Einrichtung von Leitplanken und Überwachung von bereits unterzeichneten URLs

AWS Präskriptive Leitlinien

AWS Präskriptive Leitlinien: Einrichtung von Leitplanken und Überwachung von bereits unterzeichneten URLs

Table of Contents

Einrichtung von Leitplanken und Überwachung vorsignierter URLs

Ryan Baker, Amazon Web Services (AWS)

Juli 2024 (Geschichte der Dokumente)

Sicherheit ist ein wichtiges Anliegen für alle Unternehmen und eine wichtige Säule des AWS Well-Architected Framework. Als Sicherheitsingenieur sollten Sie administrative Schutzmaßnahmen implementieren, die auf die organisatorischen Kontrollanforderungen abgestimmt sind. Im AWS Well-Architected Framework definieren Leitplanken die Grenzen, die die Aktivität einschränken.

Dieses Handbuch bietet Hintergrundinformationen und bewährte Methoden für die Verwendung vorsignierter URLs, die mit Amazon Simple Storage Service (Amazon S3) -Objekten verwendet werden. Vorsignierte URLs ermöglichen es Benutzern oder Anwendungen, die Zugriff auf gültige Anmeldeinformationen haben, Anfragen zu generieren, die im Voraus signiert und bis zu einer definierten Ablaufzeit akzeptiert werden. Ein häufiger Anwendungsfall für vorsignierte URLs besteht darin, den Zugriff auf Objekte oder Ressourcen zu erweitern, indem diese Anfragen gemeinsam genutzt werden. Gemeinsam genutzte vorsignierte Anfragen werden von Systemen oder Benutzern generiert, die über die Rechte zur Ausführung einer bestimmten Anfrage verfügen. Sie können dann an andere Systeme oder Benutzer gesendet werden, um die Möglichkeit zu erweitern, dieselbe Anfrage auszuführen.

In diesem Leitfaden erfahren Sie:

- Die Konzepte von vorsignierten URLs
- Anwendungsfälle für vorsignierte URLs
- Empfohlene und optionale Leitplanken
- Überwachungsoptionen
- Beispiele für die AWS-Services Verwendung vorsignierter URLs

Zielgruppe

Dieser Leitfaden richtet sich an Architekten und Sicherheitsingenieure, die für die Implementierung von Sicherheitskontrollen in der AWS Cloud verantwortlich sind.

Ziele

Als Sicherheitsingenieur möchten Sie wissen, wie Lösungsentwickler Sicherheit implementieren und welche Art von Zugriff Ihre Endbenutzer haben. Dieses Handbuch behandelt eine Art von Zugriff, vorsignierte URLs, die häufig mit Amazon S3 verwendet werden. Vorsignierte URLs bieten Entwicklern Optionen zur effizienten Überbrückung von Authentifizierungsmechanismen.

In Amazon S3 stellen vorsignierte URLs eine eindeutige Kategorie von Anfragen dar. Sicherheitstechniker können diese Anfragen überwachen und verwalten, um sicherzustellen, dass sie nur dort verwendet werden, wo es angemessen und notwendig ist. Ziel dieses Leitfadens ist es, Sicherheitsingenieuren dabei zu helfen, diese Art von Aufsicht auf hoher Ebene zu gewährleisten.

Nachdem Sie dieses Handbuch gelesen haben, sollten Sie verstehen, was eine vorsignierte URL ist, wann sie normalerweise verwendet wird und welche Beweggründe für ihre Verwendung sprechen.

Voraussetzungen

Wenn Ihr Unternehmen keine Sicherheitsrichtlinien, Kontrollziele oder Standards definiert hat, wie im Leitfaden Implementierung von Sicherheitskontrollen auf AWS beschrieben, empfehlen wir Ihnen, diese Governance-Aufgaben zu erledigen, bevor Sie mit diesem Leitfaden fortfahren.

Bevor Sie beginnen, sollten Sie sich auch mit den empfohlenen und optionalen bewährten Methoden für Kontrolle und Überwachung vertraut machen. Weitere Informationen finden Sie hier:

- Richtlinien zur Servicesteuerung (AWS Organizations Dokumentation)
- Bucket-Richtlinien für Amazon S3 (Amazon S3 S3-Dokumentation)
- Protokollierung von Anfragen mit Serverzugriffsprotokollierung (Amazon S3 S3-Dokumentation)
- Protokollieren von Amazon S3 S3-API-Aufrufen mithilfe von AWS CloudTrail (Amazon S3 S3-Dokumentation)

Übersicht über vorsignierte URLs

Eine vorsignierte URL ist eine Art von HTTP-Anfrage, die vom AWS Identity and Access Management (IAM -) Dienst erkannt wird. Was diese Art von Anfrage von allen anderen AWS Anfragen unterscheidet, ist der Abfrageparameter X-Amz-Expires. Wie bei anderen authentifizierten Anfragen enthalten vorsignierte URL-Anfragen eine Signatur. Bei vorsignierten URL-Anfragen wird diese Signatur übertragen. `X-Amz-Signature` Die Signatur verwendet kryptografische Operationen von Signature Version 4, um alle anderen Anforderungsparameter zu codieren.

Hinweise

- Signature Version 2 wird derzeit als veraltet eingestuft, wird aber in einigen Fällen immer noch unterstützt. AWS-Regionen Dieses Handbuch bezieht sich auf das Signieren mit Signature Version 4.
- Der empfangende Dienst könnte unsignierte Header verarbeiten, aber die Unterstützung für diese Option ist begrenzt und entspricht den bewährten Methoden. Sofern nicht anders angegeben, gehen Sie davon aus, dass alle Header signiert sein müssen, damit eine Anfrage akzeptiert wird.

Der `X-Amz-Expires` Parameter ermöglicht die Verarbeitung einer Signatur als gültig mit einer größeren Abweichung von der codierten Datums- und Uhrzeitangabe. Andere Aspekte der Signaturgültigkeit werden noch bewertet. Die Signaturdaten dürfen, sofern sie temporär sind, zum Zeitpunkt der Signaturverarbeitung nicht abgelaufen sein. Die Signieranmeldedaten müssen einem IAM-Prinzipal zugeordnet werden, der zum Zeitpunkt der Verarbeitung über ausreichende Autorisierungen verfügt.

Vorsignierte URLs sind eine Teilmenge der vorsignierten Anfragen

Eine vorsignierte URL ist nicht die einzige Methode, um eine Anfrage für einen future Zeitpunkt zu signieren. Amazon S3 unterstützt auch POST-Anfragen, die üblicherweise ebenfalls vorsigniert sind. Eine vorsignierte POST-Signatur ermöglicht Uploads, die einer signierten Richtlinie entsprechen und deren Ablaufdatum in dieser Richtlinie verankert ist.

Unterschriften für Anfragen können in der future datiert werden, obwohl dies ungewöhnlich ist. Solange die zugrunde liegenden Anmeldeinformationen gültig sind, verbietet der Signaturalgorithmus zukünftige Datierungen nicht. Diese Anfragen können jedoch erst nach ihrem gültigen Zeitfenster

erfolgreich bearbeitet werden, was eine future Datierung für die meisten Anwendungsfälle unpraktisch macht.

Was ermöglicht eine vorab signierte Anfrage?

Eine vorsignierte Anfrage kann nur Aktionen zulassen, die aufgrund der Anmeldeinformationen zulässig sind, die zum Signieren der Anfrage verwendet wurden. Wenn die Anmeldeinformationen die in der vorsignierten Anfrage angegebene Aktion implizit oder explizit verweigern, wird die vorsignierte Anfrage beim Senden verweigert. Dies gilt für Folgendes:

- Sitzungsrichtlinien, die mit den Anmeldeinformationen verknüpft sind
- Richtlinien, die dem Prinzipal zugeordnet sind, dem die Anmeldeinformationen zugeordnet sind
- Ressourcenrichtlinien, die sich auf die Sitzung oder den Prinzipal auswirken
- Richtlinien zur Dienststeuerung, die sich auf die Sitzung oder den Prinzipal auswirken

Beweggründe für die Verwendung von vorab signierten Anfragen

Als Sicherheitsingenieur sollten Sie sich darüber im Klaren sein, was Lösungsentwickler dazu bewegt, vorsignierte URLs zu verwenden. Wenn Sie wissen, was notwendig und was optional ist, können Sie besser mit Lösungsentwicklern kommunizieren. Zu den Beweggründen könnten die folgenden gehören:

- Um einen Nicht-IAM-Authentifizierungsmechanismus zu unterstützen und gleichzeitig von der Skalierbarkeit in Amazon S3 zu profitieren. Eine zentrale Motivation besteht darin, direkt mit Amazon S3 zu kommunizieren, um von der integrierten Skalierbarkeit zu profitieren, die dieser Service bietet. Ohne diese direkte Kommunikation müsste eine Lösung die Last aus der erneuten Übertragung von eingehenden Bytes PutObjectund GetObjectAufrufen unterstützen. Je nach Gesamtlast führt diese Anforderung zu zusätzlichen Skalierungsherausforderungen, die ein Solution Builder möglicherweise vermeiden möchte.

