Implementierung von Richtlinien für Berechtigungen mit den geringsten Rechten für AWS CloudFormation

AWS Präskriptive Leitlinien

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Präskriptive Leitlinien: Implementierung von Richtlinien für Berechtigungen mit den geringsten Rechten für AWS CloudFormation

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Die Handelsmarken und Handelsaufmachung von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, durch die Kunden irregeführt werden könnten oder Amazon in schlechtem Licht dargestellt oder diskreditiert werden könnte. Alle anderen Handelsmarken, die nicht Eigentum von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise zu Amazon gehören oder nicht, mit Amazon verbunden sind oder von Amazon gesponsert werden.

Table of Contents

Einführung ... 1
Was sind die geringsten Rechte? ... 2
Gezielte Geschäftsergebnisse ... 3
Zielgruppe ... 3
Verwenden von Zugriffsrichtlinien ... 4
Berechtigungen zur Verwendung von CloudFormation ... 5
Identitätsbasierte Richtlinien ... 6
Bewährte Methoden ... 7
Beispielrichtlinien ... 8
Servicerollen ... 12
Implementierung der geringsten Rechte für Servicerollen CloudFormation ... 13
Konfiguration von Servicerollen ... 14
Einem IAM-Prinzipal Berechtigungen zur Verwendung einer CloudFormation Servicerolle gewähren ... 14
Konfiguration einer Vertrauensrichtlinie für die CloudFormation Servicerolle ... 16
Zuordnen einer Servicerolle zu einem Stack ... 17
Richtlinien stapeln ... 17
Konfiguration von Stack-Richtlinien ... 18
Stack-Richtlinien festlegen und überschreiben ... 19
Stack-Richtlinien einschränken und vorschreiben ... 19
Berechtigungen für bereitgestellte Ressourcen ... 23
Beispiel: Amazon S3 S3-Bucket ... 24
Bewährte Methoden ... 27
Nächste Schritte ... 29
Ressourcen ... 31
CloudFormation Dokumentation ... 31
IAM-Dokumentation ... 31
Andere Referenzen AWS ... 31
Dokumentverlauf ... 32
Glossar ... 33
... 33
A ... 34
B ... 37
C ... 39

D 43
E 47
F 49
G 51
H 52
I 54
L 57
M 58
O 62
P 65
Q 68
R 69
S 72
T 76
U 78
V 78
W 79
Z 80
..... lxxxi

Implementierung von Richtlinien für Berechtigungen mit den geringsten Rechten für AWS CloudFormation

Nima Fotouhi und Moumita Saha, Amazon Web Services ()AWS

Mai 2023 (Dokumentverlauf)

AWS CloudFormationist ein Infrastructure-as-Code-Service (IaC), mit dem Sie Ihre Cloud-Infrastrukturentwicklung durch die Bereitstellung von Ressourcen skalieren können. AWS Er hilft Ihnen auch dabei, diese Ressourcen während ihres gesamten Lebenszyklus, über und hinweg AWS-Konten zu verwalten. AWS-Regionen In CloudFormation definieren Sie Vorlagen, die als Vorlage für eine Reihe von Ressourcen dienen. Anschließend stellen Sie diese Ressourcen bereit, indem Sie einen Stack erstellen und bereitstellen. Dabei handelt es sich um eine Gruppe verwandter Ressourcen, die Sie als eine Einheit verwalten. Sie können damit auch Stack-Sets bereitstellen. Dabei handelt es sich CloudFormation um Gruppen von Stacks, die Sie für mehrere Konten und AWS-Regionen mit einem einzigen Vorgang erstellen, aktualisieren und löschen können. Dieses Handbuch bietet einen Überblick darüber, wie Sie Berechtigungen mit den geringsten Rechten für AWS CloudFormation und Ressourcen, die über bereitgestellt werden, implementieren können. CloudFormation

Sie können CloudFormation Stacks oder Stack-Sets bereitstellen, indem Sie einen der folgenden Schritte ausführen:

- Greifen Sie über einen AWS Identity and Access Management (IAM-) Principal direkt auf die AWS Umgebung zu und stellen Sie CloudFormation Stacks bereit.
- Führen Sie die CloudFormation Stacks in einer Bereitstellungspipeline durch und initiieren Sie die Stack-Bereitstellung über die Pipeline. Die Pipeline greift über einen IAM-Principal auf die AWS Umgebung zu und stellt die Stacks bereit. Dieser Ansatz ist eine empfohlene bewährte Methode.

Für jeden dieser Ansätze sind Berechtigungen zum Bereitstellen von CloudFormation Stacks erforderlich. Stellen Sie sich zum Beispiel einen Benutzer vor, der plant CloudFormation , eine Amazon Elastic Compute Cloud (Amazon EC2) -Instance zu erstellen. Für diese Instanz wäre ein IAM-Instanzprofil erforderlich, um auf eine andere AWS-Services Instanz zugreifen zu können. Der für die Bereitstellung des CloudFormation Stacks verwendete IAM-Principal würde die folgenden Berechtigungen benötigen:

- Zugriffsberechtigungen CloudFormation
- Berechtigungen zum Erstellen von Stacks in CloudFormation
- Berechtigungen zum Erstellen von Instances in Amazon EC2
- Berechtigungen zum Erstellen der erforderlichen IAM-Instanzprofile

Was sind die geringsten Rechte?

Geringste Berechtigung ist die bewährte Methode, die für die Ausführung einer Aufgabe erforderlichen Mindestberechtigungen zu gewähren. Das Prinzip der geringsten Rechte ist Teil der Sicherheitssäule im AWS Well-Architected Framework. Wenn Sie diese bewährte Methode implementieren, kann sie dazu beitragen, Ihre AWS Umgebung vor Risiken durch die Eskalation von Rechten zu schützen, die Angriffsfläche zu reduzieren, die Datensicherheit zu verbessern und Benutzerfehler zu verhindern (wie z. B. eine fehlerhafte Konfiguration oder das versehentliche Löschen einer Ressource).

Um die geringsten Rechte für Ihre AWS Ressourcen zu implementieren, konfigurieren Sie Richtlinien, wie z. B. identitätsbasierte Richtlinien in AWS Identity and Access Management (IAM). Diese Richtlinien definieren Berechtigungen und legen die Zugriffsbedingungen fest. Organizations beginnen möglicherweise mit AWS verwalteten Richtlinien, erstellen dann aber in der Regel benutzerdefinierte Richtlinien, die den Umfang der Berechtigungen auf die Aktionen beschränken, die für die Arbeitslast oder den Anwendungsfall erforderlich sind.

Die Verwendung von Berechtigungen mit den geringsten Rechten für den CloudFormation Dienst ist ein wichtiger Sicherheitsaspekt. Da Benutzer und Entwickler, die mit ihnen interagieren, in der Lage sein CloudFormation können, Ressourcen schnell und in großem Umfang zu erstellen, zu ändern oder zu löschen, ist die geringste Zugriffsberechtigung besonders wichtig. CloudFormation Erfordert jedoch die erforderlichen Berechtigungen, um Ressourcen in Ihrem zu erstellen, zu aktualisieren und zu ändern AWS-Konten. Sie müssen den Bedarf an Berechtigungen für den Betrieb CloudFormation mit dem Prinzip der geringsten Rechte in Einklang bringen.

Bei der Anwendung des Prinzips der geringsten Rechte auf müssen Sie Folgendes berücksichtigen: CloudFormation

- Berechtigungen für den CloudFormation Service — Welche Benutzer benötigen Zugriff CloudFormation, welche Zugriffsebene benötigen sie und welche Aktionen können sie ergreifen, um Stacks zu erstellen, zu aktualisieren oder zu löschen?

