-in-vpc-onlyin der Dokumentation AWS Config
- OpenSearchDomänen sollten sich in der Security Hub CSPM-Dokumentation in einer VPC befinden

Konfigurieren Sie Warnmeldungen für das Löschen AWS KMS key

AWS Key Management Service (AWS KMS) Schlüssel können nicht wiederhergestellt werden, nachdem sie gelöscht wurden. Wenn ein KMS-Schlüssel gelöscht wird, können Daten, die unter diesem Schlüssel noch verschlüsselt sind, dauerhaft nicht wiederhergestellt werden. Wenn Sie den Zugriff auf die Daten behalten möchten, müssen Sie die Daten vor dem Löschen des Schlüssels entschlüsseln oder mit einem neuen KMS-Schlüssel erneut verschlüsseln. Löschen Sie einen KMS-Schlüssel nur, wenn Sie sicher sind, dass Sie ihn nicht mehr benötigen.

Wir empfehlen Ihnen, einen CloudWatch Amazon-Alarm zu konfigurieren, der Sie benachrichtigt, wenn jemand das Löschen eines KMS-Schlüssels initiiert. Da das Löschen eines KMS-Schlüssels zerstörerisch und potenziell gefährlich ist, AWS KMS müssen Sie eine Wartezeit festlegen und das Löschen auf 7—30 Tage planen. Dies bietet Ihnen die Möglichkeit, den geplanten Löschvorgang zu überprüfen und ihn gegebenenfalls abzubrechen.

Weitere Informationen finden Sie in den folgenden Ressourcen:

- Das Löschen von Schlüsseln wird in der Dokumentation geplant und storniert AWS KMS
- In der Dokumentation wird ein Alarm erstellt, der die Verwendung eines KMS-Schlüssels erkennt, dessen Löschung noch aussteht AWS KMS
- AWS KMS keys sollte nicht unbeabsichtigt in der Security Hub CSPM-Dokumentation gelöscht werden

Sperren Sie den öffentlichen Zugriff auf AWS KMS keys

Wichtige Richtlinien sind die wichtigste Methode zur Steuerung des Zugriffs auf AWS KMS keys. Jeder KMS-Schlüssel besitzt genau eine Schlüsselrichtlinie. Wenn Sie anonymen Zugriff auf KMS-Schlüssel zulassen, kann dies zu einem Verlust vertraulicher Daten führen. Wir empfehlen Ihnen, alle

öffentlich zugänglichen KMS-Schlüssel zu identifizieren und ihre Zugriffsrichtlinien zu aktualisieren, um zu verhindern, dass unsignierte Anfragen an diese Ressourcen gestellt werden.

Weitere Informationen finden Sie in den folgenden Ressourcen:

- Bewährte Sicherheitsmethoden finden Sie AWS Key Management Service in der Dokumentation AWS KMS
- Änderung einer wichtigen Richtlinie in der AWS KMS Dokumentation
- Bestimmung des Zugriffs auf AWS KMS keys in der AWS KMS Dokumentation

Konfigurieren Sie Load Balancer-Listener für die Verwendung sicherer Protokolle

Elastic Load Balancing verteilt den eingehenden Anwendungsdatenverkehr automatisch auf mehrere Ziele. Sie konfigurieren Ihren Load Balancer für eingehenden Datenverkehr, indem Sie einen oder mehrere Listener angeben. Ein Listener ist ein Prozess, der mit dem Protokoll und dem Port, das bzw. den Sie konfigurieren, Verbindungsanforderungen prüft. Jeder Load Balancer-Typ unterstützt unterschiedliche Protokolle und Ports:

- Application Load Balancer treffen Routing-Entscheidungen auf Anwendungsebene und verwenden HTTP- oder HTTPS-Protokolle.
- Network Load Balancer treffen Routing-Entscheidungen auf der Transportschicht und verwenden die Protokolle TCP, TLS, UDP oder TCP_UDP.
- Classic Load Balancer treffen Routing-Entscheidungen entweder auf der Transportschicht (mithilfe von TCP- oder SSL-Protokollen) oder auf der Anwendungsebene (mithilfe von HTTP- oder HTTPS-Protokollen).

Wir empfehlen, immer die Protokolle HTTPS oder TLS zu verwenden. Diese Protokolle stellen sicher, dass der Load Balancer für die Verschlüsselung und Entschlüsselung des Datenverkehrs zwischen dem Client und dem Ziel verantwortlich ist.

Weitere Informationen finden Sie in den folgenden Ressourcen:

- Listener für Ihre Application Load Balancer in der Elastic Load Balancing Balancing-Dokumentation
- Listener für Ihren Classic Load Balancer in der Elastic Load Balancing Balancing-Dokumentation
- Listener für Ihre Network Load Balancer in der Elastic Load Balancing Balancing-Dokumentation

- Stellen Sie in Prescriptive Guidance sicher, dass AWS Load Balancer sichere Listener-Protokolle verwenden AWS
- elb-tls-https-listeners-nur in der Dokumentation AWS Config
- Classic Load Balancer Balancer-Listener sollten in der Security Hub CSPM-Dokumentation mit HTTPS- oder TLS-Terminierung konfiguriert werden
- Der Application Load Balancer sollte in der Security Hub CSPM-Dokumentation so konfiguriert sein, dass alle HTTP-Anfragen an HTTPS umgeleitet werden

Sicherheitsempfehlungen für die Reaktion auf Vorfälle

Wenn in Ihrem Unternehmen ein Sicherheitsereignis eintritt, müssen Ihre Benutzer darauf vorbereitet sein, darauf zu reagieren. Alle Benutzer sollten ein grundlegendes Verständnis der Sicherheitsreaktionsprozesse Ihres Unternehmens haben. Planung, Schulung und Erfahrung sind entscheidend für ein erfolgreiches Incident-Response-Programm. Idealerweise bereiten Sie Ihr Unternehmen darauf vor, dass ein potenzielles Sicherheitsereignis eintritt. Das AWS Well-Architected Framework identifiziert drei Grundlagen, die für ein erfolgreiches Incident-Response-Programm in der Cloud erforderlich sind: Vorbereitung, Betrieb und Aktivitäten nach dem Vorfall. Weitere Informationen finden Sie unter Aspekte der Reaktion auf AWS Vorfälle im AWS Well-Architected Framework.

Mit Ausnahme von Sicherheitskontrollen, die Sie über Ereignisse informieren oder automatisch darauf reagieren, gibt es nur begrenzte Kontrollen, die Sie für die Reaktion auf Vorfälle einrichten können. Eine solide Reaktion auf Vorfälle wird in erster Linie durch die Pläne, Prozesse, Runbooks, Playbooks und Schulungsprogramme geschaffen, die Sie in Ihrem Unternehmen verwenden. Sie können die Kontrollen und Empfehlungen in diesem Abschnitt verwenden, um bewährte Verfahren für Ihr Incident-Response-Programm umzusetzen. Weitere Informationen zu bewährten Methoden für die Reaktion auf Vorfälle und Anleitungen zur Implementierung finden Sie unter Reaktion auf Vorfälle im AWS Well-Architected Framework.

Empfehlungen in diesem Abschnitt:

- Definieren Sie einen Plan zur Reaktion auf Vorfälle
- Erstellen und verwalten Sie Runbooks und Playbooks zur Reaktion auf Vorfälle
- Implementieren Sie eine ereignisgesteuerte Sicherheitsautomatisierung
- Dokumentieren Sie, wie Betriebsteams mit Support
- Konfigurieren Sie Warnmeldungen für Sicherheitsereignisse

Definieren Sie einen Plan zur Reaktion auf Vorfälle

Erstellen Sie einen klar definierten Plan zur Reaktion auf Vorfälle (IRP). Der Incident-Response-Plan soll die Grundlage für Ihr Incident-Response-Programm bilden. Dieser Plan muss an die Bedürfnisse jedes Unternehmens angepasst werden.

Weitere Informationen finden Sie in den folgenden Ressourcen:

- Entwickeln und testen Sie im AWS Security Incident Response Guide einen Plan zur Reaktion auf Vorfälle
- Entwickeln Sie Incident-Management-Pläne im AWS Well-Architected Framework
- Identifizieren Sie wichtige Mitarbeiter und externe Ressourcen im AWS Well-Architected Framework

Erstellen und verwalten Sie Runbooks und Playbooks zur Reaktion auf Vorfälle

Ein wichtiger Teil der Vorbereitung von Prozessen zur Reaktion auf Vorfälle ist die Entwicklung von Playbooks. Playbooks zur Reaktion auf Vorfälle enthalten eine Reihe von empfohlenen Schritten, die Benutzer befolgen müssen, wenn ein Sicherheitsereignis eintritt. Eine klare Struktur und klare Schritte vereinfachen die Reaktion und verringern die Wahrscheinlichkeit menschlicher Fehler.

Weitere Informationen finden Sie in den folgenden Ressourcen:

- Wofür sollten Playbooks im AWS Security Incident Response Guide erstellt werden
- AWS Beispiele für Playbooks zur Reaktion auf Incident Response auf GitHub
- Entwickeln und testen Sie Playbooks zur Reaktion auf Sicherheitsvorfälle im AWS Well-Architected Framework

Implementieren Sie eine ereignisgesteuerte Sicherheitsautomatisierung

Die Automatisierung von Sicherheitsreaktionen ist eine vordefinierte und programmierte Aktion, die darauf ausgelegt ist, automatisch auf ein Sicherheitsereignis zu reagieren oder es zu beheben. Diese Automatisierungen dienen als detektive oder reaktionsschnelle Sicherheitskontrollen, die Sie bei der Implementierung bewährter AWS Sicherheitsmethoden unterstützen. Beispiele für automatisierte Antwortaktionen sind das Ändern einer VPC-Sicherheitsgruppe, das Patchen einer EC2 Amazon-Instance oder das Rotieren von Anmeldeinformationen.

Viele AWS-Services unterstützen automatisierte Antworten. Sie können beispielsweise einen CloudWatch Amazon-Alarm für bestimmte Messwerte konfigurieren, und der Alarm kann eine Aktion einleiten, wenn der Alarm seinen Status ändert. Über Amazon EventBridge können Sie auch

automatische Reaktionen und Abhilfemaßnahmen für Ergebnisse in AWS Security Hub CSPM Amazon Inspector konfigurieren.

Weitere Informationen finden Sie in den folgenden Ressourcen:

- Automatisches Korrigieren von Amazon Inspector-Sicherheitsproblemen im AWS Sicherheits-Blog
- Erste Schritte mit der Automatisierung von Sicherheitsreaktionen finden Sie AWS im AWS Sicherheits-Blog
- Automatisierte Sicherheitsabwehr ist AWS in der AWS Solutions Library verfügbar
- Verwendung von CloudWatch Amazon-Alarmen in der CloudWatch Dokumentation
- Automatisierte Reaktion und Problembehebung in der Security Hub CSPM-Dokumentation
- Erstellen von benutzerdefinierten Antworten auf Ergebnisse von Amazon Inspector mit Amazon EventBridge in der Amazon Inspector Inspector-Dokumentation

Dokumentieren Sie, wie Betriebsteams mit Support

Für Ihren AWS-Konto können Sie einen Hauptansprechpartner und drei alternative Ansprechpartner definieren. Wir empfehlen, dass Sie für jeden AWS-Konto oder für Ihr Unternehmen einen Sicherheitskontakt angeben.

AWS Support bietet eine Reihe von Plänen, die den Zugriff auf Tools und Fachwissen ermöglichen, die den Erfolg und die Funktionsfähigkeit von AWS Lösungen unterstützen können. Überlegen Sie auch, ob Ihr Unternehmen von einer Nutzung AWS Managed Services statt eines Support Plans profitieren würde. AWS Managed Services (AMS) unterstützt Sie dabei, effizienter und sicherer zu arbeiten, indem es eine kontinuierliche Verwaltung Ihrer AWS Infrastruktur bietet, einschließlich Überwachung, Incident-Management, Sicherheitsberatung, Patch-Support und Backup für AWS Workloads. Das AMS-Supportmodell eignet sich möglicherweise besser für Unternehmen, deren Cloud-Betriebsteams nur über begrenzte Ressourcen verfügen. Wir empfehlen Ihnen, diese Modelle und Pläne miteinander zu vergleichen, um die für Ihr Unternehmen am besten geeignete Lösung und den Cloud-Reifegrad auszuwählen.

Weitere Informationen finden Sie in den folgenden Ressourcen:

- Erfahren Sie AWS mehr über Reaktionsteams und Support im AWS Security Incident Response Guide
- Aktualisieren Sie die alternativen Ansprechpartner für Sie AWS-Konto im AWS Account Management Guide

- Vergleichen Sie die Support Tarife auf der AWS Website
- Strategie AWS Managed Services zur Erreichung der angestrebten Geschäftsergebnisse im Rahmen von AWS Prescriptive Guidance

Konfigurieren Sie Warnmeldungen für Sicherheitsereignisse

Die Erkennung einer Abnormalität ist ebenso wichtig wie die Maßnahmen zur Bekämpfung dieser Abnormalität. Eine Warnung ist der Hauptbestandteil der Erkennungsphase. Es generiert eine Benachrichtigung, um den Prozess zur Reaktion auf Vorfälle auf der Grundlage der AWS-Konto gewünschten Aktivität einzuleiten. Stellen Sie sicher, dass die Benachrichtigungen relevante Informationen enthalten, damit das Team Maßnahmen ergreifen kann.

Weitere Informationen finden Sie in den folgenden Ressourcen:

- Erkennung im Leitfaden zur Reaktion auf AWS Sicherheitsvorfälle
- Bereiten Sie forensische Funktionen im Well-Architected Framework vor AWS
- Implementieren Sie umsetzbare Sicherheitsereignisse im AWS Well-Architected Framework

Nächste Schritte

Wenn Sie Ihre Reise in die Cloud fortsetzen, ist es wichtig, dass Sie diese dokumentierten Kontrollen, Anleitungen und Abhilfemaßnahmen anwenden. Diese Empfehlungen tragen dazu bei, Ihre Cloud-Sicherheit zu verbessern und Ihnen dabei zu helfen, Ihren Sicherheitsaufgaben nachzukommen AWS Cloud, wie sie im Modell der AWS gemeinsamen Verantwortung definiert sind.