  Andere Methoden der direkten Kommunikation mit Amazon S3, wie z. B. die Verwendung temporärer Anmeldeinformationen in AWS Security Token Service (AWS STS) oder Signature Version 4-Signaturen außerhalb von URLs, sind für Ihren Anwendungsfall möglicherweise nicht geeignet. Amazon S3 identifiziert Benutzer anhand von AWS Anmeldeinformationen, wohingegen vorab signierte Anfragen die Identifizierung durch andere Mechanismen als Anmeldeinformationen voraussetzen. AWS Durch vorab signierte Anfragen ist es möglich, diesen Unterschied zu überbrücken und gleichzeitig die direkte Kommunikation für Daten aufrechtzuerhalten.

- Um vom systemeigenen Verständnis eines Browsers für URLs zu profitieren. URLs werden von Browsern verstanden, AWS STS Anmeldeinformationen und Signaturen der Version 4 dagegen nicht. Dies ist bei der Integration mit browserbasierten Lösungen von Vorteil. Alternative Lösungen erfordern mehr Code, benötigen mehr Speicher für große Dateien und werden möglicherweise von Erweiterungen wie Malware- und Virenscannern anders behandelt.

Vergleich mit temporären AWS STS Anmeldeinformationen

Temporäre Anmeldeinformationen ähneln vorsignierten Anfragen. Beide laufen ab, ermöglichen die Festlegung des Zugriffs und werden häufig verwendet, um Nicht-IAM-Anmeldeinformationen mit einer Nutzung zu verbinden, für die AWS-Anmeldeinformationen erforderlich sind.

Sie können temporäre AWS STS Anmeldeinformationen eng auf ein einzelnes S3-Objekt und eine einzelne Aktion beschränken. Dies kann jedoch zu Skalierungsproblemen führen, da APIs Grenzen haben. AWS STS (Weitere Informationen finden Sie im Artikel How can I resolve API Throttling or „Rate exceeded“ -Fehler für IAM und AWS STS auf der AWS re:POST-Website.) Darüber hinaus erfordert jeder generierte Berechtigungsnachweis einen AWS STS API-Aufruf, was die Latenz und eine neue Abhängigkeit erhöht, die sich auf die Ausfallsicherheit auswirken kann. Temporäre AWS STS Anmeldeinformationen haben außerdem eine Mindestablaufzeit von 15 Minuten, wohingegen eine vorab signierte Anfrage kürzere Zeiträume unterstützen kann. (60 Sekunden sind unter den richtigen Bedingungen praktisch.)

Vergleich mit reinen Signaturlösungen

Die einzige inhärent geheime Komponente einer vorab signierten Anfrage ist ihre Signature Version 4-Signatur. Wenn ein Client die anderen Details einer Anfrage kennt und über eine gültige Signatur verfügt, die diesen Angaben entspricht, kann er eine gültige Anfrage senden. Ohne eine gültige Signatur ist dies nicht möglich.

Vorsignierte URLs und reine Signaturlösungen sind sich kryptografisch ähnlich. Reine Signaturlösungen bieten jedoch praktische Vorteile, z. B. die Möglichkeit, einen HTTP-Header anstelle eines Abfragezeichenfolgenparameters für die Übertragung der Signatur zu verwenden (siehe Abschnitt Protokollierung von Interaktionen und Abhilfemaßnahmen). Administratoren sollten auch berücksichtigen, dass Abfragezeichenfolgen häufiger als Metadaten behandelt werden, während Header seltener als solche behandelt werden.

Andererseits bieten AWS SDKs weniger Unterstützung für die direkte Generierung und Verwendung von Signaturen. Für die Erstellung einer reinen Signaturlösung ist mehr benutzerdefinierter

Code erforderlich. Aus praktischer Sicht ist die Verwendung von Bibliotheken anstelle von benutzerdefiniertem Code aus Sicherheitsgründen eine allgemein bewährte Methode. Daher muss der Code für reine Signaturlösungen genauer geprüft werden.

Reine Signaturlösungen verwenden die `X-Amz-Expires` Abfragezeichenfolge nicht und geben keinen ausdrücklichen Gültigkeitszeitraum an. IAM verwaltet die impliziten Gültigkeitszeiträume von Signaturen, die keine explizite Ablaufzeit haben. Diese impliziten Zeiträume werden nicht veröffentlicht. Sie ändern sich normalerweise nicht, aber sie werden unter Berücksichtigung der Sicherheit verwaltet, sodass Sie sich nicht von den Gültigkeitszeiträumen abhängig machen sollten. Es gibt einen Kompromiss zwischen der expliziten Kontrolle über das Ablaufdatum und der Verwaltung des Ablaufdatums durch IAM.

Als Administrator bevorzugen Sie möglicherweise eine reine Signaturlösung. In der Praxis müssen Sie jedoch Lösungen so unterstützen, wie sie erstellt wurden.

Identifizieren vorab signierter Anfragen

Identifizieren von Anfragen, die eine vorsignierte URL verwendeten

Amazon S3 bietet zwei integrierte Mechanismen zur Überwachung der Nutzung auf Anforderungsebene: Amazon S3 S3-Serverzugriffsprotokolle und AWS CloudTrail Datenereignisse. Beide Mechanismen können die Nutzung vorab signierter URLs identifizieren.

Um Logs nach der Nutzung vorsignierter URLs zu filtern, können Sie den Authentifizierungstyp verwenden. Überprüfen Sie für Serverzugriffsprotokolle das Feld Authentifizierungstyp, das normalerweise den Namen authtype hat, wenn es in einer Amazon Athena Athena-Tabelle definiert ist. Für CloudTrail, untersuchen Sie das AuthenticationMethod`additionalEventData`Feld. In beiden Fällen ist der Feldwert für Anfragen, die vorsignierte URLs verwenden`QueryString`, der `AuthHeader` Wert für die meisten anderen Anfragen.

`QueryString`Die Verwendung ist nicht immer mit vorsignierten URLs verknüpft. Um Ihre Suche nur auf die Verwendung vorsignierter URLs zu beschränken, suchen Sie nach Anfragen, die den Abfragezeichenfolgenparameter enthalten. `X-Amz-Expires` Überprüfen Sie bei Serverzugriffsprotokollen die Anforderungs-URI und suchen Sie nach Anfragen, die einen `X-Amz-Expires` Parameter in der Abfragezeichenfolge enthalten. Untersuchen Sie das `requestParameters` Element für ein `X-Amz-Expires` Element. CloudTrail

```
{"Records": [{…, "requestParameters": {…, "X-Amz-Expires": "300"}}, …]}
```

Die folgende Athena-Abfrage wendet diesen Filter an:

```
SELECT * FROM {athena-table} WHERE
  authtype = 'QueryString' AND
  request_uri LIKE '%X-Amz-Expires=%';
```

Für AWS CloudTrail Lake wendet die folgende Abfrage diesen Filter an:

```
SELECT * FROM {data-store-event-id} WHERE
  additionalEventData['AuthenticationMethod'] = 'QueryString' AND
  requestParameters['X-Amz-Expires'] IS NOT NULL
```

Identifizieren anderer Arten von vorab signierten Anfragen

Die POST-Anforderung hat auch einen eindeutigen AuthentifizierungstypHtmlForm, in den Amazon S3 S3-Serverzugriffsprotokollen und CloudTrail. Dieser Authentifizierungstyp ist weniger verbreitet, sodass Sie diese Anfragen möglicherweise nicht in Ihrer Umgebung finden.

Die folgende Athena-Abfrage wendet den Filter für `HtmlForm` an:

```
SELECT * FROM {athena-table} WHERE
  authtype = 'HtmlForm';
```

Für CloudTrail Lake wendet die folgende Abfrage den Filter an:

```
SELECT * FROM {data-store-event-id} WHERE
  additionalEventData['AuthenticationMethod'] = 'HtmlForm'
```

Identifizieren von Anforderungsmustern

Sie können vorsignierte Anfragen mithilfe der im vorherigen Abschnitt beschriebenen Techniken finden. Um diese Daten jedoch nutzbar zu machen, sollten Sie nach Mustern suchen. Die einfachen `TOP 10` Ergebnisse Ihrer Abfrage geben Ihnen vielleicht Aufschluss, aber wenn das nicht ausreicht, verwenden Sie die Gruppierungsoptionen in der folgenden Tabelle.

Gruppierungsoption	Serverzugriffsprotokolle	CloudTrailSee	Beschreibung
Benutzeragent	`GROUP BY useragent`	`GROUP BY userAgent`	Diese Gruppierungsoption hilft Ihnen dabei, die Quelle und den Zweck von Anfragen zu finden. Der Benutzeragent wird vom Benutzer bereitgestellt und ist als Authentifizierungs- oder Autorisierungsmechanismus

Gruppierungsoption	Serverzugriffsprotokolle	CloudTrailSee	Beschreibung
			nicht zuverlässig. Es kann jedoch viel verraten, wenn Sie nach Mustern suchen, da die meisten Clients eine eindeutige Zeichenfolge verwenden, die zumindest teilweise von Menschen lesbar ist.