- Berechtigungen zur Bereitstellung von Ressourcen — Über welche Ressourcen können Benutzer Ressourcen bereitstellen? CloudFormation
- Berechtigungen für bereitgestellte Ressourcen — Wie konfigurieren Sie Berechtigungen mit den geringsten Rechten für die Ressourcen, über die Sie die Bereitstellung vornehmen? CloudFormation

Gezielte Geschäftsergebnisse

Wenn Sie die bewährten Methoden und Empfehlungen in diesem Leitfaden befolgen, können Sie:

- Ermitteln Sie, für welche Benutzer in Ihrer Organisation Zugriff erforderlich ist CloudFormation, und konfigurieren Sie dann die Berechtigungen mit den geringsten Rechten für diese Benutzer.
- Verwenden Sie Stack-Richtlinien, um CloudFormation Stacks vor unbeabsichtigten Updates zu schützen.
- Konfigurieren Sie Berechtigungen mit den geringsten Rechten für CloudFormation Benutzer und Ressourcen, um eine Eskalation von Rechten und das Problem des verwirrten Stellvertreters zu verhindern.
- Wird verwendet AWS CloudFormation , um AWS Ressourcen mit den geringsten Rechten bereitzustellen. Dies hilft Ihrem Unternehmen dabei, ein robusteres Sicherheitsniveau aufrechtzuerhalten.
- Reduzieren Sie proaktiv den Zeit-, Energie- und Kostenaufwand für die Untersuchung und Abwehr von Sicherheitsvorfällen.

Zielgruppe

Dieses Handbuch richtet sich an Cloud-Infrastrukturarchitekten, DevOps Techniker und Techniker für die Zuverlässigkeit von Websites (SREs), die Ressourcen mithilfe von verwalten und bereitstellen. CloudFormation

Verwenden von Zugriffsrichtlinien zum Erteilen von Berechtigungen in AWS

Sie verwalten den Zugriff in, AWS indem Sie identitätsbasierte Richtlinien erstellen und diese an AWS Identity and Access Management (IAM-) Prinzipale wie Rollen oder Benutzer anhängen. Außerdem erstellen Sie ressourcenbasierte Richtlinien und fügen sie Ressourcen hinzu. AWS AWS bewertet diese Richtlinien bei jeder Anfrage. Die Berechtigungen in den Richtlinien legen fest, ob eine Anforderung zugelassen oder abgelehnt wird.

Um zu verstehen, wie der Zugriff mit den geringsten Rechten in Richtlinien konfiguriert wird, müssen Sie die verschiedenen Arten von Richtlinien, die Elemente und die Struktur einer Richtlinie sowie die Art und Weise, wie Richtlinien bewertet werden, verstehen. Dieser Leitfaden konzentriert sich nur auf identitätsbasierte Richtlinien und ressourcenbasierte Richtlinien. Es AWS enthält jedoch auch andere Arten von Richtlinien, z. B. Richtlinien zur Dienststeuerung (SCPs), Berechtigungsgrenzen und Sitzungsrichtlinien. Jeder Richtlinientyp spielt eine Rolle bei der Implementierung von Berechtigungen mit den geringsten Rechten in Ihrem. AWS-Konten Weitere Informationen finden Sie in der IAM-Dokumentation unter Richtlinien und Berechtigungen und Anwenden von Berechtigungen mit den geringsten Rechten.

Konfiguration der zu verwendenden Berechtigungen mit den geringsten Rechten CloudFormation

In diesem Kapitel werden die Optionen für die Konfiguration von Zugriffs- und Nutzungsberechtigungen für den AWS CloudFormation Dienst beschrieben.

Wenn ein Benutzer oder ein Dienst AWS Ressourcen bereitstellt CloudFormation, besteht der erste Schritt darin, den CloudFormation Dienst über einen AWS Identity and Access Management (IAM-) Principal aufzurufen. Dieser IAM-Prinzipal muss über Berechtigungen zum Erstellen der CloudFormation Stacks verfügen. Als Nächstes verwendet der IAM-Prinzipal einen der folgenden Ansätze zur Bereitstellung von Ressourcen über: CloudFormation

- Wenn der IAM-Prinzipal die Stack-Operationen nicht an eine CloudFormation Servicerolle weitergibt, CloudFormation verwendet er die Anmeldeinformationen des IAM-Prinzipals, um die Stack-Operationen auszuführen. Dies ist die Standardeinstellung. Daher benötigt der IAM-Principal zusätzlich zu den Berechtigungen zur Ausführung der CloudFormation Stack-Operationen auch Berechtigungen zur Bereitstellung der Ressourcen, die in den CloudFormation Vorlagen definiert sind, die er verwenden wird. Wenn der IAM-Principal beispielsweise nicht berechtigt ist, Amazon Elastic Compute Cloud (Amazon EC2) -Instances zu erstellen, kann er keinen CloudFormation Stack erstellen, der eine EC2 Amazon-Instance bereitstellen würde.
- Wenn der IAM-Principal die Stack-Operationen an eine CloudFormation Service-Rolle weitergibt, CloudFormation verwendet er dann die Service-Rolle, um die Stack-Operationen durchzuführen und die Ressourcen in der CloudFormation Vorlage bereitzustellen. Diese CloudFormation Servicerolle sollte mit Berechtigungen zur Bereitstellung im Namen des AWS-Services IAM-Prinzipals definiert werden. Bei diesem Ansatz wird vermieden, dass dem IAM-Prinzipal direkte Berechtigungen zur Bereitstellung der in den AWS CloudFormation Vorlagen definierten Ressourcen erteilt werden. Der IAM-Principal benötigt Berechtigungen zur CloudFormation Stack-Erstellung und CloudFormation verwendet anstelle der Richtlinie des IAM-Prinzipals die Richtlinie der Servicerolle, um Aufrufe zu tätigen.

Durch die Verwendung des Service-Rollen-Ansatzes und des Prinzips der geringsten Rechte können Sie die Ressourcenbereitstellung in Ihrer AWS Umgebung standardisieren und vorschreiben, dass Benutzer Ressourcen als IaC bereitstellen. CloudFormation Da die den IAM-Prinzipalen zugewiesenen Richtlinien keine Berechtigungen für die direkte Bereitstellung von AWS Ressourcen enthalten, müssen Benutzer diese für die Bereitstellung verwenden. CloudFormation

In diesem Kapitel werden die folgenden Mechanismen zur Konfiguration und Verwaltung des Zugriffs auf den CloudFormation Service und die Stacks beschrieben: CloudFormation

- Identitätsbasierte Richtlinien für CloudFormation— Verwenden Sie diese Art von Richtlinie, um zu konfigurieren, auf welche IAM-Prinzipale zugreifen können CloudFormation und welche Aktionen sie ausführen können. CloudFormation
- Servicerollen für CloudFormation— Erstellen Sie eine Servicerolle, die es ermöglicht CloudFormation , Stack-Ressourcen im Namen des IAM-Prinzipals, der den Stack bereitstellt, zu erstellen, zu aktualisieren oder zu löschen. Die Servicerolle wird in IAM erstellt und kann einem oder mehreren Stacks zugeordnet werden.
- CloudFormation Richtlinien stapeln— Verwenden Sie diese Art von Richtlinie, um zu bestimmen, wann ein Stack aktualisiert werden kann. Diese Art von Richtlinie kann dazu beitragen, zu verhindern, dass Stack-Ressourcen unbeabsichtigt aktualisiert oder gelöscht werden. Stack-Richtlinien werden erstellt und Stacks in zugeordnet. CloudFormation

Identitätsbasierte Richtlinien für CloudFormation

Berücksichtigen Sie die Benutzertypen, auf die Sie Zugriff benötigen AWS CloudFormation, und überlegen Sie, welche Aktionen diese Benutzer ausführen müssen. CloudFormation Sie konfigurieren Benutzerberechtigungen mithilfe identitätsbasierter Richtlinien, die Sie einem AWS Identity and Access Management (IAM-) Prinzipal zuordnen, z. B. einer Rolle oder einem Benutzer.