Für die nächsten Schritte empfehlen wir Folgendes:

- Weitere Informationen zu Best Practices und Implementierungsleitlinien finden Sie in den sechs Säulen des AWS Well-Architected Framework.
- Sehen Sie AWS-Services sich die Liste der verfügbaren AWS Security Hub CSPM Kontrollen für die in Ihrer Organisation verwendeten Kontrollen an und prüfen Sie, ob Sie eine dieser Kontrollen in Ihrer Umgebung aktivieren sollten.
- Sehen Sie AWS-Services sich die Liste der verfügbaren AWS Config verwalteten Regeln für die in Ihrer Organisation verwendeten Regeln an und überlegen Sie, ob Sie eine dieser Regeln in Ihrer Umgebung aktivieren sollten.

Dokumentverlauf

In der folgenden Tabelle werden wichtige Änderungen in diesem Leitfaden beschrieben. Um Benachrichtigungen über zukünftige Aktualisierungen zu erhalten, können Sie einen RSS-Feed abonnieren.

Änderung	Beschreibung	Datum
MFA für Root-Benutzer	Wir haben die Empfehlungen aktualisiert und weitere Informationen im Abschnitt MFA für Root-Benutzer bereitgestellt.	9. November 2023
Erste Veröffentlichung	—	27. Oktober 2023

AWS Glossar zu präskriptiven Leitlinien

Die folgenden Begriffe werden häufig in Strategien, Leitfäden und Mustern verwendet, die von AWS Prescriptive Guidance bereitgestellt werden. Um Einträge vorzuschlagen, verwenden Sie bitte den Link Feedback geben am Ende des Glossars.

Zahlen

7 Rs

Sieben gängige Migrationsstrategien für die Verlagerung von Anwendungen in die Cloud. Diese Strategien bauen auf den 5 Rs auf, die Gartner 2011 identifiziert hat, und bestehen aus folgenden Elementen:

- Faktorwechsel/Architekturwechsel – Verschieben Sie eine Anwendung und ändern Sie ihre Architektur, indem Sie alle Vorteile cloudnativer Feature nutzen, um Agilität, Leistung und Skalierbarkeit zu verbessern. Dies beinhaltet in der Regel die Portierung des Betriebssystems und der Datenbank. Beispiel: Migrieren Sie Ihre lokale Oracle-Datenbank auf die Amazon Aurora PostgreSQL-kompatible Edition.
- Plattformwechsel (Lift and Reshape) – Verschieben Sie eine Anwendung in die Cloud und führen Sie ein gewisses Maß an Optimierung ein, um die Cloud-Funktionen zu nutzen. Beispiel: Migrieren Sie Ihre lokale Oracle-Datenbank zu Amazon Relational Database Service (Amazon RDS) für Oracle in der. AWS Cloud
- Neukauf (Drop and Shop) – Wechseln Sie zu einem anderen Produkt, indem Sie typischerweise von einer herkömmlichen Lizenz zu einem SaaS-Modell wechseln. Beispiel: Migrieren Sie Ihr CRM-System (Customer Relationship Management) zu Salesforce.com.
- Hostwechsel (Lift and Shift) – Verschieben Sie eine Anwendung in die Cloud, ohne Änderungen vorzunehmen, um die Cloud-Funktionen zu nutzen. Beispiel: Migrieren Sie Ihre lokale Oracle-Datenbank zu Oracle auf einer EC2 Instanz in der. AWS Cloud
- Verschieben (Lift and Shift auf Hypervisor-Ebene) – Verlagern Sie die Infrastruktur in die Cloud, ohne neue Hardware kaufen, Anwendungen umschreiben oder Ihre bestehenden Abläufe ändern zu müssen. Sie migrieren Server von einer lokalen Plattform zu einem Cloud-Dienst für dieselbe Plattform. Beispiel: Migrieren Sie eine Microsoft Hyper-V Anwendung zu AWS.
- Beibehaltung (Wiederaufgreifen) – Bewahren Sie Anwendungen in Ihrer Quellumgebung auf. Dazu können Anwendungen gehören, die einen umfangreichen Faktorwechsel erfordern und

die Sie auf einen späteren Zeitpunkt verschieben möchten, sowie ältere Anwendungen, die Sie beibehalten möchten, da es keine geschäftliche Rechtfertigung für ihre Migration gibt.

- Außerbetriebnahme – Dekommissionierung oder Entfernung von Anwendungen, die in Ihrer Quellumgebung nicht mehr benötigt werden.

A

ABAC

Siehe attributbasierte Zugriffskontrolle.

abstrahierte Dienste

Siehe Managed Services.

ACID

Siehe Atomarität, Konsistenz, Isolierung und Haltbarkeit.

Aktiv-Aktiv-Migration

Eine Datenbankmigrationsmethode, bei der die Quell- und Zieldatenbanken synchron gehalten werden (mithilfe eines bidirektionalen Replikationstools oder dualer Schreibvorgänge) und beide Datenbanken Transaktionen von miteinander verbundenen Anwendungen während der Migration verarbeiten. Diese Methode unterstützt die Migration in kleinen, kontrollierten Batches, anstatt einen einmaligen Cutover zu erfordern. Es ist flexibler, erfordert aber mehr Arbeit als eine aktiv-passive Migration.

Aktiv-Passiv-Migration

Eine Datenbankmigrationsmethode, bei der die Quell- und Zieldatenbanken synchron gehalten werden, aber nur die Quelldatenbank verarbeitet Transaktionen von verbindenden Anwendungen, während Daten in die Zieldatenbank repliziert werden. Die Zieldatenbank akzeptiert während der Migration keine Transaktionen.

Aggregatfunktion

Eine SQL-Funktion, die mit einer Gruppe von Zeilen arbeitet und einen einzelnen Rückgabewert für die Gruppe berechnet. Beispiele für Aggregatfunktionen sind `SUM` und`MAX`.

AI

Siehe künstliche Intelligenz.

AIOps

Siehe Operationen im Bereich künstliche Intelligenz.

Anonymisierung

Der Prozess des dauerhaften Löschens personenbezogener Daten in einem Datensatz. Anonymisierung kann zum Schutz der Privatsphäre beitragen. Anonymisierte Daten gelten nicht mehr als personenbezogene Daten.

Anti-Muster

Eine häufig verwendete Lösung für ein wiederkehrendes Problem, bei dem die Lösung kontraproduktiv, ineffektiv oder weniger wirksam als eine Alternative ist.

Anwendungssteuerung

Ein Sicherheitsansatz, bei dem nur zugelassene Anwendungen verwendet werden können, um ein System vor Schadsoftware zu schützen.

Anwendungsportfolio

Eine Sammlung detaillierter Informationen zu jeder Anwendung, die von einer Organisation verwendet wird, einschließlich der Kosten für die Erstellung und Wartung der Anwendung und ihres Geschäftswerts. Diese Informationen sind entscheidend für den Prozess der Portfoliofindung und -analyse und hilft bei der Identifizierung und Priorisierung der Anwendungen, die migriert, modernisiert und optimiert werden sollen.

künstliche Intelligenz (KI)

Das Gebiet der Datenverarbeitungswissenschaft, das sich der Nutzung von Computertechnologien zur Ausführung kognitiver Funktionen widmet, die typischerweise mit Menschen in Verbindung gebracht werden, wie Lernen, Problemlösen und Erkennen von Mustern. Weitere Informationen finden Sie unter Was ist künstliche Intelligenz?

Operationen mit künstlicher Intelligenz (AIOps)

Der Prozess des Einsatzes von Techniken des Machine Learning zur Lösung betrieblicher Probleme, zur Reduzierung betrieblicher Zwischenfälle und menschlicher Eingriffe sowie zur Steigerung der Servicequalität. Weitere Informationen darüber, wie AIOps es in der AWS Migrationsstrategie verwendet wird, finden Sie im Operations Integration Guide.

Asymmetrische Verschlüsselung

Ein Verschlüsselungsalgorithmus, der ein Schlüsselpaar, einen öffentlichen Schlüssel für die Verschlüsselung und einen privaten Schlüssel für die Entschlüsselung verwendet. Sie können den öffentlichen Schlüssel teilen, da er nicht für die Entschlüsselung verwendet wird. Der Zugriff auf den privaten Schlüssel sollte jedoch stark eingeschränkt sein.

Atomizität, Konsistenz, Isolierung, Haltbarkeit (ACID)

Eine Reihe von Softwareeigenschaften, die die Datenvalidität und betriebliche Zuverlässigkeit einer Datenbank auch bei Fehlern, Stromausfällen oder anderen Problemen gewährleisten.

Attributbasierte Zugriffskontrolle (ABAC)

Die Praxis, detaillierte Berechtigungen auf der Grundlage von Benutzerattributen wie Abteilung, Aufgabenrolle und Teamname zu erstellen. Weitere Informationen finden Sie unter ABAC AWS in der AWS Identity and Access Management (IAM-) Dokumentation.

maßgebliche Datenquelle

Ein Ort, an dem Sie die primäre Version der Daten speichern, die als die zuverlässigste Informationsquelle angesehen wird. Sie können Daten aus der maßgeblichen Datenquelle an andere Speicherorte kopieren, um die Daten zu verarbeiten oder zu ändern, z. B. zu anonymisieren, zu redigieren oder zu pseudonymisieren.

Availability Zone

Ein bestimmter Standort innerhalb einer AWS-Region , der vor Ausfällen in anderen Availability Zones geschützt ist und kostengünstige Netzwerkkonnektivität mit niedriger Latenz zu anderen Availability Zones in derselben Region bietet.

AWS Framework für die Einführung der Cloud (AWS CAF)

Ein Framework mit Richtlinien und bewährten Verfahren, das Unternehmen bei der Entwicklung eines effizienten und effektiven Plans für den erfolgreichen Umstieg auf die Cloud unterstützt. AWS AWS CAF unterteilt die Leitlinien in sechs Schwerpunktbereiche, die als Perspektiven bezeichnet werden: Unternehmen, Mitarbeiter, Unternehmensführung, Plattform, Sicherheit und Betrieb. Die Perspektiven Geschäft, Mitarbeiter und Unternehmensführung konzentrieren sich auf Geschäftskompetenzen und -prozesse, während sich die Perspektiven Plattform, Sicherheit und Betriebsabläufe auf technische Fähigkeiten und Prozesse konzentrieren. Die Personalperspektive zielt beispielsweise auf Stakeholder ab, die sich mit Personalwesen (HR), Personalfunktionen und Personalmanagement befassen. Aus dieser Perspektive bietet AWS CAF Leitlinien für Personalentwicklung, Schulung und Kommunikation, um das Unternehmen auf eine erfolgreiche

Cloud-Einführung vorzubereiten. Weitere Informationen finden Sie auf der AWS -CAF-Webseite und dem AWS -CAF-Whitepaper.

AWS Workload-Qualifizierungsrahmen (AWS WQF)

Ein Tool, das Workloads bei der Datenbankmigration bewertet, Migrationsstrategien empfiehlt und Arbeitsschätzungen bereitstellt. AWS WQF ist in () enthalten. AWS Schema Conversion Tool AWS SCT Es analysiert Datenbankschemas und Codeobjekte, Anwendungscode, Abhängigkeiten und Leistungsmerkmale und stellt Bewertungsberichte bereit.

B

schlechter Bot

Ein Bot, der Einzelpersonen oder Organisationen stören oder ihnen Schaden zufügen soll.

BCP

Siehe Planung der Geschäftskontinuität.

Verhaltensdiagramm

Eine einheitliche, interaktive Ansicht des Ressourcenverhaltens und der Interaktionen im Laufe der Zeit. Sie können ein Verhaltensdiagramm mit Amazon Detective verwenden, um fehlgeschlagene Anmeldeversuche, verdächtige API-Aufrufe und ähnliche Vorgänge zu untersuchen. Weitere Informationen finden Sie unter Daten in einem Verhaltensdiagramm in der Detective-Dokumentation.

Big-Endian-System

Ein System, welches das höchstwertige Byte zuerst speichert. Siehe auch Endianness.

Binäre Klassifikation

Ein Prozess, der ein binäres Ergebnis vorhersagt (eine von zwei möglichen Klassen). Beispielsweise könnte Ihr ML-Modell möglicherweise Probleme wie „Handelt es sich bei dieser E-Mail um Spam oder nicht?“ vorhersagen müssen oder „Ist dieses Produkt ein Buch oder ein Auto?“

Bloom-Filter

Eine probabilistische, speichereffiziente Datenstruktur, mit der getestet wird, ob ein Element Teil einer Menge ist.

Blau/Grün-Bereitstellung

Eine Bereitstellungsstrategie, bei der Sie zwei separate, aber identische Umgebungen erstellen. Sie führen die aktuelle Anwendungsversion in einer Umgebung (blau) und die neue Anwendungsversion in der anderen Umgebung (grün) aus. Mit dieser Strategie können Sie schnell und mit minimalen Auswirkungen ein Rollback durchführen.

Bot

Eine Softwareanwendung, die automatisierte Aufgaben über das Internet ausführt und menschliche Aktivitäten oder Interaktionen simuliert. Manche Bots sind nützlich oder nützlich, wie z. B. Webcrawler, die Informationen im Internet indexieren. Einige andere Bots, die als bösartige Bots bezeichnet werden, sollen Einzelpersonen oder Organisationen stören oder ihnen Schaden zufügen.

Botnetz

Netzwerke von Bots, die mit Malware infiziert sind und unter der Kontrolle einer einzigen Partei stehen, die als Bot-Herder oder Bot-Operator bezeichnet wird. Botnetze sind der bekannteste Mechanismus zur Skalierung von Bots und ihrer Wirkung.

branch

Ein containerisierter Bereich eines Code-Repositorys. Der erste Zweig, der in einem Repository erstellt wurde, ist der Hauptzweig. Sie können einen neuen Zweig aus einem vorhandenen Zweig erstellen und dann Feature entwickeln oder Fehler in dem neuen Zweig beheben. Ein Zweig, den Sie erstellen, um ein Feature zu erstellen, wird allgemein als Feature-Zweig bezeichnet. Wenn das Feature zur Veröffentlichung bereit ist, führen Sie den Feature-Zweig wieder mit dem Hauptzweig zusammen. Weitere Informationen finden Sie unter Über Branches (GitHub Dokumentation).