Gruppierungsoption	Serverzugriffsprotokolle	CloudTrailSee	Beschreibung
Auftraggeber	`GROUP BY requester`	`GROUP BY userIdentity['arn']`	Diese Gruppierungsoption hilft dabei, IAM-Prinzipale zu finden, die Anfragen signiert haben. Wenn Sie diese Anfragen blockieren oder eine Ausnahme für bestehende Anfragen erstellen möchten, bieten diese Abfragen ausreichend Informationen für diesen Zweck. Wenn Sie Rollen gemäß den Best Practices von IAM verwenden, hat die Rolle einen eindeutig identifizierten Besitzer, und Sie können diese Informationen verwenden, um mehr zu erfahren.

Gruppierungsoption	Serverzugriffsprotokolle	CloudTrailSee	Beschreibung
Quell-IP-Adresse	`GROUP BY remoteip`	`GROUP BY sourceIPAddress`	Diese Option gruppiert nach dem letzten Netzwerkübersetzungsschritt, bevor Amazon S3 erreicht wird. • Wenn der Datenverkehr ein NAT-Gateway passiert, ist dies die NAT-Gateway-Adresse. • Wenn der Verkehr über ein Internet-Gateway geleitet wird, ist dies die öffentliche IP-Adresse, die den Verkehr an das Internet-Gateway gesendet hat. • Wenn der Verkehr von außen stammt AWS, ist dies die öffentliche Internetadresse, die dem Ursprung zugeordnet ist.

Gruppierungsoption	Serverzugriffsprotokolle	CloudTrailSee	Beschreibung
			• Wenn es über einen Gateway-VPC-Endpunkt (Virtual Private Cloud) geleitet wird, ist dies die IP-Adresse der Instanz in der VPC. • Wenn sie eine öffentliche virtuelle Schnittstelle (VIF) passiert, ist dies die lokale IP-Adresse des Anforderers oder eines beliebigen Vermittlers wie eines Proxyservers oder einer Firewall, die nur dessen IP-Adresse offenlegt. • Wenn es einen VPC-Schnittstellen-Endpunkt passiert, kann dies die IP-Adresse einer Instanz in der VPC sein. Es kann sich auch um eine IP-Adresse von einer anderen VPC oder einem lokalen

Gruppierungsoption	Serverzugriffsprotokolle	CloudTrailSee	Beschreibung
			Netzwerk handeln. Wie bei öffentlichen VIFs kann dies die IP-Adresse eines beliebigen Vermittlers sein. Diese Daten sind nützlich, wenn Sie Netzwerkkontrollen durchsetzen möchten. Möglicherweise müssen Sie diese Option mit Daten wie `endpoint` (für Serverzugriffsprotokolle) oder `vpcEndpointId` (für CloudTrail Lake) kombinieren, um die Quelle zu klären, da verschiedene Netzwerke private IP-Adressen duplizieren können.

Gruppierungsoption	Serverzugriffsprotokolle	CloudTrailSee	Beschreibung
Name des S3-Buckets	`GROUP BY bucket_name`	`GROUP BY requestParameters['bucketName']`	Diese Gruppierungsoption hilft dabei, Buckets zu finden, die Anfragen erhalten haben. Auf diese Weise können Sie erkennen, ob Ausnahmen erforderlich sind.

Bewährte Methoden für die Verwendung von vorab signierten Anfragen

In diesem Abschnitt werden bewährte Methoden für die Verwendung von vorab signierten Anfragen beschrieben, die ein Sicherheitsingenieur berücksichtigen sollte. Zu den Richtlinien gehören:

- Grundlegende bewährte Verfahren, d. h. Praktiken, die jedes Unternehmen befolgen sollte.
- Zusätzliche Leitlinien. Dabei handelt es sich um Praktiken, die Sie in Betracht ziehen sollten, die Sie jedoch möglicherweise nur teilweise oder mit Ausnahmen umsetzen möchten. Diese sollen zusätzliche Kontrolle und eingehendere Abwehr bieten, sollten aber gegen die allgemeine Komplexität abgewogen werden.
- Protokollierung von Interaktionen, die sich aus Geräten oder Diensten ergeben können, für die Sie oder Ihr Kunde im Rahmen des Modells der gemeinsamen Verantwortung verantwortlich sind. Dieser Abschnitt enthält Vorsichtsmaßnahmen zur Einschränkung der Informationen, auf die über Protokolle zugegriffen werden kann.

Grundlegende bewährte Methoden

Allgemeine bewährte Verfahren, die als wirksame Kontrollen für andere AWS API-Anfragen dienen, gelten auch für vorab signierte Anfragen. In diesem Abschnitt werden zwei der relevantesten Praktiken behandelt: geringste Zugriffsrechte und Datenperimeter. Diese Praktiken bieten eine Tiefe von Kontrollen, über die andere Praktiken hinausgehen.

Wenden Sie das Prinzip der geringsten Rechte an

Der erste Schritt zur Beschränkung der Verwendung von vorab signierten Anfragen ist die allgemeine Beschränkung des Zugriffs auf Amazon S3. Eine vorsignierte URL kann keinen Zugriff auf Ressourcen gewähren, die nicht dem Prinzipal gewährt wurden, der die Signatur für die vorsignierte URL generiert hat. Sie kann auch keinen Zugriff auf eine Ressource auf eine Weise ermöglichen, die diesem Prinzipal nicht gewährt wurde. Daher ist die Anwendung bewährter Verfahren, um diesen Auftraggebern die geringsten Rechte einzuräumen, eine wirksame Schutzmaßnahme.

Das Erstellen einer vorsignierten URL ist ein algorithmischer Vorgang, der auf einem veröffentlichten Standard (Signature Version 4) für die Signaturgenerierung basiert. Daher ist es nicht möglich, der Generierung von vorsignierten Wörtern Grenzen zu setzen. URLs Um relevant zu sein, muss eine

vorsignierte URL jedoch gültig sein und Zugriff auf Ressourcen bieten. Daher ist die Gültigkeit einer vorsignierten URL auch ein wirksames Schutzschild.

Weitere Informationen zu Least Privilege finden Sie unter Grant Least Privilege access im AWS Well-Architected Framework, Säule Sicherheit.

Implementieren Sie einen Datenperimeter

Eine Erweiterung der geringsten Rechte besteht darin, einen Datenperimeter aufrechtzuerhalten, der den Anforderungen Ihres Unternehmens entspricht. Presigned URLs sind mit Datenperimetern kompatibel. Wie bei anderen Anfragen wird die Gültigkeit einer vorab signierten URL-Anforderung zum Zeitpunkt der Anfrage bewertet. Wenn sich die Eigenschaften des Netzwerks, der Ressource, der Rollensitzung und des Prinzipals ändern, werden sie zu dem Zeitpunkt und anhand der Methode bewertet, mit der eine Anfrage empfangen wird.

Nehmen wir zum Beispiel an, dass ein Service, der in einem Amazon Elastic Kubernetes Service (Amazon EKS) -Container ausgeführt wird, eine Anfrage signiert. Die Anfrage wird später vom PC eines Benutzers gesendet, der mit dem Internet verbunden ist. In diesem Fall bewertet die aws: SourceIp -Bedingung die sichtbare öffentliche IP-Adresse der Anfrage vom persönlichen System des Benutzers, nicht die IP-Adresse des Dienstes im Amazon EKS-Container.

Wenn sich die Tags des Prinzipals oder der Ressource ändern, bevor die Anfrage gesendet wird, gelten entsprechend den Bedingungen aws: /tag-key und aws: PrincipalTag /tag-key die aktualisierten und nicht originalen Werte für die Anfrage. ResourceTag

Zusätzliche Leitplanken

Wenn vorab signierte Anfragen von Lösungsentwicklern und Benutzern angemessen verwendet werden, bieten sie einen sicheren Mechanismus, um Benutzern Zugriff auf Daten zu gewähren. Darüber hinaus bietet die Möglichkeit, vorab signierte Anfragen zu generieren, den Prinzipalen keinen Zugriff, den sie nicht bereits hatten.

Sind in diesem Zusammenhang zusätzliche Kontrollen erforderlich? Zusätzliche Kontrollen werden nicht mit der Notwendigkeit gerechtfertigt, den Zugriff zu verweigern, sondern mit der Möglichkeit, die Nutzung zu überwachen, zu genehmigen und Grenzen festzulegen und das Risiko von Benutzerfehlern zu verringern. Auf diese Weise können Sie sicherstellen, dass die Nutzung angemessen und notwendig ist.

Die folgenden Leitplanken unterstützen Sie bei diesem Ziel. Bevor Sie diese Steuerelemente aktivieren, sollten Sie die aktuelle Nutzung ermitteln, indem Sie vorab signierte Anfragen identifizieren. Diese Identifizierung hilft Ihnen, sich auf die Auswirkungen der Leitplanke auf die bestehende Nutzung vorzubereiten oder bei Bedarf Ausnahmen zu planen.

Leitplanke für S3: Signature Age

Ein entscheidendes Merkmal vorsignierter Anfragen ist, dass sie eine Ablaufzeit beschreiben. Die Signatur der Anfrage enthält ein Datum. Dieses Datum wird als `X-Amz-Date` Abfragezeichenfolgenparameter für einen vorsignierten URLs und als Datum oder x-amz-date Header für einen vorsignierten POST übertragen.