Wenn Sie eine identitätsbasierte Richtlinie konfigurieren, sind die Elemente, `Effect` und `Action` erforderlich. `Resource` Sie können optional auch ein `Condition` Element definieren. Weitere Informationen zu diesen Elementen finden Sie in der Referenz zu den IAM-JSON-Richtlinienelementen.

In diesem Abschnitt werden folgende Themen behandelt:

- Bewährte Methoden für die Konfiguration identitätsbasierter Richtlinien für den Zugriff mit geringsten Rechten CloudFormation
- Beispiele für identitätsbasierte Richtlinien für CloudFormation

Bewährte Methoden für die Konfiguration identitätsbasierter Richtlinien für den Zugriff mit geringsten Rechten CloudFormation

- Für IAM-Prinzipale, die Zugriffsberechtigungen benötigen CloudFormation, müssen Sie den Bedarf an Berechtigungen für den Betrieb mit dem Prinzip der geringsten Rechte abwägen. CloudFormation Um Ihnen die Einhaltung des Prinzips der geringsten Rechte zu erleichtern, empfehlen wir Ihnen, die Identität des IAM-Prinzipals anhand bestimmter Aktionen zu definieren, die es dem Prinzipal ermöglichen, Folgendes zu tun:
  - Einen Stack erstellen, aktualisieren und löschen. CloudFormation
  - Übergeben Sie eine oder mehrere Servicerollen, die über die erforderlichen Berechtigungen verfügen, um die in den CloudFormation Vorlagen definierten Ressourcen bereitzustellen. Auf diese Weise können CloudFormation Sie die Servicerolle übernehmen und die Ressourcen im Stack im Namen des IAM-Prinzipals bereitstellen.
- Die Eskalation von Rechten bezieht sich auf die Fähigkeit eines Benutzers mit Zugriff, seine Berechtigungsstufen zu erhöhen und die Sicherheit zu gefährden. Least-Privilege ist eine wichtige bewährte Methode, die dazu beitragen kann, eine Eskalation von Rechten zu verhindern. Da CloudFormation die Bereitstellung von IAM-Ressourcentypen wie Richtlinien und Rollen unterstützt wird, könnte ein IAM-Principal seine Rechte wie folgt erweitern: CloudFormation
  - Verwendung eines CloudFormation Stacks zur Bereitstellung eines IAM-Prinzipals mit hochprivilegierten Berechtigungen, Richtlinien oder Anmeldeinformationen — Um dies zu verhindern, empfehlen wir, die Zugriffsebene für IAM-Prinzipale mithilfe von Berechtigungsleitlinien einzuschränken. Berechtigungsleitlinien legen die maximalen Berechtigungen fest, die eine identitätsbasierte Richtlinie einem IAM-Prinzipal gewähren kann. Dies trägt dazu bei, eine absichtliche und unbeabsichtigte Eskalation von Rechten zu verhindern. Sie können die folgenden Arten von Richtlinien als Schutzmaßnahmen für Berechtigungen verwenden:
    - Berechtigungsgrenzen definieren die maximalen Berechtigungen, die eine identitätsbasierte Richtlinie einem IAM-Prinzipal gewähren kann. Weitere Informationen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten.
    - In AWS Organizations können Sie Dienststeuerungsrichtlinien (SCPs) verwenden, um die maximal verfügbaren Berechtigungen auf Organisationsebene zu definieren. SCPs betreffen nur IAM-Rollen und Benutzer, die von Konten in der Organisation verwaltet werden. Sie können Verbindungen SCPs zu Konten, Organisationseinheiten oder zum Stammverzeichnis der Organisation hinzufügen. Weitere Informationen zu SCP-Auswirkungen auf Berechtigungen.

- Eine CloudFormation Servicerolle erstellen, die umfangreiche Berechtigungen bietet — Um dies zu verhindern, empfehlen wir, dass Sie den identitätsbasierten Richtlinien für IAM-Prinzipale, die sie verwenden werden, die folgenden detaillierten Berechtigungen hinzufügen: CloudFormation
  - Verwenden Sie den `cloudformation:RoleARN` Bedingungsschlüssel, um zu steuern, welche CloudFormation Servicerollen der IAM-Prinzipal verwenden kann.
  - Lassen Sie die `iam:PassRole` Aktion nur für die spezifischen CloudFormation Dienstrollen zu, die der IAM-Prinzipal bestehen muss.

  Weitere Informationen finden Sie unter Einem IAM-Prinzipal Berechtigungen zur Verwendung einer CloudFormation Servicerolle gewähren in diesem Handbuch.
- Schränken Sie Berechtigungen ein, indem Sie Leitplanken für Berechtigungen verwenden, wie z. B. Berechtigungsgrenzen und SCPs, und gewähren Sie Berechtigungen mithilfe einer identitäts- oder ressourcenbasierten Richtlinie.

Beispiele für identitätsbasierte Richtlinien für CloudFormation

Dieser Abschnitt enthält Beispiele für identitätsbasierte Richtlinien, die zeigen, wie Berechtigungen erteilt und verweigert werden können. CloudFormation Anhand dieser Beispielrichtlinien können Sie damit beginnen, Ihre eigenen Richtlinien zu entwerfen, die dem Prinzip der geringsten Rechte entsprechen.

Eine Liste der CloudFormation spezifischen Aktionen und Bedingungen finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für AWS CloudFormation und AWS CloudFormation Bedingungen. Eine Liste der Ressourcentypen, die mit Bedingungen verwendet werden können, finden Sie in der Referenz zu AWS Ressourcen- und Eigenschaftstypen.

Dieser Abschnitt enthält die folgenden Beispielrichtlinien:

- Lesezugriff zulassen
- Erlaubt die Erstellung von Stacks auf der Grundlage der Vorlage
- Verweigert die Aktualisierung oder Löschung eines Stacks

Lesezugriff zulassen

Der Lesezugriff ist die Art des Zugriffs auf mit den geringsten Rechten. CloudFormation Diese Art von Richtlinie ist möglicherweise für diejenigen IAM-Prinzipale geeignet, die alle Stacks in der einsehen

möchten. CloudFormation AWS-Konto Die folgende Beispielrichtlinie gewährt Berechtigungen zum Anzeigen der Details aller CloudFormation Stacks im Konto.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources"
      ],
      "Resource": "*"
    }
  ]
}
```

Erlaubt die Erstellung von Stacks auf der Grundlage der Vorlage

Die folgende Beispielrichtlinie ermöglicht es IAM-Prinzipalen, Stacks zu erstellen, indem sie nur die CloudFormation Vorlagen verwenden, die in einem bestimmten Amazon Simple Storage Service (Amazon S3) -Bucket gespeichert sind. Der Bucket-Name lautet. `my-CFN-templates` Sie können genehmigte Vorlagen in diesen Bucket hochladen. Der `cloudformation:TemplateUrl` Bedingungsschlüssel in der Richtlinie verhindert, dass der IAM-Prinzipal andere Vorlagen zum Erstellen von Stacks verwendet.

> **Important**
>
> Erlauben Sie dem IAM-Prinzipal, schreibgeschützten Zugriff auf diesen S3-Bucket zu haben. Dadurch wird verhindert, dass der IAM-Prinzipal die genehmigten Vorlagen hinzufügt, entfernt oder ändert.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```
      "Effect": "Allow",
      "Action": [
        "cloudformation:CreateStack"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "cloudformation:TemplateUrl": "https:// my-CFN-templates.s3.amazonaws.com/*"
        }
      }
    }
  ]
}
```

Verweigert die Aktualisierung oder Löschung eines Stacks

Um bestimmte CloudFormation Stacks zu schützen, die geschäftskritische AWS Ressourcen bereitstellen, können Sie die Aktualisierungs- und Löschaktionen für diesen bestimmten Stack einschränken. Sie können diese Aktionen nur für einige bestimmte IAM-Prinzipale zulassen und sie für alle anderen IAM-Prinzipale in der Umgebung verweigern. In der folgenden Richtlinienerklärung werden Berechtigungen zum Aktualisieren oder Löschen eines bestimmten CloudFormation Stacks in einem bestimmten und verweigert. AWS-Region AWS-Konto