Zugang durch Glasbruch

Unter außergewöhnlichen Umständen und im Rahmen eines genehmigten Verfahrens ist dies eine schnelle Methode für einen Benutzer, auf einen Bereich zuzugreifen AWS-Konto , für den er in der Regel keine Zugriffsrechte besitzt. Weitere Informationen finden Sie unter dem Indikator Implementation break-glass procedures in den AWS Well-Architected-Leitlinien.

Brownfield-Strategie

Die bestehende Infrastruktur in Ihrer Umgebung. Wenn Sie eine Brownfield-Strategie für eine Systemarchitektur anwenden, richten Sie sich bei der Gestaltung der Architektur nach den

Einschränkungen der aktuellen Systeme und Infrastruktur. Wenn Sie die bestehende Infrastruktur erweitern, könnten Sie Brownfield- und Greenfield-Strategien mischen.

Puffer-Cache

Der Speicherbereich, in dem die am häufigsten abgerufenen Daten gespeichert werden.

Geschäftsfähigkeit

Was ein Unternehmen tut, um Wert zu generieren (z. B. Vertrieb, Kundenservice oder Marketing). Microservices-Architekturen und Entwicklungsentscheidungen können von den Geschäftskapazitäten beeinflusst werden. Weitere Informationen finden Sie im Abschnitt Organisiert nach Geschäftskapazitäten des Whitepapers Ausführen von containerisierten Microservices in AWS.

Planung der Geschäftskontinuität (BCP)

Ein Plan, der die potenziellen Auswirkungen eines störenden Ereignisses, wie z. B. einer groß angelegten Migration, auf den Betrieb berücksichtigt und es einem Unternehmen ermöglicht, den Betrieb schnell wieder aufzunehmen.

C

CAF

Weitere Informationen finden Sie unter Framework AWS für die Cloud-Einführung.

Bereitstellung auf Kanaren

Die langsame und schrittweise Veröffentlichung einer Version für Endbenutzer. Wenn Sie sich sicher sind, stellen Sie die neue Version bereit und ersetzen die aktuelle Version vollständig.

CCoE

Weitere Informationen finden Sie im Cloud Center of Excellence.

CDC

Siehe Erfassung von Änderungsdaten.

Erfassung von Datenänderungen (CDC)

Der Prozess der Nachverfolgung von Änderungen an einer Datenquelle, z. B. einer Datenbanktabelle, und der Aufzeichnung von Metadaten zu der Änderung. Sie können CDC für

verschiedene Zwecke verwenden, z. B. für die Prüfung oder Replikation von Änderungen in einem Zielsystem, um die Synchronisation aufrechtzuerhalten.

Chaos-Technik

Absichtliches Einführen von Ausfällen oder Störungsereignissen, um die Widerstandsfähigkeit eines Systems zu testen. Sie können AWS Fault Injection Service (AWS FIS) verwenden, um Experimente durchzuführen, die Ihre AWS Workloads stress, und deren Reaktion zu bewerten.

CI/CD

Siehe Continuous Integration und Continuous Delivery.

Klassifizierung

Ein Kategorisierungsprozess, der bei der Erstellung von Vorhersagen hilft. ML-Modelle für Klassifikationsprobleme sagen einen diskreten Wert voraus. Diskrete Werte unterscheiden sich immer voneinander. Beispielsweise muss ein Modell möglicherweise auswerten, ob auf einem Bild ein Auto zu sehen ist oder nicht.

clientseitige Verschlüsselung

Lokale Verschlüsselung von Daten, bevor das Ziel sie AWS-Service empfängt.

Cloud-Exzellenzzentrum (CCoE)

Ein multidisziplinäres Team, das die Cloud-Einführung in der gesamten Organisation vorantreibt, einschließlich der Entwicklung bewährter Cloud-Methoden, der Mobilisierung von Ressourcen, der Festlegung von Migrationszeitplänen und der Begleitung der Organisation durch groß angelegte Transformationen. Weitere Informationen finden Sie in den CCoE-Beiträgen im AWS Cloud Enterprise Strategy Blog.

Cloud Computing

Die Cloud-Technologie, die typischerweise für die Ferndatenspeicherung und das IoT-Gerätemanagement verwendet wird. Cloud Computing ist häufig mit Edge-Computing-Technologie verbunden.

Cloud-Betriebsmodell

In einer IT-Organisation das Betriebsmodell, das zum Aufbau, zur Weiterentwicklung und Optimierung einer oder mehrerer Cloud-Umgebungen verwendet wird. Weitere Informationen finden Sie unter Aufbau Ihres Cloud-Betriebsmodells.

Phasen der Einführung der Cloud

Die vier Phasen, die Unternehmen bei der Migration in der Regel durchlaufen AWS Cloud:

- Projekt – Durchführung einiger Cloud-bezogener Projekte zu Machbarkeitsnachweisen und zu Lernzwecken
- Fundament — Tätigen Sie grundlegende Investitionen, um Ihre Cloud-Einführung zu skalieren (z. B. Einrichtung einer landing zone, Definition eines CCo E, Einrichtung eines Betriebsmodells)
- Migration – Migrieren einzelner Anwendungen
- Neuentwicklung – Optimierung von Produkten und Services und Innovation in der Cloud

Diese Phasen wurden von Stephen Orban im Blogbeitrag The Journey Toward Cloud-First & the Stages of Adoption im AWS Cloud Enterprise Strategy-Blog definiert. Informationen darüber, wie sie mit der AWS Migrationsstrategie zusammenhängen, finden Sie im Leitfaden zur Vorbereitung der Migration.

CMDB

Siehe Datenbank für das Konfigurationsmanagement.

Code-Repository

Ein Ort, an dem Quellcode und andere Komponenten wie Dokumentation, Beispiele und Skripts gespeichert und im Rahmen von Versionskontrollprozessen aktualisiert werden. Zu den gängigen Cloud-Repositorys gehören GitHub oderBitbucket Cloud. Jede Version des Codes wird Zweig genannt. In einer Microservice-Struktur ist jedes Repository einer einzelnen Funktionalität gewidmet. Eine einzelne CI/CD-Pipeline kann mehrere Repositorien verwenden.

Kalter Cache

Ein Puffer-Cache, der leer oder nicht gut gefüllt ist oder veraltete oder irrelevante Daten enthält. Dies beeinträchtigt die Leistung, da die Datenbank-Instance aus dem Hauptspeicher oder der Festplatte lesen muss, was langsamer ist als das Lesen aus dem Puffercache.

Kalte Daten

Daten, auf die selten zugegriffen wird und die in der Regel historisch sind. Bei der Abfrage dieser Art von Daten sind langsame Abfragen in der Regel akzeptabel. Durch die Verlagerung dieser Daten auf leistungsschwächere und kostengünstigere Speicherstufen oder -klassen können Kosten gesenkt werden.

Computer Vision (CV)

Ein Bereich der KI, der maschinelles Lernen nutzt, um Informationen aus visuellen Formaten wie digitalen Bildern und Videos zu analysieren und zu extrahieren. Amazon SageMaker AI bietet beispielsweise Bildverarbeitungsalgorithmen für CV.

Drift in der Konfiguration

Bei einer Arbeitslast eine Änderung der Konfiguration gegenüber dem erwarteten Zustand. Dies kann dazu führen, dass der Workload nicht mehr richtlinienkonform wird, und zwar in der Regel schrittweise und unbeabsichtigt.

Verwaltung der Datenbankkonfiguration (CMDB)

Ein Repository, das Informationen über eine Datenbank und ihre IT-Umgebung speichert und verwaltet, inklusive Hardware- und Softwarekomponenten und deren Konfigurationen. In der Regel verwenden Sie Daten aus einer CMDB in der Phase der Portfolioerkennung und -analyse der Migration.

Konformitätspaket

Eine Sammlung von AWS Config Regeln und Abhilfemaßnahmen, die Sie zusammenstellen können, um Ihre Konformitäts- und Sicherheitsprüfungen individuell anzupassen. Mithilfe einer YAML-Vorlage können Sie ein Conformance Pack als einzelne Entität in einer AWS-Konto AND-Region oder unternehmensweit bereitstellen. Weitere Informationen finden Sie in der Dokumentation unter Conformance Packs. AWS Config

Kontinuierliche Bereitstellung und kontinuierliche Integration (CI/CD)

Der Prozess der Automatisierung der Quell-, Build-, Test-, Staging- und Produktionsphasen des Softwareveröffentlichungsprozesses. CI/CD wird allgemein als Pipeline beschrieben. CI/CD kann Ihnen helfen, Prozesse zu automatisieren, die Produktivität zu steigern, die Codequalität zu verbessern und schneller zu liefern. Weitere Informationen finden Sie unter Vorteile der kontinuierlichen Auslieferung. CD kann auch für kontinuierliche Bereitstellung stehen. Weitere Informationen finden Sie unterKontinuierliche Auslieferung im Vergleich zu kontinuierlicher Bereitstellung.

CV

Siehe Computer Vision.

D

Daten im Ruhezustand

Daten, die in Ihrem Netzwerk stationär sind, z. B. Daten, die sich im Speicher befinden.

Datenklassifizierung

Ein Prozess zur Identifizierung und Kategorisierung der Daten in Ihrem Netzwerk auf der Grundlage ihrer Kritikalität und Sensitivität. Sie ist eine wichtige Komponente jeder Strategie für das Management von Cybersecurity-Risiken, da sie Ihnen hilft, die geeigneten Schutz- und Aufbewahrungskontrollen für die Daten zu bestimmen. Die Datenklassifizierung ist ein Bestandteil der Sicherheitssäule im AWS Well-Architected Framework. Weitere Informationen finden Sie unter Datenklassifizierung.

Datendrift

Eine signifikante Abweichung zwischen den Produktionsdaten und den Daten, die zum Trainieren eines ML-Modells verwendet wurden, oder eine signifikante Änderung der Eingabedaten im Laufe der Zeit. Datendrift kann die Gesamtqualität, Genauigkeit und Fairness von ML-Modellvorhersagen beeinträchtigen.

Daten während der Übertragung

Daten, die sich aktiv durch Ihr Netzwerk bewegen, z. B. zwischen Netzwerkressourcen.

Datennetz

Ein architektonisches Framework, das verteilte, dezentrale Dateneigentum mit zentraler Verwaltung und Steuerung ermöglicht.

Datenminimierung

Das Prinzip, nur die Daten zu sammeln und zu verarbeiten, die unbedingt erforderlich sind. Durch Datenminimierung im AWS Cloud können Datenschutzrisiken, Kosten und der CO2-Fußabdruck Ihrer Analysen reduziert werden.

Datenperimeter

Eine Reihe präventiver Schutzmaßnahmen in Ihrer AWS Umgebung, mit denen sichergestellt werden kann, dass nur vertrauenswürdige Identitäten auf vertrauenswürdige Ressourcen von erwarteten Netzwerken zugreifen. Weitere Informationen finden Sie unter Aufbau eines Datenperimeters auf. AWS

Vorverarbeitung der Daten

Rohdaten in ein Format umzuwandeln, das von Ihrem ML-Modell problemlos verarbeitet werden kann. Die Vorverarbeitung von Daten kann bedeuten, dass bestimmte Spalten oder Zeilen entfernt und fehlende, inkonsistente oder doppelte Werte behoben werden.

Herkunft der Daten

Der Prozess der Nachverfolgung des Ursprungs und der Geschichte von Daten während ihres gesamten Lebenszyklus, z. B. wie die Daten generiert, übertragen und gespeichert wurden.

betroffene Person

Eine Person, deren Daten gesammelt und verarbeitet werden.

Data Warehouse

Ein Datenverwaltungssystem, das Business Intelligence wie Analysen unterstützt. Data Warehouses enthalten in der Regel große Mengen an historischen Daten und werden in der Regel für Abfragen und Analysen verwendet.

Datenbankdefinitionssprache (DDL)

Anweisungen oder Befehle zum Erstellen oder Ändern der Struktur von Tabellen und Objekten in einer Datenbank.

Datenbankmanipulationssprache (DML)

Anweisungen oder Befehle zum Ändern (Einfügen, Aktualisieren und Löschen) von Informationen in einer Datenbank.

DDL

Siehe Datenbankdefinitionssprache.

Deep-Ensemble

Mehrere Deep-Learning-Modelle zur Vorhersage kombinieren. Sie können Deep-Ensembles verwenden, um eine genauere Vorhersage zu erhalten oder um die Unsicherheit von Vorhersagen abzuschätzen.

Deep Learning

Ein ML-Teilbereich, der mehrere Schichten künstlicher neuronaler Netzwerke verwendet, um die Zuordnung zwischen Eingabedaten und Zielvariablen von Interesse zu ermitteln.

defense-in-depth

Ein Ansatz zur Informationssicherheit, bei dem eine Reihe von Sicherheitsmechanismen und -kontrollen sorgfältig in einem Computernetzwerk verteilt werden, um die Vertraulichkeit, Integrität und Verfügbarkeit des Netzwerks und der darin enthaltenen Daten zu schützen. Wenn Sie diese Strategie anwenden AWS, fügen Sie mehrere Steuerelemente auf verschiedenen Ebenen der AWS Organizations Struktur hinzu, um die Ressourcen zu schützen. Ein defense-in-depth Ansatz könnte beispielsweise Multi-Faktor-Authentifizierung, Netzwerksegmentierung und Verschlüsselung kombinieren.

delegierter Administrator

In AWS Organizations kann ein kompatibler Dienst ein AWS Mitgliedskonto registrieren, um die Konten der Organisation und die Berechtigungen für diesen Dienst zu verwalten. Dieses Konto wird als delegierter Administrator für diesen Service bezeichnet. Weitere Informationen und eine Liste kompatibler Services finden Sie unter Services, die mit AWS Organizations funktionieren in der AWS Organizations -Dokumentation.

Einsatz

Der Prozess, bei dem eine Anwendung, neue Feature oder Codekorrekturen in der Zielumgebung verfügbar gemacht werden. Die Bereitstellung umfasst das Implementieren von Änderungen an einer Codebasis und das anschließende Erstellen und Ausführen dieser Codebasis in den Anwendungsumgebungen.

Entwicklungsumgebung

Siehe Umgebung.