Amazon S3 stellt einen Bedingungsschlüssel, s3:SignatureAge, zur Verfügung, mit dem Sie die maximale Zeit zwischen dem Datum der Unterzeichnung und dem effektiven Ablauf der Anfrage begrenzen können. Diese Bedingung kann die Gültigkeitsdauer niemals verlängern, aber sie kann sie verkürzen.

In der folgenden Richtlinie begrenzt der `s3:signatureAge` Bedingungsschlüssel die Gültigkeitsdauer vorab signierter Anfragen auf 15 Minuten. Die folgenden Beispiele verwenden alle 15 Minuten, um die Gültigkeit auf einen ähnlichen Zeitraum zu beschränken, wie es die Standardsignatur unterstützt.

Die zweite Aussage der Richtlinie verweigert jeglichen Zugriff auf Signature Version 2. Diese Version des Signaturprotokolls ist veraltet, wird aber von einigen noch unterstützt. AWS-Regionen Wir empfehlen, dass Sie es explizit blockieren, bevor es vollständig veraltet ist.

Sie können die folgende Richtlinie als AWS Organizations Service Control Policy (SCP) anwenden. Benutzer können weiterhin vorsignierte Anfragen verwenden und Lösungen bereitstellen, die von diesen Anforderungen abhängen, sofern zwischen der Generierung und Verwendung der Signatur weniger als 15 Minuten liegen. Je nach Implementierung hat diese Einschränkung möglicherweise keine Auswirkungen, sie kann dazu führen, dass die Lösung unbrauchbar wird, oder sie kann gelegentlich zu Fehlern führen, die erneut versucht werden können.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyPresignedOver15Minutes",
      "Effect": "Deny",
```

```
      "Action": "s3:*",
      "Resource": "*",
      "Condition": {
        "NumericGreaterThan": {
          "s3:signatureAge": "900000"
        }
      }
    },
    {
      "Sid": "DenySignatureVersion2",
      "Effect": "Deny",
      "Action": "s3:*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
           "s3:signatureversion": "AWS"
        }
      }
    }
  ]
}
```

Ausnahmen

Wenn eine Lösung länger dauert, bis sie abläuft und sie daher von der oben genannten Richtlinie betroffen ist, empfehlen wir Ihnen, eine Methode zur Genehmigung von Ausnahmen bereitzustellen. Um zu vermeiden, dass Ausnahmen in einem SCP aufgezählt werden, verwenden Sie aws:PrincipalTag, wie in der folgenden Richtlinie, um Ausnahmen auf skalierbare Weise zu verwalten. Andere AWS Beispiele, wie z. B. die AWS-Datenperimeter-Richtlinien, verwenden diese Strategie.

Wenn Sie eine Ausnahmerichtlinie mithilfe von implementierenaws:PrincipalTag, müssen Sie den Zugriff auf Einstellungs-Tags für Prinzipale kontrollieren. Tags dieses Typs können direkt von Prinzipalen stammen und von einem SCP gesteuert werden, wie in diesem Beispiel zur Steuerung, welche Tag-Werte festgelegt werden können. Ein Tag dieses Typs kann auch aus Sitzungs-Tags stammen, die von einem Identity Provider (IdP) oder bei der Verwendung AWS STS gesetzt werden. Die Steuerung des Zugriffs auf aws:PrincipalTag ist ein komplexes Thema. Ein Unternehmen, das Erfahrung mit der Verwendung der attributebasierten Zugriffskontrolle (ABAC) hat, wird jedoch über die nötige Erfahrung und Kontrolle verfügen, um die aws:PrincipalTag für diesen Anwendungsfall geeignete Verwendung von zu ermöglichen.

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyPresignedOver15Minutes",
      "Effect": "Deny",
      "Action": "s3:*",
      "Resource": "*",
      "Condition": {
        "NumericGreaterThan": {
          "s3:signatureAge": "900000"
        },
--- Example exception ---
        "StringNotEquals": {
          "aws:PrincipalTag/long-presigned-allowed": "true"
        }
--- Example exception end ---
      }
    }
  ]
}
```

Bucket-Richtlinien

Sie können Bucket-Richtlinien auf alle oder ausgewählte Buckets anwenden, indem Sie eine Richtlinie wie im folgenden Beispiel verwenden. Im Gegensatz zu einem SCP zielt eine Bucket-Richtlinie auch auf die Nutzung des Serviceprinzipals ab. Anhang A dokumentiert nicht die erwartete Nutzung von vorab signierten Anfragen durch den Serviceprinzipal. Wenn Sie jedoch eine Kontrolle implementieren möchten, um diese Grenze nachzuweisen, bietet die folgende Richtlinie diese Kontrolle. Im Gegensatz zu einem SCP kann eine Bucket-Richtlinie auch für Prinzipale in Ihrem Verwaltungskonto gelten. ABAC-basierte Ausnahmen funktionieren in Bucket-Richtlinien genauso wie SCP.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyPresignedOver15Minutes",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::{bucket-name}/*",
```

```
      "Condition": {
        "NumericGreaterThan": {
          "s3:signatureAge": "900000"
        },
--- Example exception ---
        "StringNotEquals": {
          "aws:PrincipalTag/long-presigned-allowed": "true"
        }
--- Example exception end ---
      }
    }
  ]
}
```

Leitplanke für S3:AuthType

Vorsignierte URLs verwenden die Authentifizierung mit Abfragezeichenfolgen, und vorsignierte verwenden immer die POST-Authentifizierung. POSTs Amazon S3 unterstützt die Ablehnung von Anfragen auf der Grundlage des Authentifizierungstyps über den Bedingungsschlüssel s3:AuthType. `REST-QUERY-STRING`ist der `s3:authType` Wert für Abfragezeichenfolgen und `POST` ist der `s3:authType` Wert für POST.

Sie können die folgende Richtlinie als SCP anwenden. Die Richtlinie erlaubt nur `s3:authType` die Header-basierte Authentifizierung. Außerdem wird eine Methode konfiguriert, um Ausnahmen für einzelne Benutzer oder Rollen bereitzustellen.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyNonHeaderAuth",
      "Effect": "Deny",
      "Action": "s3:*",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "s3:authType": "REST-HEADER",
          "aws:PrincipalTag/non-header-auth-allowed": "true"
        }
      }
    }
```

```
  ]
}
```

Das Ablehnen von Anfragen auf der Grundlage des Authentifizierungstyps wirkt sich auf alle Lösungen oder Funktionen aus, die den verweigerten Authentifizierungstyp verwenden. Durch das Ablehnen werden Benutzer beispielsweise `REST-QUERY-STRING` daran gehindert, Uploads oder Downloads von der Amazon S3 S3-Konsole aus durchzuführen. Wenn Sie möchten, dass Benutzer die Amazon S3 S3-Konsole verwenden, verwenden Sie diese Leitplanke nicht und machen Sie keine Ausnahme für Benutzer. Wenn Sie jedoch nicht möchten, dass Benutzer die Amazon S3 S3-Konsole verwenden, können Sie dies `REST-QUERY-STRING` für Benutzer verweigern.

Vielleicht verweigern Sie Benutzern bereits den direkten Zugriff auf Amazon S3 S3-Ressourcen. In diesem Fall ist eine Leitplanke für den Authentifizierungstyp überflüssig. Eine `s3:authType` defense-in-depth Deny-Anweisung ist jedoch nützlich, da Implementierungen zur Verweigerung des direkten Zugriffs in der Regel viele Steueranweisungen umfassen, von denen einige Ausnahmen enthalten.

Rollen, die für Workloads verwendet werden, benötigen normalerweise keinen Zugriff auf die Abfragezeichenfolge oder `POST` Authentifizierung. Ausnahmen sind Rollen, die Dienste unterstützen, die für die Verwendung vorsignierter Anfragen konzipiert sind. Sie können spezielle Ausnahmen für diese Rollen erstellen.

Sie können eine Bucket-Richtlinie auch auf alle oder ausgewählte Buckets anwenden, indem Sie eine Richtlinie wie die folgende verwenden:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyNonHeaderAuth",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::{bucket-name}/*",
      "Condition": {
        "StringNotEquals": {
          "s3:authType": "REST-HEADER",
          "aws:PrincipalTag/non-header-auth-allowed": "true"
        }
      }
```

```
    }
  ]
}
```

Diese Bucket-Richtlinie hat zur Folge, dass die Verwendung von CopyObjectund UploadPartCopy APIs zum Erstellen regionsübergreifender Kopien verweigert wird. Amazon S3 Replication ist nicht betroffen, da es sich nicht auf diese stützt APIs.

Wenn Sie eine Bucket-Richtlinie wie die vorherige Richtlinie verwenden und trotzdem die regionsübergreifende Richtlinie CopyObjectoder UploadPartCopyAPI unterstützen möchten, fügen Sie eine Bedingung hinzu, die der folgenden `aws:ViaAWSService` ähnelt:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyNonHeaderAuth",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::{bucket-name}/*",
      "Condition": {
        "StringNotEquals": {
          "s3:authType": "REST-HEADER",
          "aws:PrincipalTag/non-header-auth-allowed": "true"
        },
        "Bool": {
          "aws:ViaAWSService": "false"
        },
      }
    }
  ]
}
```

Kombination von vordefinierten Leitplanken und Ausnahmen zu anderen Leitplanken

Wenn Sie nicht planen, eine Guardrail generell auf Ihre Benutzer und Rollen anzuwenden, sollten Sie sie vielleicht auf die Ausnahmen anderer gängiger Guardrails anwenden, sodass diese Ausnahmen keine vorsignierten Anfragen unterstützen.