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "cloudformation:DeleteStack",
        "cloudformation:UpdateStack"
      ],
      "Resource": "arn:aws:cloudformation:us-east-1:123456789012:stack/
MyProductionStack/<stack_ID>"
    }
  ]
}
```

In dieser Richtlinienerklärung werden Berechtigungen zum Aktualisieren oder Löschen des `MyProductionStack` CloudFormation Stacks verweigert, der sich im `us-east-1` AWS-Region und im befindet. `123456789012` AWS-Konto Sie können die Stack-ID in der CloudFormation Konsole

einsehen. Im Folgenden finden Sie einige Beispiele dafür, wie Sie das `Resource` Element dieser Anweisung für Ihren Anwendungsfall ändern können:

- Sie können dem `Resource` Element dieser Richtlinie mehrere CloudFormation Stapel IDs hinzufügen.
- Sie können `arn:aws:cloudformation:us-east-1:123456789012:stack/*` damit verhindern, dass IAM-Prinzipale alle Stacks aktualisieren oder löschen, die sich im `us-east-1` AWS-Region und im `123456789012` Konto befinden.

Ein wichtiger Schritt ist die Entscheidung, welche Richtlinie diese Aussage enthalten soll. Sie könnten diese Aussage zu den folgenden Richtlinien hinzufügen:

- Die identitätsbasierte Richtlinie, die dem IAM-Prinzipal zugeordnet ist — Wenn Sie die Anweisung in diese Richtlinie aufnehmen, wird der spezifische IAM-Prinzipal daran gehindert, einen bestimmten Stack zu erstellen oder zu löschen. CloudFormation
- Eine dem IAM-Prinzipal zugeordnete Berechtigungsgrenze — Wenn Sie die Anweisung in diese Richtlinie aufnehmen, entsteht eine Schutzbarriere für Berechtigungen. Sie verhindert, dass mehr als ein IAM-Prinzipal einen bestimmten CloudFormation Stack erstellt oder löscht, aber es schränkt nicht alle Prinzipale in Ihrer Umgebung ein.
- Ein SCP, der einem Konto, einer Organisationseinheit oder einer Organisation zugeordnet ist — Wenn Sie die Erklärung in diese Richtlinie aufnehmen, entsteht eine Schutzbarriere für Berechtigungen. Sie verhindert, dass alle IAM-Prinzipale im Zielkonto, in der Organisationseinheit oder in der Organisation einen bestimmten Stack erstellen oder löschen. CloudFormation

  Wenn Sie jedoch nicht zulassen, dass mindestens ein IAM-Prinzipal, ein privilegierter Principal, den CloudFormation Stack aktualisiert oder löscht, können Sie bei Bedarf keine Änderungen an den über diesen Stack bereitgestellten Ressourcen vornehmen. Ein Benutzer oder eine Entwicklungspipeline (empfohlen) kann diesen privilegierten Prinzipal übernehmen. Wenn Sie die Einschränkung als SCP implementieren möchten, empfehlen wir stattdessen die folgende Richtlinienerklärung.

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

```
        "cloudformation:DeleteStack",
        "cloudformation:UpdateStack"
      ],
      "Resource": "arn:aws:cloudformation:us-east-1:123456789012:stack/
MyProductionStack/<stack_ID>",
      "Condition": {
        "ArnNotLike": {
          "aws:PrincipalARN": [
            "<ARN of the allowed privilege IAM principal>"
          ]
        }
      }
    }
  ]
}
```

In dieser Anweisung definiert das `Condition` Element den IAM-Prinzipal, der vom SCP ausgeschlossen ist. Diese Anweisung verweigert jegliche IAM-Prinzipalberechtigungen zum Aktualisieren oder Löschen von CloudFormation Stacks, es sei denn, der ARN des IAM-Prinzipals entspricht dem ARN im Element. `Condition` Der `aws:PrincipalARN` Bedingungsschlüssel akzeptiert eine Liste, was bedeutet, dass Sie je nach Bedarf in Ihrer Umgebung mehr als einen IAM-Prinzipal von den Einschränkungen ausschließen können. Ein ähnliches SCP, das Änderungen an CloudFormation Ressourcen verhindert, finden Sie unter SCP-CLOUDFORMATION-1 (). GitHub

Servicerollen für CloudFormation

Eine Servicerolle ist eine AWS Identity and Access Management (IAM-) Rolle, die es ermöglicht, AWS CloudFormation Stack-Ressourcen zu erstellen, zu aktualisieren oder zu löschen. Wenn Sie keine Servicerolle angeben, CloudFormation verwendet die Anmeldeinformationen des IAM-Prinzipals, um die Stack-Operationen auszuführen. Wenn Sie eine Servicerolle für erstellen CloudFormation und diese bei der Stack-Erstellung angeben, werden für die Ausführung der Operationen die Anmeldeinformationen der Servicerolle CloudFormation verwendet, anstatt die Anmeldeinformationen des IAM-Prinzipals.

Wenn Sie eine Servicerolle verwenden, erfordert die dem IAM-Prinzipal zugeordnete identitätsbasierte Richtlinie keine Berechtigungen zur Bereitstellung aller in der Vorlage definierten AWS Ressourcen. CloudFormation Wenn Sie nicht bereit sind, AWS Ressourcen für kritische Geschäftsabläufe über eine Entwicklungspipeline bereitzustellen (eine AWS empfohlene bewährte

Methode), kann die Verwendung einer Servicerolle eine zusätzliche Schutzebene für das Ressourcenmanagement in bieten. AWS Die Vorteile dieses Ansatzes sind:

- Die IAM-Prinzipale in Ihrer Organisation folgen einem Modell mit den geringsten Rechten, das sie daran hindert, Ressourcen in Ihrer Umgebung manuell zu erstellen oder zu ändern AWS .
- Um AWS Ressourcen zu erstellen, zu aktualisieren oder zu löschen, müssen IAM-Prinzipale Folgendes verwenden: CloudFormation Dadurch wird die Ressourcenbereitstellung über Infrastructure-as-Code standardisiert.

Um beispielsweise einen Stack zu erstellen, der eine Amazon Elastic Compute Cloud (Amazon EC2) -Instance enthält, müsste der IAM-Principal über Berechtigungen zum Erstellen von EC2 Instances gemäß seiner identitätsbasierten Richtlinie verfügen. Stattdessen CloudFormation kann er eine Servicerolle annehmen, die berechtigt ist, EC2 Instanzen im Namen des Prinzipals zu erstellen. Bei diesem Ansatz kann der IAM-Prinzipal den Stack erstellen, und Sie müssen dem IAM-Prinzipal keine allzu umfassenden Berechtigungen für einen Dienst erteilen, auf den er keinen regulären Zugriff haben sollte.

Um eine Servicerolle zum Erstellen von CloudFormation Stacks verwenden zu können, müssen IAM-Prinzipale über Berechtigungen zur Weitergabe der Servicerolle verfügen CloudFormation, und die Vertrauensrichtlinie der Servicerolle muss die Übernahme der Rolle ermöglichen. CloudFormation

In diesem Abschnitt werden folgende Themen behandelt:

- Implementierung der geringsten Rechte für Servicerollen CloudFormation
- Konfiguration von Servicerollen
- Einem IAM-Prinzipal Berechtigungen zur Verwendung einer CloudFormation Servicerolle gewähren
- Konfiguration einer Vertrauensrichtlinie für die CloudFormation Servicerolle
- Zuordnen einer Servicerolle zu einem Stack

Implementierung der geringsten Rechte für Servicerollen CloudFormation

In einer Servicerolle definieren Sie eine Berechtigungsrichtlinie, die explizit festlegt, welche Aktionen der Dienst ausführen kann. Dies sind möglicherweise nicht dieselben Aktionen, die ein IAM-Principal ausführen kann. Wir empfehlen, dass Sie von Ihren CloudFormation Vorlagen ausgehend eine Servicerolle erstellen, die dem Prinzip der geringsten Rechte entspricht.

Wenn Sie die identitätsbasierte Richtlinie eines IAM-Prinzipals so festlegen, dass nur bestimmte Servicerollen übergeben werden, und die Vertrauensrichtlinie einer Servicerolle so, dass nur bestimmte Prinzipale die Rolle übernehmen können, verhindern Sie eine mögliche Eskalation von Rechten durch Servicerollen.

Konfiguration von Servicerollen

> **Note**
>
> Servicerollen werden in IAM konfiguriert. Um eine Servicerolle zu erstellen, müssen Sie über die entsprechenden Berechtigungen verfügen. Ein IAM-Prinzipal mit der Berechtigung, eine Rolle zu erstellen und eine beliebige Richtlinie anzuhängen, kann seine eigenen Berechtigungen erweitern. AWS empfiehlt, für jeden Anwendungsfall jeweils eine AWS-Service Servicerolle zu erstellen. Nachdem Sie CloudFormation Servicerollen für Ihre Anwendungsfälle erstellt haben, können Sie Benutzern erlauben, nur die genehmigte Servicerolle an diese weiterzugeben CloudFormation. Beispiele für identitätsbasierte Richtlinien, die es Benutzern ermöglichen, Servicerollen zu erstellen, finden Sie in der IAM-Dokumentation unter Berechtigungen für Servicerollen.

Anweisungen zum Erstellen von Servicerollen finden Sie unter Eine Rolle erstellen, um Berechtigungen an eine zu delegieren. AWS-Service Legen Sie CloudFormation (`cloudformation.amazonaws.com`) als den Dienst fest, der die Rolle annehmen kann. Dadurch wird verhindert, dass ein IAM-Prinzipal die Rolle selbst übernimmt oder sie an andere Dienste weitergibt. Wenn Sie eine Servicerolle konfigurieren, sind die `Effect` `Resource` Elemente`Action`, und erforderlich. Sie können optional auch ein `Condition` Element definieren.

Weitere Informationen zu diesen Elementen finden Sie in der Referenz zu den IAM-JSON-Richtlinienelementen. Eine vollständige Liste der Aktionen, Ressourcen und Bedingungsschlüssel finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Identitäts- und Zugriffsmanagement.

Einem IAM-Prinzipal Berechtigungen zur Verwendung einer CloudFormation Servicerolle gewähren

Um Ressourcen CloudFormation mithilfe der CloudFormation Servicerolle bereitstellen zu können, muss der IAM-Prinzipal über die erforderlichen Berechtigungen zum Weitergeben der Servicerolle

verfügen. Sie können die Berechtigungen des IAM-Prinzipals so einschränken, dass nur bestimmte Rollen übergeben werden, indem Sie den ARN der Rolle in den Berechtigungen des Prinzipals angeben. Weitere Informationen finden Sie in der IAM-Dokumentation unter Einem Benutzer Berechtigungen zur Übergabe einer Rolle AWS-Service an einen gewähren.

Die folgende identitätsbasierte IAM-Richtlinienanweisung ermöglicht es dem Principal, Rollen, einschließlich Servicerollen, zu übergeben, die sich im Pfad befinden. `cfnroles` Der Principal kann keine Rollen weitergeben, die sich auf einem anderen Pfad befinden.