Detektivische Kontrolle

Eine Sicherheitskontrolle, die darauf ausgelegt ist, ein Ereignis zu erkennen, zu protokollieren und zu warnen, nachdem ein Ereignis eingetreten ist. Diese Kontrollen stellen eine zweite Verteidigungslinie dar und warnen Sie vor Sicherheitsereignissen, bei denen die vorhandenen präventiven Kontrollen umgangen wurden. Weitere Informationen finden Sie unter Detektivische Kontrolle in Implementierung von Sicherheitskontrollen in AWS.

Abbildung des Wertstroms in der Entwicklung (DVSM)

Ein Prozess zur Identifizierung und Priorisierung von Einschränkungen, die sich negativ auf Geschwindigkeit und Qualität im Lebenszyklus der Softwareentwicklung auswirken. DVSM erweitert den Prozess der Wertstromanalyse, der ursprünglich für Lean-Manufacturing-Praktiken

konzipiert wurde. Es konzentriert sich auf die Schritte und Teams, die erforderlich sind, um durch den Softwareentwicklungsprozess Mehrwert zu schaffen und zu steigern.

digitaler Zwilling

Eine virtuelle Darstellung eines realen Systems, z. B. eines Gebäudes, einer Fabrik, einer Industrieanlage oder einer Produktionslinie. Digitale Zwillinge unterstützen vorausschauende Wartung, Fernüberwachung und Produktionsoptimierung.

Maßtabelle

In einem Sternschema eine kleinere Tabelle, die Datenattribute zu quantitativen Daten in einer Faktentabelle enthält. Bei Attributen von Dimensionstabellen handelt es sich in der Regel um Textfelder oder diskrete Zahlen, die sich wie Text verhalten. Diese Attribute werden häufig zum Einschränken von Abfragen, zum Filtern und zur Kennzeichnung von Ergebnismengen verwendet.

Katastrophe

Ein Ereignis, das verhindert, dass ein Workload oder ein System seine Geschäftsziele an seinem primären Einsatzort erfüllt. Diese Ereignisse können Naturkatastrophen, technische Ausfälle oder das Ergebnis menschlichen Handelns sein, z. B. unbeabsichtigte Fehlkonfigurationen oder ein Malware-Angriff.

Disaster Recovery (DR)

Die Strategie und der Prozess, mit denen Sie Ausfallzeiten und Datenverluste aufgrund einer Katastrophe minimieren. Weitere Informationen finden Sie unter Disaster Recovery von Workloads unter AWS: Wiederherstellung in der Cloud im AWS Well-Architected Framework.

DML

Siehe Sprache zur Datenbankmanipulation.

Domainorientiertes Design

Ein Ansatz zur Entwicklung eines komplexen Softwaresystems, bei dem seine Komponenten mit sich entwickelnden Domains oder Kerngeschäftszielen verknüpft werden, denen jede Komponente dient. Dieses Konzept wurde von Eric Evans in seinem Buch Domaingesteuertes Design: Bewältigen der Komplexität im Herzen der Software (Boston: Addison-Wesley Professional, 2003) vorgestellt. Informationen darüber, wie Sie domaingesteuertes Design mit dem Strangler-Fig-Muster verwenden können, finden Sie unter Schrittweises Modernisieren älterer Microsoft ASP.NET (ASMX)-Webservices mithilfe von Containern und Amazon API Gateway.

DR

Siehe Disaster Recovery.

Erkennung von Driften

Verfolgung von Abweichungen von einer Basiskonfiguration. Sie können es beispielsweise verwenden, AWS CloudFormation um Abweichungen bei den Systemressourcen zu erkennen, oder Sie können AWS Control Tower damit Änderungen in Ihrer landing zone erkennen, die sich auf die Einhaltung von Governance-Anforderungen auswirken könnten.

DVSM

Siehe Abbildung des Wertstroms in der Entwicklung.

E

EDA

Siehe explorative Datenanalyse.

EDI

Siehe elektronischer Datenaustausch.

Edge-Computing

Die Technologie, die die Rechenleistung für intelligente Geräte an den Rändern eines IoT-Netzwerks erhöht. Im Vergleich zu Cloud Computing kann Edge Computing die Kommunikationslatenz reduzieren und die Reaktionszeit verbessern.

elektronischer Datenaustausch (EDI)

Der automatisierte Austausch von Geschäftsdokumenten zwischen Organisationen. Weitere Informationen finden Sie unter Was ist elektronischer Datenaustausch.

Verschlüsselung

Ein Rechenprozess, der Klartextdaten, die für Menschen lesbar sind, in Chiffretext umwandelt.

Verschlüsselungsschlüssel

Eine kryptografische Zeichenfolge aus zufälligen Bits, die von einem Verschlüsselungsalgorithmus generiert wird. Schlüssel können unterschiedlich lang sein, und jeder Schlüssel ist so konzipiert, dass er unvorhersehbar und einzigartig ist.

Endianismus

Die Reihenfolge, in der Bytes im Computerspeicher gespeichert werden. Big-Endian-Systeme speichern das höchstwertige Byte zuerst. Little-Endian-Systeme speichern das niedrigwertigste Byte zuerst.

Endpunkt

Siehe Service-Endpunkt.

Endpunkt-Services

Ein Service, den Sie in einer Virtual Private Cloud (VPC) hosten können, um ihn mit anderen Benutzern zu teilen. Sie können einen Endpunktdienst mit anderen AWS-Konten oder AWS Identity and Access Management (IAM AWS PrivateLink -) Prinzipalen erstellen und diesen Berechtigungen gewähren. Diese Konten oder Prinzipale können sich privat mit Ihrem Endpunktservice verbinden, indem sie Schnittstellen-VPC-Endpunkte erstellen. Weitere Informationen finden Sie unter Einen Endpunkt-Service erstellen in der Amazon Virtual Private Cloud (Amazon VPC)-Dokumentation.

Unternehmensressourcenplanung (ERP)

Ein System, das wichtige Geschäftsprozesse (wie Buchhaltung, MES und Projektmanagement) für ein Unternehmen automatisiert und verwaltet.

Envelope-Verschlüsselung

Der Prozess der Verschlüsselung eines Verschlüsselungsschlüssels mit einem anderen Verschlüsselungsschlüssel. Weitere Informationen finden Sie unter Envelope-Verschlüsselung in der AWS Key Management Service (AWS KMS) -Dokumentation.

Umgebung

Eine Instance einer laufenden Anwendung. Die folgenden Arten von Umgebungen sind beim Cloud-Computing üblich:

- Entwicklungsumgebung – Eine Instance einer laufenden Anwendung, die nur dem Kernteam zur Verfügung steht, das für die Wartung der Anwendung verantwortlich ist. Entwicklungsumgebungen werden verwendet, um Änderungen zu testen, bevor sie in höhere Umgebungen übertragen werden. Diese Art von Umgebung wird manchmal als Testumgebung bezeichnet.
- Niedrigere Umgebungen – Alle Entwicklungsumgebungen für eine Anwendung, z. B. solche, die für erste Builds und Tests verwendet wurden.

- Produktionsumgebung – Eine Instance einer laufenden Anwendung, auf die Endbenutzer zugreifen können. In einer CI/CD Pipeline ist die Produktionsumgebung die letzte Bereitstellungsumgebung.
- Höhere Umgebungen – Alle Umgebungen, auf die auch andere Benutzer als das Kernentwicklungsteam zugreifen können. Dies kann eine Produktionsumgebung, Vorproduktionsumgebungen und Umgebungen für Benutzerakzeptanztests umfassen.

Epics

In der agilen Methodik sind dies funktionale Kategorien, die Ihnen helfen, Ihre Arbeit zu organisieren und zu priorisieren. Epics bieten eine allgemeine Beschreibung der Anforderungen und Implementierungsaufgaben. Zu den Sicherheitsepen AWS von CAF gehören beispielsweise Identitäts- und Zugriffsmanagement, Detektivkontrollen, Infrastruktursicherheit, Datenschutz und Reaktion auf Vorfälle. Weitere Informationen zu Epics in der AWS -Migrationsstrategie finden Sie im Leitfaden zur Programm-Implementierung.

ERP

Siehe Enterprise Resource Planning.

Explorative Datenanalyse (EDA)

Der Prozess der Analyse eines Datensatzes, um seine Hauptmerkmale zu verstehen. Sie sammeln oder aggregieren Daten und führen dann erste Untersuchungen durch, um Muster zu finden, Anomalien zu erkennen und Annahmen zu überprüfen. EDA wird durchgeführt, indem zusammenfassende Statistiken berechnet und Datenvisualisierungen erstellt werden.

F

Faktentabelle

Die zentrale Tabelle in einem Sternschema. Sie speichert quantitative Daten über den Geschäftsbetrieb. In der Regel enthält eine Faktentabelle zwei Arten von Spalten: Spalten, die Kennzahlen enthalten, und Spalten, die einen Fremdschlüssel für eine Dimensionstabelle enthalten.

schnell scheitern

Eine Philosophie, die häufige und inkrementelle Tests verwendet, um den Entwicklungslebenszyklus zu verkürzen. Dies ist ein wichtiger Bestandteil eines agilen Ansatzes.

Grenze zur Fehlerisolierung

Dabei handelt es sich um eine Grenze AWS Cloud, z. B. eine Availability Zone AWS-Region, eine Steuerungsebene oder eine Datenebene, die die Auswirkungen eines Fehlers begrenzt und die Widerstandsfähigkeit von Workloads verbessert. Weitere Informationen finden Sie unter Grenzen zur AWS Fehlerisolierung.

Feature-Zweig

Siehe Zweig.

Features

Die Eingabedaten, die Sie verwenden, um eine Vorhersage zu treffen. In einem Fertigungskontext könnten Feature beispielsweise Bilder sein, die regelmäßig von der Fertigungslinie aus aufgenommen werden.

Bedeutung der Feature

Wie wichtig ein Feature für die Vorhersagen eines Modells ist. Dies wird in der Regel als numerischer Wert ausgedrückt, der mit verschiedenen Techniken wie Shapley Additive Explanations (SHAP) und integrierten Gradienten berechnet werden kann. Weitere Informationen finden Sie unter Interpretierbarkeit von Modellen für maschinelles Lernen mit AWS.

Featuretransformation

Daten für den ML-Prozess optimieren, einschließlich der Anreicherung von Daten mit zusätzlichen Quellen, der Skalierung von Werten oder der Extraktion mehrerer Informationssätze aus einem einzigen Datenfeld. Das ermöglicht dem ML-Modell, von den Daten profitieren. Wenn Sie beispielsweise das Datum „27.05.2021 00:15:37“ in „2021“, „Mai“, „Donnerstag“ und „15“ aufschlüsseln, können Sie dem Lernalgorithmus helfen, nuancierte Muster zu erlernen, die mit verschiedenen Datenkomponenten verknüpft sind.

Eingabeaufforderung mit wenigen Klicks

Bereitstellung einer kleinen Anzahl von Beispielen, die die Aufgabe und das gewünschte Ergebnis veranschaulichen, bevor das LLM aufgefordert wird, eine ähnliche Aufgabe auszuführen. Bei dieser Technik handelt es sich um eine Anwendung des kontextbezogenen Lernens, bei der Modelle anhand von Beispielen (Aufnahmen) lernen, die in Eingabeaufforderungen eingebettet sind. Bei Aufgaben, die spezifische Formatierungs-, Argumentations- oder Fachkenntnisse erfordern, kann die Eingabeaufforderung mit wenigen Handgriffen effektiv sein. Siehe auch Zero-Shot Prompting.

FGAC

Siehe detaillierte Zugriffskontrolle.

Feinkörnige Zugriffskontrolle (FGAC)

Die Verwendung mehrerer Bedingungen, um eine Zugriffsanfrage zuzulassen oder abzulehnen.

Flash-Cut-Migration

Eine Datenbankmigrationsmethode, bei der eine kontinuierliche Datenreplikation durch Erfassung von Änderungsdaten verwendet wird, um Daten in kürzester Zeit zu migrieren, anstatt einen schrittweisen Ansatz zu verwenden. Ziel ist es, Ausfallzeiten auf ein Minimum zu beschränken.

FM

Siehe Fundamentmodell.

Fundamentmodell (FM)

Ein großes neuronales Deep-Learning-Netzwerk, das mit riesigen Datensätzen generalisierter und unbeschrifteter Daten trainiert wurde. FMs sind in der Lage, eine Vielzahl allgemeiner Aufgaben zu erfüllen, z. B. Sprache zu verstehen, Text und Bilder zu generieren und Konversationen in natürlicher Sprache zu führen. Weitere Informationen finden Sie unter Was sind Foundation-Modelle.

G

Generative KI

Eine Untergruppe von KI-Modellen, die mit großen Datenmengen trainiert wurden und mit einer einfachen Textaufforderung neue Inhalte und Artefakte wie Bilder, Videos, Text und Audio erstellen können. Weitere Informationen finden Sie unter Was ist Generative KI.

Geoblocking

Siehe geografische Einschränkungen.

Geografische Einschränkungen (Geoblocking)

Bei Amazon eine Option CloudFront, um zu verhindern, dass Benutzer in bestimmten Ländern auf Inhaltsverteilungen zugreifen. Sie können eine Zulassungsliste oder eine Sperrliste verwenden,

um zugelassene und gesperrte Länder anzugeben. Weitere Informationen finden Sie in der Dokumentation unter Beschränkung der geografischen Verteilung Ihrer Inhalte. CloudFront

Gitflow-Workflow

Ein Ansatz, bei dem niedrigere und höhere Umgebungen unterschiedliche Zweige in einem Quellcode-Repository verwenden. Der Gitflow-Workflow gilt als veraltet, und der Trunk-basierte Workflow ist der moderne, bevorzugte Ansatz.

goldenes Bild

Ein Snapshot eines Systems oder einer Software, der als Vorlage für die Bereitstellung neuer Instanzen dieses Systems oder dieser Software verwendet wird. In der Fertigung kann ein Golden Image beispielsweise zur Bereitstellung von Software auf mehreren Geräten verwendet werden und trägt zur Verbesserung der Geschwindigkeit, Skalierbarkeit und Produktivität bei der Geräteherstellung bei.