Wenn Sie Netzwerkeinschränkungen haben, aber Ausnahmen für externe Partner oder spezielle Anwendungsfälle zulassen, sollten Sie die Abfragezeichenfolge oder die `POST` Authentifizierung blockieren, wenn diese Ausnahmen angewendet werden, sofern sie nicht ausdrücklich als erforderlich gekennzeichnet sind.

Einschränkungen für S3: SignatureAge

Administratoren werden es nützlich finden, die Auswirkungen von genauer zu verstehen. `s3:signatureAge` Jede signierte Anfrage enthält`X-Amz-Date`, was die aktuelle Uhrzeit angeben sollte. Dieser Wert wird vom Client und vom Unterzeichner der Anfrage eingegeben. AWS lehnt Anfragen ab, von denen er annimmt, dass sie ungültige Zeiten haben. Ein Unterzeichner könnte jedoch Signaturen im Voraus mit einem future Zeitpunkt generieren. Amazon S3 lehnt Anfragen ab, die eine future Uhrzeit angeben, wenn sie zu weit im Voraus gesendet wurden. Wenn die Anfrage jedoch erst zu dem Zeitpunkt gesendet wird, zu dem die Signatur unterzeichnet wurde, kann die Signatur früher generiert und später gesendet werden.

`s3:signatureAge`schränkt das maximale Alter von `X-Amz-Date` in einer Signatur nur für vorab signierte Anfragen ein. Anfragen, die älter als das angegebene Alter sind, werden abgelehnt, auch wenn sie aufgrund des `X-Amz-Expires` Ablaufs oder einer `POST` Richtlinie für gültig erklärt worden wären. `s3:signatureAge`ändert nicht den Gültigkeitszeitraum für Anfragen, die kein explizites Ablaufdatum enthalten. Es kontrolliert auch nicht den Wert`X-Amz-Date`, den ein Client für eine Signatur verwendet.

Wenn die Systemuhr falsch ist oder wenn ein Client Anfragen absichtlich in die Zukunft datiert, entspricht die signierte Zeit möglicherweise nicht der Zeit, zu der die Signatur generiert wurde. Das schränkt die Möglichkeiten ein`s3:signatureAge`, Lösungen zu kontrollieren. Eine Lösung, die bei der Generierung von Signaturen die aktuelle Uhrzeit verwendet, ist erwartungsgemäß eingeschränkt: Die Signaturen bleiben für die in angegebene Anzahl von Millisekunden gültig. `s3:signatureAge` Für eine Lösung, die die aktuelle Zeit nicht verwendet, gelten andere Grenzwerte. Eine Einschränkung besteht darin, dass die Anmeldeinformationen, die zum Signieren der Signatur verwendet wurden, weiterhin gültig sein müssen. Als Administrator können Sie die maximale Gültigkeit der ausgegebenen temporären Anmeldeinformationen kontrollieren. Sie können festlegen, dass die Anmeldeinformationen bis zu 36 Stunden gültig sind, oder die Gültigkeitsdauer auf 15 Minuten beschränken. Der Ablauf temporärer Anmeldeinformationen hängt nicht vom Wert von ab`X-Amz-Date`.

Für permanente Anmeldeinformationen gilt diese Einschränkung nicht. Es hat sich bewährt, nur temporäre Anmeldeinformationen zu verwenden, und Sie können alle permanenten

Anmeldeinformationen explizit widerrufen, wodurch auch alle Signaturen, die auf diesen Anmeldeinformationen basieren, ungültig werden würden.

Es `s3:signatureAge` wird zwar in Millisekunden gemessen, es ist jedoch nicht praktikabel, es auf weniger als 60 Sekunden einzustellen, selbst wenn Sie eine gut synchronisierte Uhr und eine geringe Latenz haben. Bei Einstellungen unter 60 Sekunden besteht das Risiko, dass gültige Anfragen abgelehnt werden. Wenn Sie mit Verzögerungen zwischen der Signaturgenerierung und dem Einreichen der Anfrage oder mit Problemen bei der Uhrsynchronisierung rechnen, sollten Sie diese bei der Verwaltung von `s3:signatureAge` berücksichtigen.

Maßstabsgetreue Ausrichtung von Buckets

SCPs kann verwendet werden`aws:PrincipalTag`, um Ausnahmen für Benutzer zu machen. Sie können in einem Bucket keine Tags verwenden, um den Zugriff zu kontrollieren `aws:ResourceTag` — nur Objekt-Tags werden für die Zugriffskontrolle verwendet. Es ist generell nicht skalierbar, jedem Objekt, auf das Sie diese Steuerung anwenden möchten, ein Tag hinzuzufügen.

Eine Lösung, die für viele Anwendungsfälle geeignet ist, besteht darin, die Richtlinie und die Ausnahme auf Kontoebene anzuwenden, indem entweder die Konten geändert werden, für die der SCP gilt, oder indem aws: ResourceAccount, aws: ResourceOrgPaths oder aws: ResourceOrg ID verwendet wird. Beispielsweise kann ein SCP auf eine Reihe von Produktionskonten angewendet werden.

Eine andere Lösung besteht darin, eine benutzerdefinierte AWS Config Regel zu verwenden, um eine detektive Kontrolle oder eine reaktionsschnelle Kontrolle zu implementieren. Das Ziel wäre, dass jeder Bucket eine Bucket-Richtlinie mit der entsprechenden Leitplanke enthält. Zusätzlich zum Testen des Inhalts einer Bucket-Richtlinie kann die benutzerdefinierte AWS Config Regel die Tags aus dem Bucket abrufen und den Bucket von der Regel ausschließen, wenn der Bucket mit einem bestimmten Wert gekennzeichnet ist. Wenn diese Regel ihre Konformitätsprüfung nicht besteht, könnte sie entweder den Bucket als nicht konform markieren oder eine Problembehebung einleiten, um die Guardrail zur Richtlinie des Buckets hinzuzufügen.

> **Note**
>
> Sie können den Tag-Inhalt von Anfragen nicht auf beschränken. PutBucketTagging Um die Kontrolle darüber zu behalten, wie ein Bucket gekennzeichnet wird, müssen Sie den Zugriff auf `PutBucketTagging` und einschränken DeleteBucketTagging.

Protokollierung von Interaktionen und Abhilfemaßnahmen

Eine vorsignierte URL enthält eine Signatur und kann in der Zeit vor Ablauf verwendet werden, um den spezifischen API-Vorgang auszuführen, für den sie signiert wurde. Sie sollte als temporäre Zugangsberechtigung behandelt werden. Die Signatur sollte nur Dritten zugänglich sein, die sie kennen müssen. In den meisten Umgebungen ist dies der Client, der die Anfrage sendet, und der Server, der sie empfängt. Das Senden der Signatur als Teil einer direkten HTTPS-Sitzung behält ihren privaten Charakter bei, da nur ein Teilnehmer der HTTPS-Sitzung Einblick in den URI hat, der die Signatur überträgt.

Beim URLs Vorsignieren wird die Signatur als `X-Amz-Signature` Abfragezeichenfolgenparameter übertragen. Abfragezeichenfolgenparameter sind Bestandteil einer URI. Das Risiko besteht darin, dass Clients den URI und die damit verbundene Signatur protokollieren könnten. Clients haben Zugriff auf die gesamte HTTP-Anfrage und können jeden Teil der Anfrage, der Daten und der Header (einschließlich der Authentifizierungsheader) protokollieren. Dies ist jedoch konventionell weniger verbreitet. Die URI-Protokollierung ist üblicher und in Fällen wie der Zugriffsprotokollierung erforderlich. Kunden sollten die Signatur vor der Protokollierung mit Schwärzung oder Maskierung entfernen. URIs

In einigen Umgebungen ermöglichen Benutzer Vermittlern (Proxys), Einblick in ihre HTTPS-Sitzungen zu erhalten. Für die Aktivierung von Proxys ist ein hohes Maß an privilegiertem Zugriff auf Clientsysteme erforderlich, da für diese eine Konfiguration und vertrauenswürdige Zertifikate erforderlich sind. Die Installation der Proxykonfiguration und vertrauenswürdiger Zertifikate im lokalen Kontext der Client-Zwischenumgebung ermöglicht ein sehr hohes Maß an Rechten. Aus diesem Grund sollte der Zugang zu solchen Vermittlern streng kontrolliert werden.