```
{
"Sid": "AllowPassingAppRoles",
"Effect": "Allow",
"Action": "iam:PassRole",
"Resource": "arn:aws:iam::<account ID>:role/cfnroles/*"
}
```

Ein anderer Ansatz, Principals auf bestimmte Rollen zu beschränken, besteht darin, ein Präfix für CloudFormation Servicerollennamen zu verwenden. Die folgende Richtlinienerklärung ermöglicht es IAM-Prinzipalen, nur Rollen zu übergeben, die über ein Präfix verfügen. `CFN-`

```
{
"Sid": "AllowPassingAppRoles",
"Effect": "Allow",
"Action": "iam:PassRole",
"Resource": "arn:aws:iam::<account ID>:role/CFN-*"
}
```

Zusätzlich zu den vorherigen Richtlinienanweisungen können Sie den `cloudformation:RoleARN` Bedingungsschlüssel verwenden, um weitere detaillierte Kontrollen in der identitätsbasierten Richtlinie für den Zugriff mit den geringsten Rechten bereitzustellen. Die folgende Richtlinienerklärung ermöglicht es dem IAM-Prinzipal, Stacks nur dann zu erstellen, zu aktualisieren und zu löschen, wenn sie eine bestimmte Servicerolle erfüllen. CloudFormation Als Variante können Sie die ARNs von mehr als einer CloudFormation Servicerolle im Bedingungsschlüssel definieren.

```
{
  "Sid": "RestrictCloudFormationAccess",
  "Effect": "Allow",
  "Action": [
    "cloudformation:CreateStack",
```

```
    "cloudformation:DeleteStack",
    "cloudformation:UpdateStack"
  ],
  "Resource": "arn:aws:iam::<account ID>:role/CFN-*",
  "Condition": {
    "StringEquals": {
      "cloudformation:RoleArn": [
        "<ARN of the specific CloudFormation service role>"
      ]
    }
  }
}
```

Darüber hinaus können Sie den `cloudformation:RoleARN` Bedingungsschlüssel verwenden, um einen IAM-Prinzipal daran zu hindern, eine hoch privilegierte CloudFormation Servicerolle für Stack-Operationen zu übergeben. Die einzige Änderung, die erforderlich ist, betrifft den Bedingungsoperator von `StringEquals` bis`StringNotEquals`.

```
{
  "Sid": "RestrictCloudFormationAccess",
  "Effect": "Allow",
  "Action": [
    "cloudformation:CreateStack",
    "cloudformation:DeleteStack",
    "cloudformation:UpdateStack"
  ],
  "Resource": "arn:aws:iam::<account ID>:role/CFN-*",
  "Condition": {
    "StringNotEquals": {
      "cloudformation:RoleArn": [
        "<ARN of a privilege CloudFormation service role>"
      ]
    }
  }
}
```

Konfiguration einer Vertrauensrichtlinie für die CloudFormation Servicerolle

Eine Rollenvertrauensrichtlinie ist eine erforderliche ressourcenbasierte Richtlinie, die einer IAM-Rolle zugeordnet ist. Eine Vertrauensrichtlinie definiert, welche IAM-Prinzipale die Rolle übernehmen können. In einer Vertrauensrichtlinie können Sie Benutzer, Rollen, Konten oder Dienste als Prinzipale

angeben. Um zu verhindern, dass IAM-Prinzipale Dienstrollen CloudFormation an andere Dienste weitergeben, können Sie dies in der CloudFormation Vertrauensrichtlinie der Rolle als Principal angeben.

Die folgende Vertrauensrichtlinie ermöglicht es nur dem CloudFormation Dienst, die Dienstrolle zu übernehmen.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Principal": {
      "Service": "cloudformation.amazonaws.com"
    },
    "Action": "sts:AssumeRole"
  }
}
```

Zuordnen einer Servicerolle zu einem Stack

Nachdem eine Servicerolle erstellt wurde, können Sie sie einem Stack zuordnen, wenn Sie den Stack erstellen. Weitere Informationen finden Sie unter Stack-Optionen konfigurieren. Bevor Sie eine Servicerolle angeben, stellen Sie sicher, dass die IAM-Prinzipale über die erforderlichen Berechtigungen verfügen, um sie weiterzugeben. Weitere Informationen finden Sie unter Einem IAM-Prinzipal Berechtigungen zur Verwendung einer CloudFormation Servicerolle gewähren.