Greenfield-Strategie

Das Fehlen vorhandener Infrastruktur in einer neuen Umgebung. Bei der Einführung einer Neuausrichtung einer Systemarchitektur können Sie alle neuen Technologien ohne Einschränkung der Kompatibilität mit der vorhandenen Infrastruktur auswählen, auch bekannt als Brownfield. Wenn Sie die bestehende Infrastruktur erweitern, könnten Sie Brownfield- und Greenfield-Strategien mischen.

Integritätsschutz

Eine allgemeine Regel, die dazu beiträgt, Ressourcen, Richtlinien und die Einhaltung von Vorschriften in allen Unternehmenseinheiten zu regeln (OUs). Präventiver Integritätsschutz setzt Richtlinien durch, um die Einhaltung von Standards zu gewährleisten. Sie werden mithilfe von Service-Kontrollrichtlinien und IAM-Berechtigungsgrenzen implementiert. Detektivischer Integritätsschutz erkennt Richtlinienverstöße und Compliance-Probleme und generiert Warnmeldungen zur Abhilfe. Sie werden mithilfe von AWS Config, AWS Security Hub CSPM, Amazon GuardDuty AWS Trusted Advisor, Amazon Inspector und benutzerdefinierten AWS Lambda Prüfungen implementiert.

H

HEKTAR

Siehe Hochverfügbarkeit.

Heterogene Datenbankmigration

Migrieren Sie Ihre Quelldatenbank in eine Zieldatenbank, die eine andere Datenbank-Engine verwendet (z. B. Oracle zu Amazon Aurora). Eine heterogene Migration ist in der Regel Teil einer Neuarchitektur, und die Konvertierung des Schemas kann eine komplexe Aufgabe sein. AWS bietet AWS SCT, welches bei Schemakonvertierungen hilft.

hohe Verfügbarkeit (HA)

Die Fähigkeit eines Workloads, im Falle von Herausforderungen oder Katastrophen kontinuierlich und ohne Eingreifen zu arbeiten. HA-Systeme sind so konzipiert, dass sie automatisch ein Failover durchführen, gleichbleibend hohe Leistung bieten und unterschiedliche Lasten und Ausfälle mit minimalen Leistungseinbußen bewältigen.

historische Modernisierung

Ein Ansatz zur Modernisierung und Aufrüstung von Betriebstechnologiesystemen (OT), um den Bedürfnissen der Fertigungsindustrie besser gerecht zu werden. Ein Historian ist eine Art von Datenbank, die verwendet wird, um Daten aus verschiedenen Quellen in einer Fabrik zu sammeln und zu speichern.

Daten zurückhalten

Ein Teil historischer, beschrifteter Daten, der aus einem Datensatz zurückgehalten wird, der zum Trainieren eines Modells für maschinelles Lernen verwendet wird. Sie können Holdout-Daten verwenden, um die Modellleistung zu bewerten, indem Sie die Modellvorhersagen mit den Holdout-Daten vergleichen.

Homogene Datenbankmigration

Migrieren Sie Ihre Quelldatenbank zu einer Zieldatenbank, die dieselbe Datenbank-Engine verwendet (z. B. Microsoft SQL Server zu Amazon RDS für SQL Server). Eine homogene Migration ist in der Regel Teil eines Hostwechsels oder eines Plattformwechsels. Sie können native Datenbankserviceprogramme verwenden, um das Schema zu migrieren.

heiße Daten

Daten, auf die häufig zugegriffen wird, z. B. Echtzeitdaten oder aktuelle Translationsdaten. Für diese Daten ist in der Regel eine leistungsstarke Speicherebene oder -klasse erforderlich, um schnelle Abfrageantworten zu ermöglichen.

Hotfix

Eine dringende Lösung für ein kritisches Problem in einer Produktionsumgebung. Aufgrund seiner Dringlichkeit wird ein Hotfix normalerweise außerhalb des typischen DevOps Release-Workflows erstellt.

Hypercare-Phase

Unmittelbar nach dem Cutover, der Zeitraum, in dem ein Migrationsteam die migrierten Anwendungen in der Cloud verwaltet und überwacht, um etwaige Probleme zu beheben. In der Regel dauert dieser Zeitraum 1–4 Tage. Am Ende der Hypercare-Phase überträgt das Migrationsteam in der Regel die Verantwortung für die Anwendungen an das Cloud-Betriebsteam.

I

IaC

Sehen Sie Infrastruktur als Code.

Identitätsbasierte Richtlinie

Eine Richtlinie, die einem oder mehreren IAM-Prinzipalen zugeordnet ist und deren Berechtigungen innerhalb der AWS Cloud Umgebung definiert.

Leerlaufanwendung

Eine Anwendung mit einer durchschnittlichen CPU- und Arbeitsspeicherauslastung zwischen 5 und 20 Prozent über einen Zeitraum von 90 Tagen. In einem Migrationsprojekt ist es üblich, diese Anwendungen außer Betrieb zu nehmen oder sie On-Premises beizubehalten.

IIoT

Siehe Industrielles Internet der Dinge.

unveränderliche Infrastruktur

Ein Modell, das eine neue Infrastruktur für Produktionsworkloads bereitstellt, anstatt die bestehende Infrastruktur zu aktualisieren, zu patchen oder zu modifizieren. Unveränderliche Infrastrukturen sind von Natur aus konsistenter, zuverlässiger und vorhersehbarer als veränderliche Infrastrukturen. Weitere Informationen finden Sie in der Best Practice Deploy using immutable infrastructure im AWS Well-Architected Framework.

Eingehende (ingress) VPC

In einer Architektur AWS mit mehreren Konten ist dies eine VPC, die Netzwerkverbindungen von außerhalb einer Anwendung akzeptiert, überprüft und weiterleitet. Die AWS Security Reference Architecture empfiehlt, Ihr Netzwerkkonto mit eingehendem und ausgehendem Datenverkehr und Inspektion einzurichten, VPCs um die bidirektionale Schnittstelle zwischen Ihrer Anwendung und dem Internet im weiteren Sinne zu schützen.

Inkrementelle Migration

Eine Cutover-Strategie, bei der Sie Ihre Anwendung in kleinen Teilen migrieren, anstatt eine einziges vollständiges Cutover durchzuführen. Beispielsweise könnten Sie zunächst nur einige Microservices oder Benutzer auf das neue System umstellen. Nachdem Sie sich vergewissert haben, dass alles ordnungsgemäß funktioniert, können Sie weitere Microservices oder Benutzer schrittweise verschieben, bis Sie Ihr Legacy-System außer Betrieb nehmen können. Diese Strategie reduziert die mit großen Migrationen verbundenen Risiken.

Industrie 4.0

Ein Begriff, der 2016 von Klaus Schwab eingeführt wurde und sich auf die Modernisierung von Fertigungsprozessen durch Fortschritte in den Bereichen Konnektivität, Echtzeitdaten, Automatisierung, Analytik und KI/ML bezieht.

Infrastruktur

Alle Ressourcen und Komponenten, die in der Umgebung einer Anwendung enthalten sind.

Infrastructure as Code (IaC)

Der Prozess der Bereitstellung und Verwaltung der Infrastruktur einer Anwendung mithilfe einer Reihe von Konfigurationsdateien. IaC soll Ihnen helfen, das Infrastrukturmanagement zu zentralisieren, Ressourcen zu standardisieren und schnell zu skalieren, sodass neue Umgebungen wiederholbar, zuverlässig und konsistent sind.

industrielles Internet der Dinge (T) IIo

Einsatz von mit dem Internet verbundenen Sensoren und Geräten in Industriesektoren wie Fertigung, Energie, Automobilindustrie, Gesundheitswesen, Biowissenschaften und Landwirtschaft. Weitere Informationen finden Sie unter Aufbau einer digitalen Transformationsstrategie für das industrielle Internet der Dinge (IIoT).

Inspektions-VPC

In einer Architektur AWS mit mehreren Konten eine zentralisierte VPC, die Inspektionen des Netzwerkverkehrs zwischen VPCs (in demselben oder unterschiedlichen AWS-Regionen), dem Internet und lokalen Netzwerken verwaltet. In der AWS Security Reference Architecture wird empfohlen, Ihr Netzwerkkonto mit eingehendem und ausgehendem Datenverkehr sowie Inspektionen einzurichten, VPCs um die bidirektionale Schnittstelle zwischen Ihrer Anwendung und dem Internet im weiteren Sinne zu schützen.

Internet of Things (IoT)

Das Netzwerk verbundener physischer Objekte mit eingebetteten Sensoren oder Prozessoren, das über das Internet oder über ein lokales Kommunikationsnetzwerk mit anderen Geräten und Systemen kommuniziert. Weitere Informationen finden Sie unter Was ist IoT?

Interpretierbarkeit

Ein Merkmal eines Modells für Machine Learning, das beschreibt, inwieweit ein Mensch verstehen kann, wie die Vorhersagen des Modells von seinen Eingaben abhängen. Weitere Informationen finden Sie unter Interpretierbarkeit des Modells für maschinelles Lernen mit. AWS

IoT

Siehe Internet der Dinge.

IT information library (ITIL, IT-Informationsbibliothek)

Eine Reihe von bewährten Methoden für die Bereitstellung von IT-Services und die Abstimmung dieser Services auf die Geschäftsanforderungen. ITIL bietet die Grundlage für ITSM.

T service management (ITSM, IT-Servicemanagement)

Aktivitäten im Zusammenhang mit der Gestaltung, Implementierung, Verwaltung und Unterstützung von IT-Services für eine Organisation. Informationen zur Integration von Cloud-Vorgängen mit ITSM-Tools finden Sie im Leitfaden zur Betriebsintegration.

BIS

Siehe IT-Informationsbibliothek.

ITSM

Siehe IT-Servicemanagement.

L

Labelbasierte Zugangskontrolle (LBAC)

: Eine Implementierung der Mandatory Access Control (MAC), bei der den Benutzern und den Daten selbst jeweils explizit ein Sicherheitslabelwert zugewiesen wird. Die Schnittmenge zwischen der Benutzersicherheitsbeschriftung und der Datensicherheitsbeschriftung bestimmt, welche Zeilen und Spalten für den Benutzer sichtbar sind.

Landing Zone

: Eine landing zone ist eine gut strukturierte AWS Umgebung mit mehreren Konten, die skalierbar und sicher ist. Dies ist ein Ausgangspunkt, von dem aus Ihre Organisationen Workloads und Anwendungen schnell und mit Vertrauen in ihre Sicherheits- und Infrastrukturumgebung starten und bereitstellen können. Weitere Informationen zu Landing Zones finden Sie unter Einrichtung einer sicheren und skalierbaren AWS -Umgebung mit mehreren Konten..

großes Sprachmodell (LLM)

: Ein Deep-Learning-KI-Modell, das anhand einer riesigen Datenmenge vorab trainiert wurde. Ein LLM kann mehrere Aufgaben ausführen, z. B. Fragen beantworten, Dokumente zusammenfassen, Text in andere Sprachen übersetzen und Sätze vervollständigen. Weitere Informationen finden Sie unter Was sind. LLMs

Große Migration

: Eine Migration von 300 oder mehr Servern.

SCHWARZ

: Siehe Labelbasierte Zugriffskontrolle.

Geringste Berechtigung

: Die bewährte Sicherheitsmethode, bei der nur die für die Durchführung einer Aufgabe erforderlichen Mindestberechtigungen erteilt werden. Weitere Informationen finden Sie unter Geringste Berechtigungen anwenden in der IAM-Dokumentation.

Lift and Shift

: Siehe 7 Rs.

Little-Endian-System

: Ein System, welches das niedrigwertigste Byte zuerst speichert. Siehe auch Endianness.

LLM

Siehe großes Sprachmodell.

Niedrigere Umgebungen

Siehe Umgebung.

M

Machine Learning (ML)

Eine Art künstlicher Intelligenz, die Algorithmen und Techniken zur Mustererkennung und zum Lernen verwendet. ML analysiert aufgezeichnete Daten, wie z. B. Daten aus dem Internet der Dinge (IoT), und lernt daraus, um ein statistisches Modell auf der Grundlage von Mustern zu erstellen. Weitere Informationen finden Sie unter Machine Learning.

Hauptzweig

Siehe Filiale.

Malware

Software, die entwickelt wurde, um die Computersicherheit oder den Datenschutz zu gefährden. Malware kann Computersysteme stören, vertrauliche Informationen durchsickern lassen oder sich unbefugten Zugriff verschaffen. Beispiele für Malware sind Viren, Würmer, Ransomware, Trojaner, Spyware und Keylogger.

verwaltete Dienste

AWS-Services für die die Infrastrukturebene, das Betriebssystem und die Plattformen AWS betrieben werden, und Sie greifen auf die Endgeräte zu, um Daten zu speichern und abzurufen. Amazon Simple Storage Service (Amazon S3) und Amazon DynamoDB sind Beispiele für Managed Services. Diese werden auch als abstrakte Dienste bezeichnet.

Manufacturing Execution System (MES)

Ein Softwaresystem zur Nachverfolgung, Überwachung, Dokumentation und Steuerung von Produktionsprozessen, bei denen Rohstoffe in der Fertigung zu fertigen Produkten umgewandelt werden.

MAP

Siehe Migration Acceleration Program.

Mechanismus

Ein vollständiger Prozess, bei dem Sie ein Tool erstellen, die Akzeptanz des Tools vorantreiben und anschließend die Ergebnisse überprüfen, um Anpassungen vorzunehmen. Ein Mechanismus ist ein Zyklus, der sich im Laufe seiner Tätigkeit selbst verstärkt und verbessert. Weitere Informationen finden Sie unter Aufbau von Mechanismen im AWS Well-Architected Framework.

Mitgliedskonto

Alle AWS-Konten außer dem Verwaltungskonto, die Teil einer Organisation in sind. AWS Organizations Ein Konto kann jeweils nur Mitglied einer Organisation sein.

MES

Siehe Manufacturing Execution System.

Message Queuing-Telemetrietransport (MQTT)

Ein leichtes machine-to-machine (M2M) -Kommunikationsprotokoll, das auf dem Publish/Subscribe-Muster für IoT-Geräte mit beschränkten Ressourcen basiert.