Der Zweck eines Vermittlers besteht in der Regel darin, ungewollten Austritt zu blockieren und anderen Austritt nachzuverfolgen. Daher ist es üblich, dass solche Vermittler Anfragen protokollieren. Zwar könnten Vermittler, wie Clients, alle Inhalte, Header und Daten protokollieren (die alle sehr sensibel wären), aber es ist üblicher, dass sie protokollieren URIs, z. B. solche, die den `X-Amz-Signature` Abfragezeichenfolgenparameter enthalten.

Abhilfemaßnahmen

Wir empfehlen, bei der URI-Protokollierung den Parameter der `X-Amz-Signature` Abfragezeichenfolge zu schwärzen, die gesamte Abfragezeichenfolge zu schwärzen oder die Informationen streng vertraulich zu behandeln, wie beim direkten Zugriff auf den Zwischenserver. Obwohl diese Schutzmaßnahmen dringend empfohlen werden, verringert die Tatsache, dass

vorsigniertes URLs Ablaufen das Risiko der Offenlegung von Protokollen verringert, sofern die Offenlegung so lange verzögert wird, dass die Signaturen ablaufen.

Amazon S3 sieht auch die Signaturen und muss sie entsprechend behandeln. Die Amazon S3 S3-Serverzugriffsprotokolle enthalten die Anfrage-URI, aber redigieren Sie sie`X-Amz-Signature`, wie empfohlen. Das Gleiche gilt, wenn CloudTrail Datenereignisse für Amazon S3 protokolliert werden. Sie können Amazon CloudWatch Logs so konfigurieren, dass Daten mithilfe von benutzerdefinierten Datenkennungen maskiert werden.

Der folgende reguläre Ausdruck entspricht dem, `X-Amz-Signature` wie er in einer URI erscheint:

```
X-Amz-Signature=[a-f0-9]{64}
```

Der folgende reguläre Ausdruck fügt Gruppierungsmuster hinzu, um den zu ersetzenden Text genauer zu identifizieren:

```
(?:X-Amz-Signature=)([a-f0-9]{64})
```

Wenn Sie einen Zugriffsprotokolleintrag wie den folgenden haben:

```
X-Amz-Signature=733255ef022bec3f2a8701cd61d4b371f3f28c9f193a1f02279211d48d5193d7
```

Der erste reguläre Ausdruck übersetzt den Eintrag im Zugriffsprotokoll in:

```
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

Der zweite reguläre Ausdruck übersetzt auf Systemen, die Gruppen ohne Erfassung von Gruppen unterstützen, den Eintrag im Zugriffsprotokoll wie folgt:

```
X-Amz-Signature=XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

Häufig gestellte Fragen

Kann eine vorsignierte Anfrage mehrfach verwendet werden? Ist das ein Sicherheitsrisiko?

Ja, eine Signatur in einer vorab signierten Anfrage könnte mehr als einmal verwendet werden. Ob es sich dabei um ein Sicherheitsrisiko handelt, ist eine kontextuelle Frage. Andere Methoden für den Zugriff auf AWS-Services ermöglichen ebenfalls Wiederholungen. Ein Benutzer oder ein Workload mit AWS Anmeldeinformationen kann viele Anfragen senden AWS-Services, und bei jeder dieser Anfragen kann es sich um Duplikate handeln.

Wenn Ihr Anwendungsfall eine einmalige Ausführung erfordert, sollten Sie andere Mechanismen implementieren, um die einmalige Verwendung zu erzwingen. Die einmalige Verwendung ist kein Merkmal von vorab signierten Anfragen. Als Sicherheitsingenieur sollten Sie die Anwendungsfälle und Implementierungen überprüfen, aber in vielen Fällen ist eine Mehrfachnutzung für eine akzeptable Verwendung ausreichend.

Kann eine andere Person als der vorgesehene Benutzer eine vorab signierte Anfrage verwenden?

Eine Signatur in einer vorab signierten Anfrage kann von jedem gesendet werden, der sie besitzt. Sie wird nur akzeptiert, wenn sie andere Formen der Validierung, wie z. B. Datenperimeterkontrollen, bestanden hat. Wenn die Signatur abgelaufen ist, die Anmeldeinformationen abgelaufen sind oder die Signaturanmeldedaten keinen Zugriff auf die angeforderten Ressourcen haben, wird die Anfrage abgelehnt.

Das Gleiche gilt für andere Methoden der Authentifizierung mit AWS-Services. Anmeldeinformationen, die unangemessen weitergegeben werden, ermöglichen einen unangemessenen Zugriff. Die wichtigste bewährte Methode besteht darin, Anmeldeinformationen und Signaturen nur an die vorgesehene Zielgruppe weiterzugeben. Wenn Sie nicht darauf vertrauen können, dass Ihre Zielgruppe private Daten sicher verwahrt und nicht an Dritte weitergibt, untergräbt dies jegliche Form der Authentifizierung.

Kann ein autorisierter Benutzer eine vorab signierte Anfrage verwenden, um Daten zu exfiltrieren?

Die Sicherung von Daten erfordert robuste Maßnahmen. Um den Zugriff für bestimmte Zwecke zu ermöglichen und gleichzeitig einen Datenperimeter aufrechtzuerhalten, ist ein umfassender Ansatz erforderlich. Der Zugriff mit geringsten Rechten, Datenperimeterkontrollen und die Verwendung nur temporärer Zugangsdaten sind allgemeine bewährte Methoden zur Sicherung von Daten. Der angemessene Einsatz dieser Kontrollen schränkt auch die Fähigkeit der Benutzer ein, Aktionen anhand der von ihnen generierten, vorab signierten Anfragen auszuführen.

Dies liegt daran, dass der durch eine vorsignierte Anfrage bereitgestellte Zugriff nur einen Teil des Zugriffs darstellt, der den Anmeldeinformationen gewährt wird, die zum Signieren der Anfrage verwendet werden. In diesem Zusammenhang gelten die bewährten Methoden, die für den Zugriff auf Daten gelten, im Allgemeinen auch für vorab signierte Anfragen, aber vorsignierte Anfragen ermöglichen keinen neuen Zugriff auf Daten.

- Die maximale Gültigkeitsdauer ist auf den Ablauf der Signaturdaten beschränkt. Wenn die Anmeldeinformationen gesperrt werden, sind Signaturen, die auf den Anmeldeinformationen basieren, nicht mehr gültig.
- Wenn die Berechtigungen für den IAM-Prinzipal, der den Signieranmeldeinformationen zugeordnet ist, nicht die Ausführung der Aktion beinhalten, die mit der vorab signierten Anfrage verknüpft ist, führt das Aufrufen einer vorab signierten Anfrage zu einer Antwort mit der Meldung „Zugriff verweigert“. Die Antwort hängt vom aktuellen Status der Berechtigungen zum Zeitpunkt des Aufrufs ab, der nichts mit dem Zeitpunkt zu tun hat, zu dem die Signatur der vorsignierten Anfrage generiert wurde.
- Die Eigenschaften des Prinzipals werden auf der Grundlage des Prinzipals bewertet, der den Signieranmeldeinformationen zugeordnet ist.
- Die Eigenschaften einer Rollensitzung werden auf der Grundlage der Rollensitzung bewertet, die den Signieranmeldeinformationen zugeordnet ist.
- Wie bei normalen Anfragen werden die Eigenschaften des Netzwerks anhand der Art und Weise bewertet, wie die Anfrage empfangen wurde.

In diesem Zusammenhang beschränkt sich die Untersuchung der Risiken im Zusammenhang mit vorab signierten Anfragen auf Bereiche, in denen sie mit Anmeldeinformationen signiert sind, die sich von den Anmeldeinformationen des Benutzers unterscheiden und Zugriff ermöglichen, der nicht Teil

des Principals eines Benutzers war. Diese Prüfung sollte auf das Design des Dienstes, die Arbeitslast oder die Lösung angewendet werden, die Signaturen im Namen eines Benutzers generiert, und nicht auf die vorsignierte Anforderungsfunktion selbst.

Kann ich den Zugriff über eine vorsignierte URL verweigern, wenn ich vermute, dass sie auf unautorisierte Weise weitergegeben wurde?

Ja. Dazu müssen die Anmeldeinformationen, mit denen die URL signiert wurde, ungültig gemacht werden. Es gibt mehrere Möglichkeiten, dies zu erreichen:

- Entfernen Sie die Berechtigungen aus dem IAM-Principal, zu dem die Anmeldeinformationen gehören. Wenn dieser IAM-Prinzipal keinen Zugriff mehr auf die Ressource und den Vorgang hat, für den die URL signiert ist, kann die URL diesen Vorgang nicht ausführen. Dies wirkt sich auf alle übereinstimmenden Verwendungen dieses IAM-Prinzipals aus.
- Wenn es sich bei den zum Signieren der URL verwendeten Anmeldeinformationen um temporäre AWS STS Anmeldeinformationen handelt, können Sie die Sitzungsberechtigungen für temporäre Anmeldeinformationen widerrufen, die vor einem bestimmten Zeitpunkt für den IAM-Prinzipal ausgestellt wurden. Je nach Anwendungsfall kann es andere gültige Sitzungen geben, die vor ihrer normalen Ablaufzeit ungültig werden, aber neue Sitzungen sind davon nicht betroffen. Durch den Widerruf von Sitzungsberechtigungen werden auch alle URLs ungültig, die mit den jeweiligen Sitzungen verknüpften Anmeldeinformationen signiert wurden. Neue URLs, die neuen Sitzungen zugeordnet sind, sind davon jedoch nicht betroffen.
- Wenn es sich bei den zum Signieren der URL verwendeten Anmeldeinformationen um permanente Anmeldeinformationen handelt, deaktivieren Sie den Zugriffsschlüssel. Dies wirkt sich auf die gesamte Nutzung aus, die mit diesen Anmeldeinformationen verknüpft ist.