CloudFormation Richtlinien stapeln

Stack-Richtlinien können dazu beitragen, zu verhindern, dass Stack-Ressourcen während eines Stack-Updates unbeabsichtigt aktualisiert oder gelöscht werden. Eine Stack-Richtlinie ist ein JSON-Dokument, das die Aktualisierungsaktionen definiert, die für bestimmte Ressourcen ausgeführt werden können. Standardmäßig kann jeder IAM-Prinzipal mit `cloudformation:UpdateStack` Berechtigungen alle Ressourcen in einem AWS CloudFormation Stack aktualisieren. Aktualisierungen können zu Unterbrechungen führen oder Ressourcen vollständig löschen und ersetzen. Sie können eine Stack-Richtlinie verwenden, um Berechtigungen mit den geringsten Rechten zu konfigurieren. Die Stack-Richtlinien können eine zusätzliche Schutzebene bieten.

Standardmäßig trägt eine Stack-Richtlinie zum Schutz aller Ressourcen im Stack bei. Der Hauptvorteil von Stack-Richtlinien besteht jedoch darin, dass sie eine detaillierte Kontrolle für

jede AWS Ressource bieten, die in einem CloudFormation Stack eingesetzt wird. Sie können eine Stack-Richtlinie verwenden, um nur bestimmte Ressourcen in einem Stack zu schützen und Aktualisierungen oder das Löschen anderer Ressourcen im selben Stack zu ermöglichen. Um Aktualisierungen für bestimmte Ressourcen zuzulassen, fügen Sie eine ausdrückliche `Allow` Erklärung für diese Ressourcen in Ihre Stack-Richtlinie ein.

Stack-Richtlinien bieten präventive Kontrollen für die CloudFormation Stacks, an die sie angehängt sind. Jeder Stack kann nur eine Stack-Richtlinie haben, aber Sie können diese Stack-Richtlinie verwenden, um alle Ressourcen innerhalb dieses Stacks zu schützen. Sie können eine Stack-Richtlinie auf mehrere Stacks anwenden.

Stellen Sie sich zum Beispiel vor, Sie haben eine Pipeline, die sensible Artefakte erzeugt und diese vorübergehend zur weiteren Verarbeitung in einem Amazon Simple Storage Service (Amazon S3) -Bucket speichert. Der S3-Bucket wird von bereitgestellt CloudFormation, und alle erforderlichen Sicherheitskontrollen sind vorhanden. Ohne Stack-Richtlinien könnte ein Entwickler das Ziel der Pipeline-Artefakte absichtlich oder unabsichtlich in einen weniger sicheren S3-Bucket ändern und sensible Daten offenlegen. Wenn Sie eine Stack-Richtlinie auf den Stack angewendet haben, verhindert diese, dass autorisierte Benutzer unerwünschte Aktualisierungs- oder Löschaktionen ausführen.

In diesem Abschnitt werden folgende Themen behandelt:

- Konfiguration von Stack-Richtlinien
- Stack-Richtlinien festlegen und überschreiben
- Stack-Richtlinien einschränken und vorschreiben

Konfiguration von Stack-Richtlinien

Wenn Sie eine Stack-Richtlinie konfigurieren, sind die Elemente`Effect`, `ActionPrincipal`, und `Resource` erforderlich. Sie können optional auch ein `Condition` Element definieren.

Wenn Sie eine Stack-Richtlinie erstellen, verhindert sie standardmäßig Aktualisierungen für alle Ressourcen im Stack. Sie passen die Stack-Richtlinie an, um zu definieren, welche Aktionen explizit zulässig sind. Wenn Sie die Richtlinie umkehren möchten, können Sie eine `Allow` Anweisung definieren, die alle Aktionen zulässt, und dann explizite `Deny` Anweisungen angeben, die Aktionen nur für bestimmte Ressourcen verhindern. Als Referenz finden Sie dieses Beispiel für eine Stack-Richtlinie in der CloudFormation Dokumentation.

Weitere Informationen zur Verwendung dieser Elemente zur Erstellung benutzerdefinierter Stack-Richtlinien und weitere Beispielrichtlinien finden Sie unter Definieren einer Stack-Richtlinie und Weitere Beispiele für Stack-Richtlinien in der CloudFormation Dokumentation.

Stack-Richtlinien festlegen und überschreiben

Nachdem Sie eine Stack-Richtlinie erstellt haben, ordnen Sie sie einem Stack zu. Wenn Sie die Stack-Richtlinie einem vorhandenen Stack zuweisen, müssen Sie die AWS Command Line Interface (AWS CLI) verwenden. Wenn Sie die Richtlinie jedoch zum Zeitpunkt der Stack-Erstellung zuweisen, können Sie entweder die CloudFormation Konsole oder die verwenden. AWS CLI Anweisungen finden Sie in der CloudFormation Dokumentation unter Eine Stack-Richtlinie einrichten.

Wenn Sie es Benutzern ermöglichen möchten, die Ressourcen im Stack zu aktualisieren oder zu löschen, müssen Sie die Stack-Richtlinie vorübergehend außer Kraft setzen. Diese Außerkraftsetzung ermöglicht es Ihnen, Aktionen mit den geschützten Ressourcen in diesem Stapel durchzuführen, die andernfalls verweigert wurden. Anweisungen finden Sie in der CloudFormation Dokumentation unter Geschützte Ressourcen aktualisieren.

Stack-Richtlinien einschränken und vorschreiben

Als bewährte Methode für Berechtigungen mit geringsten Rechten sollten Sie erwägen, von IAM-Prinzipalen die Zuweisung von Stack-Richtlinien zu verlangen und einzuschränken, welche Stack-Richtlinien IAM-Prinzipale zuweisen können. Viele IAM-Prinzipale sollten nicht berechtigt sein, benutzerdefinierte Stack-Richtlinien zu erstellen und ihren eigenen Stacks zuzuweisen.

Nachdem Sie Ihre Stack-Richtlinien erstellt haben, empfehlen wir, sie in einen S3-Bucket hochzuladen. Sie können dann auf diese Stack-Richtlinien verweisen, indem Sie den `cloudformation:StackPolicyUrl` Bedingungsschlüssel verwenden und die URL der Stack-Richtlinie im S3-Bucket angeben.

Erteilen von Berechtigungen zum Anhängen von Stack-Richtlinien

Als bewährte Methode für Berechtigungen mit den geringsten Rechten sollten Sie erwägen, einzuschränken, welche Stack-Richtlinien IAM-Prinzipale an Stacks anhängen können. CloudFormation In der identitätsbasierten Richtlinie für den IAM-Prinzipal können Sie angeben, welche Stack-Richtlinien der IAM-Prinzipal zuweisen darf. Dadurch wird verhindert, dass der IAM-Prinzipal eine Stack-Richtlinie anhängt, wodurch das Risiko einer Fehlkonfiguration verringert werden kann.

Beispielsweise kann eine Organisation unterschiedliche Teams mit unterschiedlichen Anforderungen haben. Dementsprechend erstellt jedes Team Stack-Richtlinien für seine teamspezifischen CloudFormation Stacks. Wenn in einer gemeinsamen Umgebung alle Teams ihre Stack-Richtlinien im selben S3-Bucket speichern, kann ein Teammitglied eine Stack-Richtlinie anhängen, die zwar verfügbar, aber nicht für die Stacks seines Teams vorgesehen ist. CloudFormation Um dieses Szenario zu vermeiden, können Sie eine Richtlinienerklärung definieren, die es IAM-Prinzipalen ermöglicht, nur bestimmte Stack-Richtlinien anzuhängen.