Microservice

Ein kleiner, unabhängiger Dienst, der über genau definierte Kanäle kommuniziert APIs und in der Regel kleinen, eigenständigen Teams gehört. Ein Versicherungssystem kann beispielsweise Microservices beinhalten, die Geschäftsfunktionen wie Vertrieb oder Marketing oder Subdomains wie Einkauf, Schadenersatz oder Analytik zugeordnet sind. Zu den Vorteilen von Microservices gehören Agilität, flexible Skalierung, einfache Bereitstellung, wiederverwendbarer Code und Ausfallsicherheit. Weitere Informationen finden Sie unter Integration von Microservices mithilfe serverloser Dienste. AWS

Microservices-Architekturen

Ein Ansatz zur Erstellung einer Anwendung mit unabhängigen Komponenten, die jeden Anwendungsprozess als Microservice ausführen. Diese Microservices kommunizieren mithilfe von Lightweight über eine klar definierte Schnittstelle. APIs Jeder Microservice in dieser Architektur kann aktualisiert, bereitgestellt und skaliert werden, um den Bedarf an bestimmten Funktionen einer Anwendung zu decken. Weitere Informationen finden Sie unter Implementieren von Microservices auf. AWS

Migration Acceleration Program (MAP)

Ein AWS Programm, das Beratung, Unterstützung, Schulungen und Services bietet, um Unternehmen dabei zu unterstützen, eine solide betriebliche Grundlage für die Umstellung auf

die Cloud zu schaffen und die anfänglichen Kosten von Migrationen auszugleichen. MAP umfasst eine Migrationsmethode für die methodische Durchführung von Legacy-Migrationen sowie eine Reihe von Tools zur Automatisierung und Beschleunigung gängiger Migrationsszenarien.

Migration in großem Maßstab

Der Prozess, bei dem der Großteil des Anwendungsportfolios in Wellen in die Cloud verlagert wird, wobei in jeder Welle mehr Anwendungen schneller migriert werden. In dieser Phase werden die bewährten Verfahren und Erkenntnisse aus den früheren Phasen zur Implementierung einer Migrationsfabrik von Teams, Tools und Prozessen zur Optimierung der Migration von Workloads durch Automatisierung und agile Bereitstellung verwendet. Dies ist die dritte Phase der AWS - Migrationsstrategie.

Migrationsfabrik

Funktionsübergreifende Teams, die die Migration von Workloads durch automatisierte, agile Ansätze optimieren. Zu den Teams in der Migrationsabteilung gehören in der Regel Betriebsabläufe, Geschäftsanalysten und Eigentümer, Migrationsingenieure, Entwickler und DevOps Experten, die in Sprints arbeiten. Zwischen 20 und 50 Prozent eines Unternehmensanwendungsportfolios bestehen aus sich wiederholenden Mustern, die durch einen Fabrik-Ansatz optimiert werden können. Weitere Informationen finden Sie in Diskussion über Migrationsfabriken und den Leitfaden zur Cloud-Migration-Fabrik in diesem Inhaltssatz.

Migrationsmetadaten

Die Informationen über die Anwendung und den Server, die für den Abschluss der Migration benötigt werden. Für jedes Migrationsmuster ist ein anderer Satz von Migrationsmetadaten erforderlich. Beispiele für Migrationsmetadaten sind das Zielsubnetz, die Sicherheitsgruppe und AWS das Konto.

Migrationsmuster

Eine wiederholbare Migrationsaufgabe, in der die Migrationsstrategie, das Migrationsziel und die verwendete Migrationsanwendung oder der verwendete Migrationsservice detailliert beschrieben werden. Beispiel: Rehost-Migration zu Amazon EC2 mit AWS Application Migration Service.

Migration Portfolio Assessment (MPA)

Ein Online-Tool, das Informationen zur Validierung des Geschäftsszenarios für die Migration auf das bereitstellt. AWS Cloud MPA bietet eine detaillierte Portfoliobewertung (richtige Servergröße, Preisgestaltung, Gesamtbetriebskostenanalyse, Migrationskostenanalyse) sowie Migrationsplanung (Anwendungsdatenanalyse und Datenerfassung, Anwendungsgruppierung,

Migrationspriorisierung und Wellenplanung). Das MPA-Tool (Anmeldung erforderlich) steht allen AWS Beratern und APN-Partnerberatern kostenlos zur Verfügung.

Migration Readiness Assessment (MRA)

Der Prozess, bei dem mithilfe des AWS CAF Erkenntnisse über den Cloud-Bereitschaftsstatus eines Unternehmens gewonnen, Stärken und Schwächen identifiziert und ein Aktionsplan zur Schließung festgestellter Lücken erstellt wird. Weitere Informationen finden Sie im Benutzerhandbuch für Migration Readiness. MRA ist die erste Phase der AWS - Migrationsstrategie.

Migrationsstrategie

Der Ansatz, der verwendet wurde, um einen Workload auf den AWS Cloud zu migrieren. Weitere Informationen finden Sie im Eintrag 7 Rs in diesem Glossar und unter Mobilisieren Sie Ihr Unternehmen, um umfangreiche Migrationen zu beschleunigen.

ML

Siehe maschinelles Lernen.

Modernisierung

Umwandlung einer veralteten (veralteten oder monolithischen) Anwendung und ihrer Infrastruktur in ein agiles, elastisches und hochverfügbares System in der Cloud, um Kosten zu senken, die Effizienz zu steigern und Innovationen zu nutzen. Weitere Informationen finden Sie unter Strategie zur Modernisierung von Anwendungen in der AWS Cloud.

Bewertung der Modernisierungsfähigkeit

Eine Bewertung, anhand derer festgestellt werden kann, ob die Anwendungen einer Organisation für die Modernisierung bereit sind, Vorteile, Risiken und Abhängigkeiten identifiziert und ermittelt wird, wie gut die Organisation den zukünftigen Status dieser Anwendungen unterstützen kann. Das Ergebnis der Bewertung ist eine Vorlage der Zielarchitektur, eine Roadmap, in der die Entwicklungsphasen und Meilensteine des Modernisierungsprozesses detailliert beschrieben werden, sowie ein Aktionsplan zur Behebung festgestellter Lücken. Weitere Informationen finden Sie unter Evaluierung der Modernisierungsbereitschaft von Anwendungen in der AWS Cloud.

Monolithische Anwendungen (Monolithen)

Anwendungen, die als ein einziger Service mit eng gekoppelten Prozessen ausgeführt werden. Monolithische Anwendungen haben verschiedene Nachteile. Wenn ein Anwendungs-Feature stark nachgefragt wird, muss die gesamte Architektur skaliert werden. Das Hinzufügen oder

Verbessern der Feature einer monolithischen Anwendung wird ebenfalls komplexer, wenn die Codebasis wächst. Um diese Probleme zu beheben, können Sie eine Microservices-Architektur verwenden. Weitere Informationen finden Sie unter Zerlegen von Monolithen in Microservices.

MPA

Siehe Bewertung des Migrationsportfolios.

MQTT

Siehe Message Queuing-Telemetrietransport.

Mehrklassen-Klassifizierung

Ein Prozess, der dabei hilft, Vorhersagen für mehrere Klassen zu generieren (wobei eines von mehr als zwei Ergebnissen vorhergesagt wird). Ein ML-Modell könnte beispielsweise fragen: „Ist dieses Produkt ein Buch, ein Auto oder ein Telefon?“ oder „Welche Kategorie von Produkten ist für diesen Kunden am interessantesten?“

veränderbare Infrastruktur

Ein Modell, das die bestehende Infrastruktur für Produktionsworkloads aktualisiert und modifiziert. Für eine verbesserte Konsistenz, Zuverlässigkeit und Vorhersagbarkeit empfiehlt das AWS Well-Architected Framework die Verwendung einer unveränderlichen Infrastruktur als bewährte Methode.

O

OAC

Weitere Informationen finden Sie unter Origin Access Control.

EICHE

Siehe Zugriffsidentität von Origin.

COM

Siehe organisatorisches Change-Management.

Offline-Migration

Eine Migrationsmethode, bei der der Quell-Workload während des Migrationsprozesses heruntergefahren wird. Diese Methode ist mit längeren Ausfallzeiten verbunden und wird in der Regel für kleine, unkritische Workloads verwendet.

OI

Siehe Betriebsintegration.

OLA

Siehe Vereinbarung auf operativer Ebene.

Online-Migration

Eine Migrationsmethode, bei der der Quell-Workload auf das Zielsystem kopiert wird, ohne offline genommen zu werden. Anwendungen, die mit dem Workload verbunden sind, können während der Migration weiterhin funktionieren. Diese Methode beinhaltet keine bis minimale Ausfallzeit und wird in der Regel für kritische Produktionsworkloads verwendet.

OPC-UA

Siehe Open Process Communications — Unified Architecture.

Offene Prozesskommunikation — Einheitliche Architektur (OPC-UA)

Ein machine-to-machine (M2M) -Kommunikationsprotokoll für die industrielle Automatisierung. OPC-UA bietet einen Interoperabilitätsstandard mit Datenverschlüsselungs-, Authentifizierungs- und Autorisierungsschemata.

Vereinbarung auf Betriebsebene (OLA)

Eine Vereinbarung, in der klargestellt wird, welche funktionalen IT-Gruppen sich gegenseitig versprechen zu liefern, um ein Service Level Agreement (SLA) zu unterstützen.

Überprüfung der Betriebsbereitschaft (ORR)

Eine Checkliste mit Fragen und zugehörigen bewährten Methoden, die Ihnen helfen, Vorfälle und mögliche Ausfälle zu verstehen, zu bewerten, zu verhindern oder deren Umfang zu reduzieren. Weitere Informationen finden Sie unter Operational Readiness Reviews (ORR) im AWS Well-Architected Framework.

Betriebstechnologie (OT)

Hardware- und Softwaresysteme, die mit der physischen Umgebung zusammenarbeiten, um industrielle Abläufe, Ausrüstung und Infrastruktur zu steuern. In der Fertigung ist die Integration von OT- und Informationstechnologie (IT) -Systemen ein zentraler Schwerpunkt der Industrie 4.0-Transformationen.

Betriebsintegration (OI)

Der Prozess der Modernisierung von Abläufen in der Cloud, der Bereitschaftsplanung, Automatisierung und Integration umfasst. Weitere Informationen finden Sie im Leitfaden zur Betriebsintegration.

Organisationspfad

Ein Pfad, der von erstellt wird und in AWS CloudTrail dem alle Ereignisse für alle AWS-Konten in einer Organisation protokolliert werden. AWS Organizations Diese Spur wird in jedem AWS-Konto , der Teil der Organisation ist, erstellt und verfolgt die Aktivität in jedem Konto. Weitere Informationen finden Sie in der CloudTrail Dokumentation unter Erstellen eines Pfads für eine Organisation.

Organisatorisches Veränderungsmanagement (OCM)

Ein Framework für das Management wichtiger, disruptiver Geschäftstransformationen aus Sicht der Mitarbeiter, der Kultur und der Führung. OCM hilft Organisationen dabei, sich auf neue Systeme und Strategien vorzubereiten und auf diese umzustellen, indem es die Akzeptanz von Veränderungen beschleunigt, Übergangsprobleme angeht und kulturelle und organisatorische Veränderungen vorantreibt. In der AWS Migrationsstrategie wird dieses Framework aufgrund der Geschwindigkeit des Wandels, der bei Projekten zur Cloud-Einführung erforderlich ist, als Mitarbeiterbeschleunigung bezeichnet. Weitere Informationen finden Sie im OCM-Handbuch.

Ursprungszugriffskontrolle (OAC)

In CloudFront, eine erweiterte Option zur Zugriffsbeschränkung, um Ihre Amazon Simple Storage Service (Amazon S3) -Inhalte zu sichern. OAC unterstützt alle S3-Buckets insgesamt AWS-Regionen, serverseitige Verschlüsselung mit AWS KMS (SSE-KMS) sowie dynamische `PUT` und `DELETE` Anfragen an den S3-Bucket.

Ursprungszugriffsidentität (OAI)

In CloudFront, eine Option zur Zugriffsbeschränkung, um Ihre Amazon S3 S3-Inhalte zu sichern. Wenn Sie OAI verwenden, CloudFront erstellt es einen Principal, mit dem sich Amazon S3 authentifizieren kann. Authentifizierte Principals können nur über eine bestimmte Distribution auf Inhalte in einem S3-Bucket zugreifen. CloudFront Siehe auch OAC, das eine detailliertere und verbesserte Zugriffskontrolle bietet.

ORR

Weitere Informationen finden Sie unter Überprüfung der Betriebsbereitschaft.

NICHT

Siehe Betriebstechnologie.

Ausgehende (egress) VPC

In einer Architektur AWS mit mehreren Konten eine VPC, die Netzwerkverbindungen verarbeitet, die von einer Anwendung aus initiiert werden. Die AWS Security Reference Architecture empfiehlt die Einrichtung Ihres Netzwerkkontos mit eingehendem und ausgehendem Datenverkehr sowie Inspektion, VPCs um die bidirektionale Schnittstelle zwischen Ihrer Anwendung und dem Internet im weiteren Sinne zu schützen.

P

Berechtigungsgrenze

Eine IAM-Verwaltungsrichtlinie, die den IAM-Prinzipalen zugeordnet ist, um die maximalen Berechtigungen festzulegen, die der Benutzer oder die Rolle haben kann. Weitere Informationen finden Sie unter Berechtigungsgrenzen für IAM-Entitys in der IAM-Dokumentation.

persönlich identifizierbare Informationen (PII)

Informationen, die, wenn sie direkt betrachtet oder mit anderen verwandten Daten kombiniert werden, verwendet werden können, um vernünftige Rückschlüsse auf die Identität einer Person zu ziehen. Beispiele für personenbezogene Daten sind Namen, Adressen und Kontaktinformationen.

Personenbezogene Daten

Siehe persönlich identifizierbare Informationen.

Playbook

Eine Reihe vordefinierter Schritte, die die mit Migrationen verbundenen Aufgaben erfassen, z. B. die Bereitstellung zentraler Betriebsfunktionen in der Cloud. Ein Playbook kann die Form von Skripten, automatisierten Runbooks oder einer Zusammenfassung der Prozesse oder Schritte annehmen, die für den Betrieb Ihrer modernisierten Umgebung erforderlich sind.

PLC

Siehe programmierbare Logiksteuerung.