Ressourcen

Amazon S3 S3-Dokumentation

- Authentifizieren von Anfragen (AWS Signature Version 4)
- Authentifizieren von Anfragen: Verwenden von Abfrageparametern (AWS Signature Version 4)
- Authentifizieren von Anfragen: Browserbasierte Uploads mit POST (AWS Signature Version 4)
- Authentifizierungsspezifische Richtlinienschlüssel für Amazon S3 Signature Version 4
- Arbeiten mit vorsignierten URLs

Andere Verweise

- Aufbau eines Datenperimeters auf AWS (AWS Whitepaper)
- SEC03-BP02 Gewähren Sie den Zugriff mit den geringsten Rechten (AWS Well Architected Framework, Säule Sicherheit)
- SEC03-BP05 Definieren Sie Richtlinien für Zugriffsberechtigungen für Ihr Unternehmen (Well Architected Framework, Security Pillar)AWS

Anhang A: Wie AWS-Services verwende ich Presigned URLs

Dieser Anhang enthält Informationen AWS-Services und Funktionen zur Verwendung von URLs Presigned. Diese Informationen dienen zwei Zwecken:

- Um Sicherheitsingenieuren, die Kontrollen implementieren, Informationen über die möglichen Auswirkungen dieser Kontrollen zur Verfügung zu stellen.
- Um das Bewusstsein für Situationen zu schärfen, in denen dieses Risiko für die URL Protokollierung von Interaktionen relevant sein könnte.

> **Important**
>
> Dieser Anhang enthält keine vollständige Liste von AWS-Services oder deren Verwendung von PresignedURLs. Er behandelt auch keine kundenspezifischen Lösungen oder Lösungen von Drittanbietern.

Amazon S3-Konsole

Principal: Konsolenbenutzer

Standardablauf: 5 Minuten

> **Haftungsausschluss**
>
> In diesem Abschnitt wird das aktuelle Verhalten der Amazon S3 S3-Konsole dokumentiert. AWS Das Verhalten der Konsole kann ohne vorherige Ankündigung geändert werden.

Die Amazon S3 S3-Konsole unterstützt das Herunterladen und Hochladen von Objekten. Für Downloads wird ein vorsignierter URL Code verwendet, der eine Ablaufzeit von 300 Sekunden (5 Minuten) hat. Das URL wird durch eine Anfrage an `https://<bucket-region>.console.aws.amazon.com/s3/batchOpsServlet-proxy` generiert.

Diese Anfrage wird initiiert, wenn der Benutzer auf eine Download-Schaltfläche klickt. Sie wird also URL nicht im Voraus generiert oder an den Client gesendet, bis die ausdrückliche Download-Anfrage erfolgt.

Uploads sind ähnlich, mit der Ausnahme, dass die Konsole zwei Anfragen sendet: `OPTIONS` als CORS Pre-Flight-Check und. `PUT` Beide Anfragen verwenden dieselbe Signatur.

Die zum Signieren verwendeten Anmeldeinformationen sind temporäre Anmeldeinformationen, die dem aktuell angemeldeten Benutzer zugeordnet sind. Einzelheiten zur Methode zum Abrufen dieser temporären Anmeldeinformationen sind nicht Gegenstand dieses Handbuchs.

Amazon S3 Object Lambda

Principal: Anrufer am Access Point

Standardablauf: 61 Sekunden

Amazon S3 Object Lambda verwendet AWS Lambda Funktionen zur automatischen Verarbeitung und Transformation von Daten, wenn sie von Amazon S3 abgerufen werden. Wenn S3 Object Lambda eine Funktion aufruft, wird der Funktion ein Presigned URL (`inputS3Url`) zugewiesen, mit dem sie das Originalobjekt vom unterstützenden Access Point herunterladen kann.

Diese vorsignierten URLs sind für den unterstützenden Amazon S3 S3-Zugriffspunkt signiert, der bei der Konfiguration von S3 Object Lambda bereitgestellt wird. (Dies ist nicht dasselbe wie der Object Lambda Access Point.) Anstatt eine Rolle zu verwenden, die an die Lambda-Funktion gebunden URL ist, wird die mit der Identität des ursprünglichen Aufrufers signiert, und die Berechtigungen dieses Benutzers gelten, wenn die URL verwendet wird. Wenn der signierte Header enthältURL, muss die Lambda-Funktion diese Header in den Aufruf von Amazon S3 einbeziehen.

Das zurückgegebene Vorzeichen URL hat eine Ablaufzeit von 61 Sekunden (eine Sekunde länger als die maximale Dauer für eine S3-Object-Lambda-Funktion). Die generierte URL Datei kann nur mit dem unterstützenden Access Point verwendet werden. Der Anrufer des S3 Object Lambda Access Points muss Zugriff auf diesen Access Point haben. Sie können diesen Zugriff auf den Kontext von S3 Object Lambda einschränken, indem Sie die Bedingung `"aws:CalledVia": ["s3-object-lambda.amazonaws.com"]` verwenden. Wenn diese Bedingung an einen unterstützenden Access Point oder Bucket angehängt ist, kann ein Benutzer nicht direkt auf den unterstützenden Access Point oder Bucket zugreifen.

Der Vorteil dieses Ansatzes besteht darin, dass Sie der Lambda-Funktion keinen Zugriff auf Ihren S3-Bucket oder Access Point gewähren müssen. Die Rolle, die der Lambda-Funktion zugeordnet ist, benötigt Berechtigungen für WriteGetObjectResponse, aber sie benötigt keine Berechtigungen für GetObject.

Wenn S3 Object Lambda vorsigniert generiertURLs, fügt es keine Netzwerkeinschränkungen hinzu, sodass a außerhalb der Lambda-Funktion verwendet werden URL kann. Alle Einschränkungen, die dem Aufrufer von S3 Object Lambda auferlegt wurden, gelten jedoch weiterhin. Wenn Ihre Lambda-Funktion beispielsweise in einem ausgeführt wird VPC und Sie den Aufrufer darauf beschränken, einen VPC Endpunkt zu verwenden, URL müsste jeder, der im Besitz des Vorsignierten ist, in der Lage sein, es über diesen Endpunkt zu senden. VPC Diese Einschränkung gilt auch für und. SourceIpVpcSourceIp

> **Note**
>
> Um eine Lambda-Funktion von S3 Object in a zu verwendenVPC, VPC müssen sie über eine Route zu öffentlichen S3-Endpunkten verfügen, die aufgerufen werden können. WriteGetObjectResponse Dies bedeutet nicht, dass die Anforderungen zur Verwendung eines VPC Endpunkts nicht für Anfragen zum Abrufen von Daten aus dem Bucket gelten würden.

AWS Lambda Regionsübergreifend CopyObject

Schulleiter: internAWS

Standardablauf: 3600 Sekunden

Wenn Sie das CopyObjectoder UploadPartCopyAPIzum Kopieren verwenden AWS-Regionen, verwendet Amazon S3 URLs intern vorsignierte Daten. Diese APIs können direkt von SDKs oder über die AWS CLI Befehle `aws s3api copy-object` und `aws s3api upload-part` aufgerufen werden. Diese werden APIs nicht für die Amazon S3 S3-Replikation verwendet, aber sie werden von den `aws s3 sync` Befehlen AWS CLI `aws s3 cp` und verwendet, wenn Quelle und Ziel S3-Buckets sind. Sie werden auch durch `TransferManager` Implementierungen in verschiedenen Bereichen unterstützt. AWS SDKs

AWS Lambda GetFunction

Prinzipal: intern AWS

Standardablauf: 10 Minuten

AWS Lambda speichert die Benutzerversion in einem S3-Bucket, der dem Lambda-Team gehört, bevor die in Lambda-Containern bereitgestellten Assets generiert werden. Wenn Sie auf den Code für Ihre Funktion zugreifen möchten, rufen Sie den auf. GetFunctionAPI Dieser API antwortet mit`Code.Location`, was einen vorsignierten Vertrag enthältURL, der für 10 Minuten gültig ist (diese Ablaufzeit ist ein aktuelles Verhalten und kein veröffentlichter Vertrag). Wenn Sie den Code nicht benötigen, können Sie eine Kombination aus GetFunctionConfiguration, und verwenden GetFunctionConcurrency, ListTagsum die anderen Daten abzurufen, die von zurückgegeben werden`GetFunction`.