Die folgende Beispielrichtlinie ermöglicht es dem IAM-Prinzipal, Stack-Richtlinien anzuhängen, die in einem teamspezifischen Ordner in einem S3-Bucket gespeichert sind. In diesem Bucket können Sie genehmigte Stack-Richtlinien speichern.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:SetStackPolicy"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "cloudformation:StackPolicyUrl": "<Bucket URL>/<Team folder>/*"
        }
      }
    }
  ]
}
```

Diese Richtlinienanweisung erfordert nicht, dass ein IAM-Prinzipal jedem Stack eine Stack-Richtlinie zuweist. Selbst wenn der IAM-Prinzipal berechtigt ist, Stacks mit einer bestimmten Stack-Richtlinie zu erstellen, könnte er sich dafür entscheiden, einen Stack zu erstellen, der keine Stack-Richtlinie hat.

Stack-Richtlinien erforderlich

Um sicherzustellen, dass alle IAM-Prinzipale ihren Stacks Stack-Richtlinien zuweisen, können Sie eine Service Control Policy (SCP) oder eine Berechtigungsgrenze als präventive Schutzmaßnahme definieren.

Die folgende Beispielrichtlinie zeigt, wie Sie ein SCP konfigurieren können, bei dem IAM-Prinzipale beim Erstellen eines Stacks eine Stack-Richtlinie zuweisen müssen. Wenn der IAM-Prinzipal keine Stack-Richtlinie anfügt, kann er den Stack nicht erstellen. Darüber hinaus verhindert diese Richtlinie, dass IAM-Prinzipale mit Stack-Aktualisierungsberechtigungen die Stack-Richtlinie während eines Updates entfernen. Die Richtlinie schränkt die `cloudformation:UpdateStack` Aktion mithilfe des Bedingungsschlüssels ein. `cloudformation:StackPolicyUrl`

```
        {
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack"
      ],
      "Resource": "*",
      "Condition": {
        "Null": {
          "cloudformation:StackPolicyUrl": "true"
        }
      }
    }
  ]
}
```

Indem Sie diese Richtlinienerklärung in ein SCP und nicht in eine Berechtigungsgrenze aufnehmen, können Sie Ihre Guardrail auf alle Konten in der Organisation anwenden. Dies kann Folgendes bewirken:

1. Reduzieren Sie den Aufwand, die Richtlinie einzeln an mehrere IAM-Prinzipale in einem anzuhängen. AWS-Konto Berechtigungsgrenzen können nur einem IAM-Prinzipal direkt zugewiesen werden.
2. Reduzieren Sie den Aufwand, mehrere Kopien der Berechtigungsgrenze für verschiedene AWS-Konten zu erstellen und zu verwalten. Dadurch wird das Risiko von Konfigurationsfehlern bei mehreren identischen Berechtigungsgrenzen reduziert.

> **Note**
>
> SCPs und Berechtigungsgrenzen sind Berechtigungsleitplanken, die die maximal verfügbaren Berechtigungen für IAM-Prinzipale in einem Konto oder einer Organisation definieren. Diese Richtlinien gewähren den IAM-Prinzipalen keine Berechtigungen. Wenn Sie die Anforderung standardisieren möchten, dass alle IAM-Prinzipale in Ihrem Konto oder Ihrer Organisation Stack-Richtlinien zuweisen, müssen Sie sowohl Richtlinien für Berechtigungen als auch identitätsbasierte Richtlinien verwenden.

Konfiguration von Berechtigungen mit den geringsten Rechten für Ressourcen, die bereitgestellt werden über CloudFormation

AWS CloudFormation ermöglicht es Ihnen, viele verschiedene Arten von AWS Ressourcen bereitzustellen. Bereitgestellte Ressourcen benötigen eigene Berechtigungen, um wie vorgesehen zu funktionieren und um zu konfigurieren, wer Zugriff auf diese Ressourcen hat. Im vorherigen Kapitel wurden Optionen für die Konfiguration von Zugriffs- und Nutzungsberechtigungen für den CloudFormation Dienst beschrieben. In diesem Kapitel wird beschrieben, wie Sie das Prinzip der geringsten Rechte auf Ressourcen anwenden können, die über CloudFormation bereitgestellt werden.

In diesem Leitfaden wäre es praktisch unmöglich, die Sicherheitsempfehlungen und bewährten Methoden für jeden AWS Ressourcentyp zu überprüfen, über den bereitgestellt werden kann. CloudFormation Wenn Sie Fragen zu einem bestimmten Dienst haben, empfehlen wir Ihnen, die Dokumentation für diesen Dienst zu lesen. Die meisten AWS-Service Dokumente enthalten einen Sicherheitsabschnitt und Informationen zu den Berechtigungen, die für die Nutzung dieses Dienstes erforderlich sind. Eine vollständige Liste der AWS-Service Dokumentation finden Sie unter AWS Dokumentation.

Im Folgenden finden Sie allgemeine, dienstunabhängige Schritte, die Sie ergreifen können, um CloudFormation Vorlagen zu erstellen, die dem Prinzip der geringsten Rechte entsprechen:

1. Erstellen Sie eine Liste der Ressourcen, mit denen Sie die Bereitstellung planen. CloudFormation
2. In der AWS Dokumentation finden Sie die entsprechenden Dienste und lesen Sie sich die Abschnitte zu Sicherheit und Zugriffsverwaltung durch. Dies hilft Ihnen, die dienstspezifischen Anforderungen und Empfehlungen zu verstehen.
3. Verwenden Sie die Informationen, die Sie in den vorherigen Schritten gesammelt haben, um CloudFormation Vorlagen und zugehörige Richtlinien zu entwerfen, die nur die erforderlichen Berechtigungen zulassen und alle anderen verweigern.

Als Nächstes gibt dieser Leitfaden anhand eines realen Anwendungsfalls ein Beispiel dafür, wie Sie das Prinzip der geringsten Rechte in CloudFormation Vorlagen anwenden können.

Beispiel: Amazon S3 S3-Bucket zum Speichern von Pipeline-Artefakten

In diesem Beispiel wird ein Amazon Simple Storage Service (Amazon S3) -Bucket erstellt, der zum Speichern von AWS CodeBuildProjektartefakten verwendet wird. AWS CodePipelineverwendet diese gespeicherten Artefakte. Sie können diesen S3-Bucket über Servicerollen zulassen CodeBuild und CodePipeline darauf zugreifen, und Sie kontrollieren diesen Zugriff mithilfe einer Amazon S3 S3-Bucket-Richtlinie. Im Folgenden sind die in diesem Beispiel verwendeten Ressourcennamen aufgeführt:

- `Deployfiles_build`ist der Name des CodeBuild Projekts.
- `Deployment-Pipeline`ist der Name der Pipeline in CodePipeline.

Definieren Sie den Amazon S3 S3-Bucket

Zunächst definieren Sie den S3-Bucket in der CloudFormation Vorlage, bei der es sich um eine YAML-formatierte Textdatei handelt.

```
amzn-s3-demo-bucket:
  Type: AWS::S3::Bucket
  Properties:
    PublicAccessBlockConfiguration:
        BlockPublicAcls: true
        BlockPublicPolicy: true
        IgnorePublicAcls: true
        RestrictPublicBuckets: true
```

Definieren Sie die Amazon S3 S3-Bucket-Richtlinie

Als Nächstes erstellen Sie in der CloudFormation Vorlage eine Bucket-Richtlinie, die nur dem `Deployfiles_build` Projekt und der `Deployment-Pipeline` Pipeline den Zugriff auf den Bucket ermöglicht.