PLM

Siehe Produktlebenszyklusmanagement.

policy

Ein Objekt, das Berechtigungen definieren (siehe identitätsbasierte Richtlinie), Zugriffsbedingungen spezifizieren (siehe ressourcenbasierte Richtlinie) oder die maximalen Berechtigungen für alle Konten in einer Organisation definieren kann AWS Organizations (siehe Dienststeuerungsrichtlinie).

Polyglotte Beharrlichkeit

Unabhängige Auswahl der Datenspeichertechnologie eines Microservices auf der Grundlage von Datenzugriffsmustern und anderen Anforderungen. Wenn Ihre Microservices über dieselbe Datenspeichertechnologie verfügen, kann dies zu Implementierungsproblemen oder zu Leistungseinbußen führen. Microservices lassen sich leichter implementieren und erzielen eine bessere Leistung und Skalierbarkeit, wenn sie den Datenspeicher verwenden, der ihren Anforderungen am besten entspricht. Weitere Informationen finden Sie unter Datenpersistenz in Microservices aktivieren.

Portfoliobewertung

Ein Prozess, bei dem das Anwendungsportfolio ermittelt, analysiert und priorisiert wird, um die Migration zu planen. Weitere Informationen finden Sie in Bewerten der Migrationsbereitschaft.

predicate

Eine Abfragebedingung, die `true` oder zurückgibt`false`, was üblicherweise in einer Klausel vorkommt. `WHERE`

Prädikat Pushdown

Eine Technik zur Optimierung von Datenbankabfragen, bei der die Daten in der Abfrage vor der Übertragung gefiltert werden. Dadurch wird die Datenmenge reduziert, die aus der relationalen Datenbank abgerufen und verarbeitet werden muss, und die Abfrageleistung wird verbessert.

Präventive Kontrolle

Eine Sicherheitskontrolle, die verhindern soll, dass ein Ereignis eintritt. Diese Kontrollen stellen eine erste Verteidigungslinie dar, um unbefugten Zugriff oder unerwünschte Änderungen an Ihrem Netzwerk zu verhindern. Weitere Informationen finden Sie unter Präventive Kontrolle in Implementierung von Sicherheitskontrollen in AWS.

Prinzipal

Eine Entität AWS , die Aktionen ausführen und auf Ressourcen zugreifen kann. Diese Entität ist in der Regel ein Root-Benutzer für eine AWS-Konto, eine IAM-Rolle oder einen Benutzer. Weitere Informationen finden Sie unter Prinzipal in Rollenbegriffe und -konzepte in der IAM-Dokumentation.

Datenschutz von Natur aus

Ein systemtechnischer Ansatz, der den Datenschutz während des gesamten Entwicklungsprozesses berücksichtigt.

Privat gehostete Zonen

Ein Container, der Informationen darüber enthält, wie Amazon Route 53 auf DNS-Abfragen für eine Domain und deren Subdomains innerhalb einer oder mehrerer VPCs Domains antworten soll. Weitere Informationen finden Sie unter Arbeiten mit privat gehosteten Zonen in der Route-53-Dokumentation.

proaktive Steuerung

Eine Sicherheitskontrolle, die den Einsatz nicht richtlinienkonformer Ressourcen verhindern soll. Diese Steuerelemente scannen Ressourcen, bevor sie bereitgestellt werden. Wenn die Ressource nicht der Kontrolle entspricht, wird sie nicht bereitgestellt. Weitere Informationen finden Sie im Referenzhandbuch zu Kontrollen in der AWS Control Tower Dokumentation und unter Proaktive Kontrollen unter Implementierung von Sicherheitskontrollen am AWS.

Produktlebenszyklusmanagement (PLM)

Das Management von Daten und Prozessen für ein Produkt während seines gesamten Lebenszyklus, vom Design, der Entwicklung und Markteinführung über Wachstum und Reife bis hin zur Markteinführung und Markteinführung.

Produktionsumgebung

Siehe Umgebung.

Speicherprogrammierbare Steuerung (SPS)

In der Fertigung ein äußerst zuverlässiger, anpassungsfähiger Computer, der Maschinen überwacht und Fertigungsprozesse automatisiert.

schnelle Verkettung

Verwendung der Ausgabe einer LLM-Eingabeaufforderung als Eingabe für die nächste Aufforderung, um bessere Antworten zu generieren. Diese Technik wird verwendet, um eine komplexe Aufgabe in Unteraufgaben zu unterteilen oder um eine vorläufige Antwort iterativ zu verfeinern oder zu erweitern. Sie trägt dazu bei, die Genauigkeit und Relevanz der Antworten eines Modells zu verbessern und ermöglicht detailliertere, personalisierte Ergebnisse.

Pseudonymisierung

Der Prozess, bei dem persönliche Identifikatoren in einem Datensatz durch Platzhalterwerte ersetzt werden. Pseudonymisierung kann zum Schutz der Privatsphäre beitragen. Pseudonymisierte Daten gelten weiterhin als personenbezogene Daten.

publish/subscribe (pub/sub)

Ein Muster, das asynchrone Kommunikation zwischen Microservices ermöglicht, um die Skalierbarkeit und Reaktionsfähigkeit zu verbessern. In einem auf Microservices basierenden MES kann ein Microservice beispielsweise Ereignismeldungen in einem Kanal veröffentlichen, den andere Microservices abonnieren können. Das System kann neue Microservices hinzufügen, ohne den Veröffentlichungsservice zu ändern.

Q

Abfrageplan

Eine Reihe von Schritten, wie Anweisungen, die für den Zugriff auf die Daten in einem relationalen SQL-Datenbanksystem verwendet werden.

Abfrageplanregression

Wenn ein Datenbankserviceoptimierer einen weniger optimalen Plan wählt als vor einer bestimmten Änderung der Datenbankumgebung. Dies kann durch Änderungen an Statistiken, Beschränkungen, Umgebungseinstellungen, Abfrageparameter-Bindungen und Aktualisierungen der Datenbank-Engine verursacht werden.

R

RACI-Matrix

Siehe verantwortlich, rechenschaftspflichtig, konsultiert, informiert (RACI).

RAG

Siehe Erweiterte Generierung beim Abrufen.

Ransomware

Eine bösartige Software, die entwickelt wurde, um den Zugriff auf ein Computersystem oder Daten zu blockieren, bis eine Zahlung erfolgt ist.

RASCI-Matrix

Siehe verantwortlich, rechenschaftspflichtig, konsultiert, informiert (RACI).

RCAC

Siehe Zugriffskontrolle für Zeilen und Spalten.

Read Replica

Eine Kopie einer Datenbank, die nur für Lesezwecke verwendet wird. Sie können Abfragen an das Lesereplikat weiterleiten, um die Belastung auf Ihrer Primärdatenbank zu reduzieren.

neu strukturieren

Siehe 7 Rs.

Recovery Point Objective (RPO)

Die maximal zulässige Zeitspanne seit dem letzten Datenwiederherstellungspunkt. Damit wird festgelegt, was als akzeptabler Datenverlust zwischen dem letzten Wiederherstellungspunkt und der Serviceunterbrechung gilt.

Wiederherstellungszeitziel (RTO)

Die maximal zulässige Verzögerung zwischen der Betriebsunterbrechung und der Wiederherstellung des Dienstes.

Refaktorierung

Siehe 7 Rs.

Region

Eine Sammlung von AWS Ressourcen in einem geografischen Gebiet. Jeder AWS-Region ist isoliert und unabhängig von den anderen, um Fehlertoleranz, Stabilität und Belastbarkeit zu gewährleisten. Weitere Informationen finden Sie unter Geben Sie an, was AWS-Regionen Ihr Konto verwenden kann.

Regression

Eine ML-Technik, die einen numerischen Wert vorhersagt. Zum Beispiel, um das Problem „Zu welchem Preis wird dieses Haus verkauft werden?“ zu lösen Ein ML-Modell könnte ein lineares Regressionsmodell verwenden, um den Verkaufspreis eines Hauses auf der Grundlage bekannter Fakten über das Haus (z. B. die Quadratmeterzahl) vorherzusagen.

rehosten

Siehe 7 Rs.

Veröffentlichung

In einem Bereitstellungsprozess der Akt der Förderung von Änderungen an einer Produktionsumgebung.

umziehen

Siehe 7 Rs.

neue Plattform

Siehe 7 Rs.

Rückkauf

Siehe 7 Rs.

Ausfallsicherheit

Die Fähigkeit einer Anwendung, Störungen zu widerstehen oder sich von ihnen zu erholen. Hochverfügbarkeit und Notfallwiederherstellung sind häufig Überlegungen bei der Planung der Ausfallsicherheit in der. AWS Cloud Weitere Informationen finden Sie unter AWS Cloud Resilienz.

Ressourcenbasierte Richtlinie

Eine mit einer Ressource verknüpfte Richtlinie, z. B. ein Amazon-S3-Bucket, ein Endpunkt oder ein Verschlüsselungsschlüssel. Diese Art von Richtlinie legt fest, welchen Prinzipalen der Zugriff gewährt wird, welche Aktionen unterstützt werden und welche anderen Bedingungen erfüllt sein müssen.

RACI-Matrix (verantwortlich, rechenschaftspflichtig, konsultiert, informiert)

Eine Matrix, die die Rollen und Verantwortlichkeiten für alle Parteien definiert, die an Migrationsaktivitäten und Cloud-Vorgängen beteiligt sind. Der Matrixname leitet sich von den in der Matrix definierten Zuständigkeitstypen ab: verantwortlich (R), rechenschaftspflichtig (A), konsultiert (C) und informiert (I). Der Unterstützungstyp (S) ist optional. Wenn Sie Unterstützung einbeziehen, wird die Matrix als RASCI-Matrix bezeichnet, und wenn Sie sie ausschließen, wird sie als RACI-Matrix bezeichnet.

Reaktive Kontrolle

Eine Sicherheitskontrolle, die darauf ausgelegt ist, die Behebung unerwünschter Ereignisse oder Abweichungen von Ihren Sicherheitsstandards voranzutreiben. Weitere Informationen finden Sie unter Reaktive Kontrolle in Implementieren von Sicherheitskontrollen in AWS.

Beibehaltung

Siehe 7 Rs.

zurückziehen

Siehe 7 Rs.

Retrieval Augmented Generation (RAG)

Eine generative KI-Technologie, bei der ein LLM auf eine maßgebliche Datenquelle verweist, die sich außerhalb seiner Trainingsdatenquellen befindet, bevor eine Antwort generiert wird. Ein RAG-Modell könnte beispielsweise eine semantische Suche in der Wissensdatenbank oder in benutzerdefinierten Daten einer Organisation durchführen. Weitere Informationen finden Sie unter Was ist RAG.

Drehung

Der Vorgang, bei dem ein Geheimnis regelmäßig aktualisiert wird, um es einem Angreifer zu erschweren, auf die Anmeldeinformationen zuzugreifen.

Zugriffskontrolle für Zeilen und Spalten (RCAC)

Die Verwendung einfacher, flexibler SQL-Ausdrücke mit definierten Zugriffsregeln. RCAC besteht aus Zeilenberechtigungen und Spaltenmasken.

RPO

Siehe Recovery Point Objective.

RTO

Siehe Ziel für die Erholungszeit.

Runbook

Eine Reihe manueller oder automatisierter Verfahren, die zur Ausführung einer bestimmten Aufgabe erforderlich sind. Diese sind in der Regel darauf ausgelegt, sich wiederholende Operationen oder Verfahren mit hohen Fehlerquoten zu rationalisieren.

S

SAML 2.0

Ein offener Standard, den viele Identitätsanbieter (IdPs) verwenden. Diese Funktion ermöglicht föderiertes Single Sign-On (SSO), sodass sich Benutzer bei den API-Vorgängen anmelden AWS-Managementkonsole oder die AWS API-Operationen aufrufen können, ohne dass Sie einen Benutzer in IAM für alle in Ihrer Organisation erstellen müssen. Weitere Informationen zum SAML-2.0.-basierten Verbund finden Sie unter Über den SAML-2.0-basierten Verbund in der IAM-Dokumentation.

SCADA

Siehe Aufsichtskontrolle und Datenerfassung.

SCP

Siehe Richtlinie zur Dienstkontrolle.

Secret

Interne AWS Secrets Manager, vertrauliche oder eingeschränkte Informationen, wie z. B. ein Passwort oder Benutzeranmeldeinformationen, die Sie in verschlüsselter Form speichern. Es besteht aus dem geheimen Wert und seinen Metadaten. Der geheime Wert kann binär, eine einzelne Zeichenfolge oder mehrere Zeichenketten sein. Weitere Informationen finden Sie unter Was ist in einem Secrets Manager Manager-Geheimnis? in der Secrets Manager Manager-Dokumentation.

Sicherheit durch Design

Ein systemtechnischer Ansatz, der die Sicherheit während des gesamten Entwicklungsprozesses berücksichtigt.

Sicherheitskontrolle

Ein technischer oder administrativer Integritätsschutz, der die Fähigkeit eines Bedrohungsakteurs, eine Schwachstelle auszunutzen, verhindert, erkennt oder einschränkt. Es gibt vier Haupttypen von Sicherheitskontrollen: präventiv, detektiv, reaktionsschnell und proaktiv.

Härtung der Sicherheit

Der Prozess, bei dem die Angriffsfläche reduziert wird, um sie widerstandsfähiger gegen Angriffe zu machen. Dies kann Aktionen wie das Entfernen von Ressourcen, die nicht mehr benötigt werden, die Implementierung der bewährten Sicherheitsmethode der Gewährung geringster Berechtigungen oder die Deaktivierung unnötiger Feature in Konfigurationsdateien umfassen.

System zur Verwaltung von Sicherheitsinformationen und Ereignissen (security information and event management – SIEM)

Tools und Services, die Systeme für das Sicherheitsinformationsmanagement (SIM) und das Management von Sicherheitsereignissen (SEM) kombinieren. Ein SIEM-System sammelt, überwacht und analysiert Daten von Servern, Netzwerken, Geräten und anderen Quellen, um Bedrohungen und Sicherheitsverletzungen zu erkennen und Warnmeldungen zu generieren.