Die zurückgegebene Datei wurde URL nicht mit den Anmeldeinformationen des aktuell angemeldeten Benutzers signiert, sondern im Namen des Benutzers von Lambda. Aus diesem Grund gelten Bedingungsschlüssel (wie`aws:SourceIP`), die auf den aktuell angemeldeten Benutzer angewendet werden, oder die temporären Sitzungsanmeldedaten des Benutzers nicht für den generierten URL Benutzer. Dies gilt unabhängig davon, ob Bedingungsschlüssel GetFunctionnur auf oder auf die gesamte AWS API Nutzung des Benutzers oder der Sitzung angewendet werden.

Die Lambda-Konsole verwendet auch GetFunctionund gibt das Vorsignierte zurückURL. Die Konsole verwendet die temporären Anmeldeinformationen, die dem aktuell angemeldeten Benutzer zugeordnet sind, um anzurufen. GetFunction Einzelheiten zum Abrufen dieser temporären Anmeldeinformationen sind in diesem Dokument nicht enthalten.

Amazon ECR

Schulleiter: AWS intern

Standardablauf: 1 Stunde

Amazon Elastic Container Registry (AmazonECR) stellt das bereit GetDownloadUrlForLayerAPI, das eine vorsignierte zurückgibtURL, die für eine Stunde gültig ist und das Herunterladen einer einzelnen Ebene aus einem ECR Amazon-Image unterstützt. Dieser Vorgang wird jedoch vom ECR Amazon-Proxy verwendet und wird im Allgemeinen nicht von Benutzern zum Abrufen und Übertragen von Bildern verwendet.

Amazon Redshift Spectrum

Principal: Rolle wurde CREATEEXTERNALSCHEMAübergeben `IAM_ROLE`

Standardablauf: 1 Stunde

Amazon Redshift Spectrum verwendet URLs intern vorsignierte und verbietet Einschränkungen bei der Kombination von Bucket und Amazon Redshift Redshift-Rolle, die vorsigniert wären. URLs Sie können einen `s3:signatureAge` Wert von 16 Minuten verwenden, aber sehr niedrige Werte sind unzuverlässig. Der Mindestwert, den Sie verwenden können, hängt vom Zeitpunkt und der Größe Ihrer Abfrage ab. Ein Wert unter 16 Minuten funktioniert zwar in vielen Szenarien, erfordert jedoch Tests. Die Rolle kann und sollte URLs darauf beschränkt werden, nur von Redshift Spectrum verwendet zu werden, wobei Redshift Spectrum die generierten Daten nicht offenlegt, wodurch die typische Rechtfertigung für niedrigere Ablaufwerte entschärft wird.

Amazon SageMaker KI-Studio

Amazon SageMaker AI Studio unterstützt zwei API Aktionen: CreatePresignedDomainUrlund CreatePresignedNotebookInstanceUrl. Diese haben jedoch nichts APIs mit der vordefinierten URL Funktion Signature Version 4 zu tun. Diese APIs erstellen eineURL, die einen `authToken` Parameter verwendet, aber sie unterstützen keinen der standardmäßigen Signature Version 4-Abfrageparameter.

`authToken`ist ein anderer Mechanismus, weist aber Ähnlichkeiten mit Presigned URLs auf. Er wird als Abfragezeichenfolgenparameter gesendet und unterstützt eine Ablaufzeit von 5 Minuten.

SageMaker KI unterstützt Netzwerkeinschränkungen. Wenn Sie der `sagemaker:CreatePresignedDomainUrl` Aktion eine Einschränkung auferlegen, gilt diese Aktion sowohl für das Aufrufen CreatePresignedDomainUrlals auch für die Verwendung der generierten AktionURL. Wenn a aus einem gültigen Netzwerk generiert und dann von einem ungültigen Netzwerk gesendet wird, URL ist der API Aufruf zur Generierung URL erfolgreich, aber die Anforderung, mit der die URL gesendet wird, schlägt fehl. Das Gleiche gilt für CreatePresignedNotebookInstanceUrlund die `sagemaker:CreatePresignedNotebookInstanceUrl` Aktion.

Weitere Informationen finden Sie in der SageMaker KI-Dokumentation.

Anhang B: Auswirkungen von Kontrollen für vorsignierte URLs AWS-Services

In diesem Anhang werden Interaktionen zwischen den AWS-Services , die vorsignierte URLs verwenden, wie in Anhang A beschrieben, und den zuvor in diesem Handbuch beschriebenen Steuerelementen beschrieben beschrieben.

Leitplanke für S3: SignatureAge

Die Amazon S3 S3-Konsole wird durch den maximalen Ablauf von 5 Minuten, der durch den `s3:signatureAge` Bedingungsschlüssel festgelegt wird, nicht gestört. Die Amazon S3 S3-Konsole generiert vorsignierte URLs, wenn Sie auf die Download-Schaltfläche klicken, und wendet eine eigene Ablaufzeit von 5 Minuten an. Eine maximale Dauer von weniger als 2 Minuten kann aufgrund von Uhrsynchronisation und Latenzen zu zufälligen Ausfällen führen.

Amazon S3 Object Lambda verwendet eine Ablaufzeit von 61 Sekunden, sodass das Festlegen von Bedingungen auf einen `s3:signatureAge` Wert von 61 Sekunden oder mehr keine Unterbrechung verursacht. Kürzere Zeiträume sind möglicherweise weniger zuverlässig und können zu zeitweiligen Ausfällen führen.

Amazon S3 Cross-Region wird CopyObjectnicht durch einen maximalen Ablauf von 5 Minuten unterbrochen. Kürzere Zeiträume können jedoch aufgrund von Uhrsynchronisierung und Latenzen zu zufälligen Ausfällen führen.

In AWS LambdaGetFunctionstellt eine URL zu Objekten außerhalb des Kundenkontos bereit, sodass sich Kundenrichtlinien nicht auf die generierten URLs auswirken.

Amazon Redshift Spectrum wurde `s3:signatureAge` unter einer Bedingung von 16 Minuten getestet. Kürzere Zeiträume können jedoch zu Störungen führen.

Guardrail für S3:AuthType, wenn keine Netzwerkeinschränkungen verwendet werden

Die Amazon S3 S3-Konsole ist normalerweise von der `s3:authType` Leitplanke betroffen. Die Konsole leitet basierend auf der lokalen Netzwerkkonfiguration zu Amazon S3 weiter. Wenn das

lokale Netzwerk auf eine Weise zu Amazon S3 weiterleitet, die die Netzwerkeinschränkung zulässt, würde die Amazon S3 S3-Konsole trotzdem funktionieren. Wenn es jedoch auf eine unzulässige Weise über einen Proxy oder das öffentliche Internet geleitet wird, wird die Nutzung blockiert. Das Blockieren der Nutzung ist jedoch wahrscheinlich die Absicht dieser Richtlinie.

Amazon S3 Object Lambda ist betroffen, wenn die Lambda-Funktion nicht mit einer geeigneten VPC verbunden ist. In dieser Konfiguration muss die VPC über ein NAT-Gateway verfügen, nicht um auf den S3-Bucket zuzugreifen, sondern um ihn aufzurufen WriteGetObjectResponse.

Amazon S3 Cross-Region CopyObjectist gestört, wenn diese Leitplanke auf eine Bucket-Richtlinie angewendet wird, ohne dass die empfohlene Ausnahme für wann wahr ist. **`aws:viaAWSService`**

Amazon Redshift Spectrum ist von der `s3:authType` Leitplanke betroffen, sofern nicht erweitertes VPC-Routing verwendet wird. Derzeit unterstützt Redshift Spectrum erweitertes VPC-Routing nur mit serverlosen Clustern, nicht mit bereitgestellten Clustern.

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
Erste Veröffentlichung	—	23. Juli 2024

AWS Glossar zu präskriptiven Leitlinien

Die folgenden Begriffe werden häufig in Strategien, Leitfäden und Mustern von AWS Prescriptive Guidance verwendet. 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

Weitere Informationen finden Sie unter 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 Transaktionen von verbindenden Anwendungen verarbeitet, 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 zur Verwendung in der AWS Migrationsstrategie finden Sie im Operations Integration Guide. AIOps

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.

autoritative 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 Cloud-Einführung (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, sogenannte bösartige Bots, 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 für die AWS 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 is commonly described as a pipeline. CI/CDkann 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 Variation 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, die sicherstellen, 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 historischer 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.

Bereitstellung

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, die Sie verwenden, um Ausfallzeiten und Datenverluste aufgrund einer Katastrophe zu 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 Sicherheitsthemen 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, 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.

Holdout-Daten

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 sich Infrastruktur als Code an.

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 von Modellen 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

Weitere Informationen finden Sie in der 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

Weitere Informationen finden Sie unter Label-basierte 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 einer Organisation angehören.

DURCHEINANDER

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 Implementierung 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

Siehe Origin Access Control.

OAI

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 Einen Trail für eine Organisation erstellen.

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. Bei dieser Entität handelt es sich in der Regel um einen 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 mit der Steuerung konform ist, 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).

LAPPEN

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 aller an Migrationsaktivitäten und Cloud-Operationen beteiligten Parteien definiert. 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 der Wiederherstellungszeit.

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 Management Console 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 Benutzeranmeldedaten, 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, während 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.

Zero-Shot-Aufforderung

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.