Automatisierung von Sicherheitsreaktionen

Eine vordefinierte und programmierte Aktion, die darauf ausgelegt ist, automatisch auf ein Sicherheitsereignis zu reagieren oder es zu beheben. Diese Automatisierungen dienen als detektive oder reaktionsschnelle Sicherheitskontrollen, die Sie bei der Implementierung bewährter AWS Sicherheitsmethoden unterstützen. Beispiele für automatisierte Antwortaktionen sind das Ändern einer VPC-Sicherheitsgruppe, das Patchen einer EC2 Amazon-Instance oder das Rotieren von Anmeldeinformationen.

Serverseitige Verschlüsselung

Verschlüsselung von Daten am Zielort durch denjenigen AWS-Service , der sie empfängt.

Service-Kontrollrichtlinie (SCP)

Eine Richtlinie, die eine zentrale Steuerung der Berechtigungen für alle Konten in einer Organisation in ermöglicht AWS Organizations. SCPs Definieren Sie Leitplanken oder legen Sie Grenzwerte für Aktionen fest, die ein Administrator an Benutzer oder Rollen delegieren kann. Sie können sie SCPs als Zulassungs- oder Ablehnungslisten verwenden, um festzulegen, welche Dienste oder Aktionen zulässig oder verboten sind. Weitere Informationen finden Sie in der AWS Organizations Dokumentation unter Richtlinien zur Dienststeuerung.

Service-Endpunkt

Die URL des Einstiegspunkts für einen AWS-Service. Sie können den Endpunkt verwenden, um programmgesteuert eine Verbindung zum Zielservice herzustellen. Weitere Informationen finden Sie unter AWS-Service -Endpunkte in der Allgemeine AWS-Referenz.

Service Level Agreement (SLA)

Eine Vereinbarung, in der klargestellt wird, was ein IT-Team seinen Kunden zu bieten verspricht, z. B. in Bezug auf Verfügbarkeit und Leistung der Services.

Service-Level-Indikator (SLI)

Eine Messung eines Leistungsaspekts eines Dienstes, z. B. seiner Fehlerrate, Verfügbarkeit oder Durchsatz.

Service-Level-Ziel (SLO)

Eine Zielkennzahl, die den Zustand eines Dienstes darstellt, gemessen anhand eines Service-Level-Indikators.

Modell der geteilten Verantwortung

Ein Modell, das die Verantwortung beschreibt, mit der Sie gemeinsam AWS für Cloud-Sicherheit und Compliance verantwortlich sind. AWS ist für die Sicherheit der Cloud verantwortlich, wohingegen Sie für die Sicherheit in der Cloud verantwortlich sind. Weitere Informationen finden Sie unter Modell der geteilten Verantwortung.

SIEM

Siehe Sicherheitsinformations- und Event-Management-System.

Single Point of Failure (SPOF)

Ein Fehler in einer einzelnen, kritischen Komponente einer Anwendung, der das System stören kann.

SLA

Siehe Service Level Agreement.

SLI

Siehe Service-Level-Indikator.

ALSO

Siehe Service-Level-Ziel.

split-and-seed Modell

Ein Muster für die Skalierung und Beschleunigung von Modernisierungsprojekten. Sobald neue Features und Produktversionen definiert werden, teilt sich das Kernteam auf, um neue Produktteams zu bilden. Dies trägt zur Skalierung der Fähigkeiten und Services Ihrer Organisation bei, verbessert die Produktivität der Entwickler und unterstützt schnelle Innovationen. Weitere Informationen finden Sie unter Schrittweiser Ansatz zur Modernisierung von Anwendungen in der AWS Cloud.

SPOTTEN

Siehe Single Point of Failure.

Sternschema

Eine Datenbank-Organisationsstruktur, die eine große Faktentabelle zum Speichern von Transaktions- oder Messdaten und eine oder mehrere kleinere dimensionale Tabellen zum Speichern von Datenattributen verwendet. Diese Struktur ist für die Verwendung in einem Data Warehouse oder für Business Intelligence-Zwecke konzipiert.

Strangler-Fig-Muster

Ein Ansatz zur Modernisierung monolithischer Systeme, bei dem die Systemfunktionen schrittweise umgeschrieben und ersetzt werden, bis das Legacy-System außer Betrieb genommen werden kann. Dieses Muster verwendet die Analogie einer Feigenrebe, die zu einem etablierten Baum heranwächst und schließlich ihren Wirt überwindet und ersetzt. Das Muster wurde eingeführt von Martin Fowler als Möglichkeit, Risiken beim Umschreiben monolithischer Systeme zu managen. Ein Beispiel für die Anwendung dieses Musters finden Sie unter Schrittweises Modernisieren älterer Microsoft ASP.NET (ASMX)-Webservices mithilfe von Containern und Amazon API Gateway.

Subnetz

Ein Bereich von IP-Adressen in Ihrer VPC. Ein Subnetz muss sich in einer einzigen Availability Zone befinden.

Aufsichtskontrolle und Datenerfassung (SCADA)

In der Fertigung ein System, das Hardware und Software zur Überwachung von Sachanlagen und Produktionsabläufen verwendet.

Symmetrische Verschlüsselung

Ein Verschlüsselungsalgorithmus, der denselben Schlüssel zum Verschlüsseln und Entschlüsseln der Daten verwendet.

synthetisches Testen

Testen eines Systems auf eine Weise, die Benutzerinteraktionen simuliert, um potenzielle Probleme zu erkennen oder die Leistung zu überwachen. Sie können Amazon CloudWatch Synthetics verwenden, um diese Tests zu erstellen.

Systemaufforderung

Eine Technik, mit der einem LLM Kontext, Anweisungen oder Richtlinien zur Verfügung gestellt werden, um sein Verhalten zu steuern. Systemaufforderungen helfen dabei, den Kontext festzulegen und Regeln für Interaktionen mit Benutzern festzulegen.

T

tags

Schlüssel-Wert-Paare, die als Metadaten für die Organisation Ihrer Ressourcen dienen. AWS Mit Tags können Sie Ressourcen verwalten, identifizieren, organisieren, suchen und filtern. Weitere Informationen finden Sie unter Markieren Ihrer AWS -Ressourcen.

Zielvariable

Der Wert, den Sie in überwachtem ML vorhersagen möchten. Dies wird auch als Ergebnisvariable bezeichnet. In einer Fertigungsumgebung könnte die Zielvariable beispielsweise ein Produktfehler sein.

Aufgabenliste

Ein Tool, das verwendet wird, um den Fortschritt anhand eines Runbooks zu verfolgen. Eine Aufgabenliste enthält eine Übersicht über das Runbook und eine Liste mit allgemeinen Aufgaben, die erledigt werden müssen. Für jede allgemeine Aufgabe werden der geschätzte Zeitaufwand, der Eigentümer und der Fortschritt angegeben.

Testumgebungen

Siehe Umgebung.

Training

Daten für Ihr ML-Modell bereitstellen, aus denen es lernen kann. Die Trainingsdaten müssen die richtige Antwort enthalten. Der Lernalgorithmus findet Muster in den Trainingsdaten, die die Attribute der Input-Daten dem Ziel (die Antwort, die Sie voraussagen möchten) zuordnen. Es gibt ein ML-Modell aus, das diese Muster erfasst. Sie können dann das ML-Modell verwenden, um Voraussagen für neue Daten zu erhalten, bei denen Sie das Ziel nicht kennen.

Transit-Gateway

Ein Netzwerk-Transit-Hub, über den Sie Ihre Netzwerke VPCs und Ihre lokalen Netzwerke miteinander verbinden können. Weitere Informationen finden Sie in der Dokumentation unter Was ist ein Transit-Gateway. AWS Transit Gateway

Stammbasierter Workflow

Ein Ansatz, bei dem Entwickler Feature lokal in einem Feature-Zweig erstellen und testen und diese Änderungen dann im Hauptzweig zusammenführen. Der Hauptzweig wird dann sequentiell für die Entwicklungs-, Vorproduktions- und Produktionsumgebungen erstellt.

Vertrauenswürdiger Zugriff

Gewährung von Berechtigungen für einen Dienst, den Sie angeben, um Aufgaben in Ihrer Organisation AWS Organizations und in deren Konten in Ihrem Namen auszuführen. Der vertrauenswürdige Service erstellt in jedem Konto eine mit dem Service verknüpfte Rolle, wenn diese Rolle benötigt wird, um Verwaltungsaufgaben für Sie auszuführen. Weitere Informationen finden Sie in der AWS Organizations Dokumentation unter Verwendung AWS Organizations mit anderen AWS Diensten.

Optimieren

Aspekte Ihres Trainingsprozesses ändern, um die Genauigkeit des ML-Modells zu verbessern. Sie können das ML-Modell z. B. trainieren, indem Sie einen Beschriftungssatz generieren, Beschriftungen hinzufügen und diese Schritte dann mehrmals unter verschiedenen Einstellungen wiederholen, um das Modell zu optimieren.

Zwei-Pizzen-Team

Ein kleines DevOps Team, das Sie mit zwei Pizzen ernähren können. Eine Teamgröße von zwei Pizzen gewährleistet die bestmögliche Gelegenheit zur Zusammenarbeit bei der Softwareentwicklung.

U

Unsicherheit

Ein Konzept, das sich auf ungenaue, unvollständige oder unbekannte Informationen bezieht, die die Zuverlässigkeit von prädiktiven ML-Modellen untergraben können. Es gibt zwei Arten von Unsicherheit: Epistemische Unsicherheit wird durch begrenzte, unvollständige Daten verursacht, wohingegen aleatorische Unsicherheit durch Rauschen und Randomisierung verursacht wird, die in den Daten liegt. Weitere Informationen finden Sie im Leitfaden Quantifizieren der Unsicherheit in Deep-Learning-Systemen.

undifferenzierte Aufgaben

Diese Arbeit wird auch als Schwerstarbeit bezeichnet. Dabei handelt es sich um Arbeiten, die zwar für die Erstellung und den Betrieb einer Anwendung erforderlich sind, aber dem Endbenutzer keinen direkten Mehrwert bieten oder keinen Wettbewerbsvorteil bieten. Beispiele für undifferenzierte Aufgaben sind Beschaffung, Wartung und Kapazitätsplanung.

höhere Umgebungen

Siehe Umgebung.

V

Vacuuming

Ein Vorgang zur Datenbankwartung, bei dem die Datenbank nach inkrementellen Aktualisierungen bereinigt wird, um Speicherplatz zurückzugewinnen und die Leistung zu verbessern.

Versionskontrolle

Prozesse und Tools zur Nachverfolgung von Änderungen, z. B. Änderungen am Quellcode in einem Repository.

VPC-Peering

Eine Verbindung zwischen zwei VPCs , die es Ihnen ermöglicht, den Verkehr mithilfe privater IP-Adressen weiterzuleiten. Weitere Informationen finden Sie unter Was ist VPC-Peering? in der Amazon-VPC-Dokumentation.

Schwachstelle

Ein Software- oder Hardwarefehler, der die Sicherheit des Systems beeinträchtigt.

W

Warmer Cache

Ein Puffer-Cache, der aktuelle, relevante Daten enthält, auf die häufig zugegriffen wird. Die Datenbank-Instance kann aus dem Puffer-Cache lesen, was schneller ist als das Lesen aus dem Hauptspeicher oder von der Festplatte.

warme Daten

Daten, auf die selten zugegriffen wird. Bei der Abfrage dieser Art von Daten sind mäßig langsame Abfragen in der Regel akzeptabel.

Fensterfunktion

Eine SQL-Funktion, die eine Berechnung für eine Gruppe von Zeilen durchführt, die sich in irgendeiner Weise auf den aktuellen Datensatz beziehen. Fensterfunktionen sind nützlich für die Verarbeitung von Aufgaben wie die Berechnung eines gleitenden Durchschnitts oder für den Zugriff auf den Wert von Zeilen auf der Grundlage der relativen Position der aktuellen Zeile.

Workload

Ein Workload ist eine Sammlung von Ressourcen und Code, die einen Unternehmenswert bietet, wie z. B. eine kundenorientierte Anwendung oder ein Backend-Prozess.

Workstream

Funktionsgruppen in einem Migrationsprojekt, die für eine bestimmte Reihe von Aufgaben verantwortlich sind. Jeder Workstream ist unabhängig, unterstützt aber die anderen Workstreams im Projekt. Der Portfolio-Workstream ist beispielsweise für die Priorisierung von Anwendungen, die Wellenplanung und die Erfassung von Migrationsmetadaten verantwortlich. Der Portfolio-Workstream liefert diese Komponenten an den Migrations-Workstream, der dann die Server und Anwendungen migriert.

WURM

Sehen Sie einmal schreiben, viele lesen.

WQF

Siehe AWS Workload-Qualifizierungsrahmen.

einmal schreiben, viele lesen (WORM)

Ein Speichermodell, das Daten ein einziges Mal schreibt und verhindert, dass die Daten gelöscht oder geändert werden. Autorisierte Benutzer können die Daten so oft wie nötig lesen, aber sie können sie nicht ändern. Diese Datenspeicherinfrastruktur gilt als unveränderlich.

Z

Zero-Day-Exploit

Ein Angriff, in der Regel Malware, der eine Zero-Day-Sicherheitslücke ausnutzt.

Zero-Day-Sicherheitslücke

Ein unfehlbarer Fehler oder eine Sicherheitslücke in einem Produktionssystem. Bedrohungsakteure können diese Art von Sicherheitslücke nutzen, um das System anzugreifen. Entwickler werden aufgrund des Angriffs häufig auf die Sicherheitsanfälligkeit aufmerksam.

Eingabeaufforderung ohne Zwischenfälle

Bereitstellung von Anweisungen für die Ausführung einer Aufgabe an einen LLM, jedoch ohne Beispiele (Schnappschüsse), die ihm als Orientierungshilfe dienen könnten. Der LLM muss sein vortrainiertes Wissen einsetzen, um die Aufgabe zu bewältigen. Die Effektivität von Zero-Shot Prompting hängt von der Komplexität der Aufgabe und der Qualität der Aufforderung ab. Siehe auch Few-Shot-Prompting.

Zombie-Anwendung

Eine Anwendung, deren durchschnittliche CPU- und Arbeitsspeichernutzung unter 5 Prozent liegt. In einem Migrationsprojekt ist es üblich, diese Anwendungen außer Betrieb zu nehmen.

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.