```
MyBucketPolicy:
  Type: AWS::S3::BucketPolicy
  Properties:
    Bucket: !Ref amzn-s3-demo-bucket
    PolicyDocument:
      Version: "2012-10-17"
```

```
      Statement:
      - Sid: "S3ArtifactRepoAccess"
        Effect: Allow
        Action:
          - ‘s3:GetObject'
          - ‘s3:GetObjectVersion'
          - ‘s3:PutObject'
          - ‘s3:GetBucketVersioning'
        Resource:
          - !Sub ‘arn:aws:s3:::${amzn-s3-demo-bucket}'
          - !Sub ‘arn:aws:s3:::${amzn-s3-demo-bucket}/*'
        Principal:
          Service:
            - codebuild.amazonaws.com
            - codepipeline.amazonaws.com
        Condition:
          StringLike:
            ‘aws:SourceArn':
              - !Sub ‘arn:aws:codebuild:${AWS::Region}:${AWS::AccountId}:project/
Deployfiles_build'
              - !Sub ‘arn:aws:codepipeline:${AWS::Region}:${AWS::AccountId}:Deployment-
Pipeline'
              - !Sub ‘arn:aws:codepipeline:${AWS::Region}:${AWS::AccountId}:Deployment-
Pipeline/*'
```

Beachten Sie Folgendes zu dieser Bucket-Richtlinie:

- Das `Resource` Element listet zwei verschiedene Ressourcentypen auf, die die folgenden Amazon Resource Name (ARN) -Formate verwenden:
  - Das ARN-Format eines S3-Objekts ist`arn:$<Partition>:s3:::$<BucketName>/$<ObjectName>`.
  - Das ARN-Format eines S3-Buckets ist`arn:$<Partition>:s3:::$<BucketName>`.

  `s3:GetObjects3:GetObjectVersion`, und `s3:PutObject` erfordern einen S3-Objektressourcentyp und `s3:GetBucketVersioning` erfordert einen S3-Bucket-Ressourcentyp. Weitere Informationen zu den erforderlichen Ressourcentypen für jede Aktion finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon S3.
- Das `Principal` Element listet die Entitäten auf, die die in der Erklärung definierten Amazon S3 S3-Aktionen ausführen dürfen. In diesem Fall dürfen nur CodeBuild und CodePipeline dürfen diese Aktionen ausführen.

- Das `Condition` Element schränkt den Zugriff auf den S3-Bucket weiter ein, sodass nur das `Deployfiles_build` CodeBuild Projekt, die `Deployment-Pipeline` CodePipeline Pipeline und die Pipeline-Aktionen auf den Bucket zugreifen können.

Erstellen Sie die Servicerollen

Die Bucket-Richtlinie steuert zwar den Zugriff auf den Bucket, gewährt aber keine Berechtigungen für den Bucket CodeBuild und den CodePipeline Zugriff darauf. Um Zugriff zu gewähren, müssen Sie für jeden Dienst eine Servicerolle erstellen und jedem Dienst die folgende Anweisung hinzufügen. Die Dienstrollen für CodeBuild und CodePipeline ermöglichen den Diensten den Zugriff auf den S3-Bucket und seine Objekte.

```
Sid: "ViewAccessToS3ArtifactRepo"
Effect: Allow
Action:
  - ‘s3:GetObject'
  - ‘s3:GetObjectVersion'
  - ‘s3:PutObject'
  - ‘s3:GetBucketVersioning'
Resource:
  - !Sub ‘arn:aws:s3:::${BuildArtifactsBucket}'
  - !Sub ‘arn:aws:s3:::${BuildArtifactsBucket}/*'
```

Bewährte Methoden für Berechtigungen mit den geringsten Rechten für AWS CloudFormation

In diesem Leitfaden werden verschiedene Ansätze und einige Arten von Richtlinien beschrieben, mit denen Sie den Zugriff auf Ressourcen mit den geringsten Rechten AWS CloudFormation und die bereitgestellten Ressourcen konfigurieren können. CloudFormation Dieser Leitfaden konzentriert sich auf die Konfiguration des Zugriffs CloudFormation über IAM-Prinzipale, Servicerollen und Stack-Richtlinien. Die enthaltenen Empfehlungen und bewährten Methoden sollen dazu beitragen, Ihre Konten und Stack-Ressourcen vor unbeabsichtigten Aktionen autorisierter Benutzer und vor böswilligen Akteuren zu schützen, die möglicherweise übermäßige Berechtigungen ausnutzen.

Im Folgenden finden Sie eine Zusammenfassung der in diesem Leitfaden erläuterten bewährten Methoden. Diese bewährten Methoden können Ihnen helfen, bei der Konfiguration von Nutzungsberechtigungen CloudFormation und Ressourcen, die bereitgestellt werden, das Prinzip der geringsten Rechte einzuhalten: CloudFormation

- Ermitteln Sie, welche Zugriffsebene Benutzer und Teams benötigen, um den CloudFormation Service zu nutzen, und gewähren Sie nur den erforderlichen Mindestzugriff. Gewähren Sie beispielsweise Praktikanten und Auditoren Lesezugriff und erlauben Sie diesen Benutzertypen nicht, Stacks zu erstellen, zu aktualisieren oder zu löschen.
- Für IAM-Prinzipale, die mehrere Arten von AWS Ressourcen über CloudFormation Stacks bereitstellen müssen, sollten Sie die Verwendung von Servicerollen in Betracht ziehen, um die Bereitstellung von Ressourcen im Namen des Prinzipals CloudFormation zu ermöglichen, anstatt den Zugriff auf diese Ressourcen AWS-Services in den identitätsbasierten Richtlinien des Prinzipals zu konfigurieren.
- Verwenden Sie in identitätsbasierten Richtlinien für IAM-Prinzipale den `cloudformation:RoleARN` Bedingungsschlüssel, um zu steuern, welche Servicerollen übergeben werden können. CloudFormation
- Gehen Sie wie folgt vor, um eine Eskalation von Rechten zu verhindern:
  - Überwachen Sie strikt alle IAM-Prinzipale, die Zugriff auf den CloudFormation Service haben, sowie deren Zugriffsebenen.
  - Überwachen Sie genau, welche Benutzer auf diese IAM-Prinzipale zugreifen können.
  - Überwachen Sie die Aktivität von IAM-Prinzipalen, an die eine privilegierte Servicerolle übergeben können. CloudFormation Auch wenn sie aufgrund ihrer identitätsbasierten Richtlinie

möglicherweise nicht berechtigt sind, IAM-Ressourcen zu erstellen, könnte die Dienstrolle, die sie übergeben können, IAM-Ressourcen erzeugen.

- Geben Sie bei der Erstellung eines Stack mit kritischen Ressourcen immer auch eine Stack-Richtlinie an. Dies kann dazu beitragen, kritische Stack-Ressourcen vor unbeabsichtigten Aktualisierungen zu schützen, die dazu führen könnten, dass diese Ressourcen unterbrochen oder ersetzt werden.
- Informationen zu Ressourcen CloudFormation, die über bereitgestellt werden, finden Sie in den Empfehlungen zur Zugriffsverwaltung und den bewährten Sicherheitsmethoden für diesen Dienst.
- Als Ergänzung zu den Empfehlungen in diesem Leitfaden für identitätsbasierte Richtlinien und ressourcenbasierte Richtlinien sollten Sie die Implementierung zusätzlicher Sicherheitskontrollen für Berechtigungen mit den geringsten Rechten in Betracht ziehen, z. B. Richtlinien zur Dienststeuerung () und Berechtigungsgrenzen. SCPs Weitere Informationen finden Sie unter Nächste Schritte.

Die CloudFormation Dokumentation enthält zusätzliche bewährte Methoden und bewährte Sicherheitsmethoden, die Ihnen helfen können, die Nutzung effektiver und sicherer zu gestalten. CloudFormation Weitere Informationen finden Sie Bewährte Methoden für die Konfiguration identitätsbasierter Richtlinien für den Zugriff mit geringsten Rechten CloudFormation in diesem Handbuch.

Nächste Schritte

Anhand der Informationen und Beispiele in diesem Leitfaden können Sie beginnen, das Prinzip der geringsten Rechte in Ihrem Unternehmen anzuwenden. Wir empfehlen Ihnen, die zusätzlichen Ressourcen in Ressourcen diesem Abschnitt zu lesen, der Dokumentationsverweise und Tools enthält, mit denen Sie Ihre Richtlinien verfeinern können.

Dieses Handbuch soll Ihnen helfen, mit der Implementierung des Zugriffs mit den geringsten Rechten für zu beginnen. AWS CloudFormation Es gibt jedoch weitere Arten von Richtlinien, die Ihnen helfen können, das Prinzip der geringsten Rechte in Ihrem Unternehmen zu stärken. Je nach Ihrer Umgebung und Ihren Geschäftsanforderungen möchten Sie möglicherweise zusätzliche Kontrollen implementieren, die in diesem Handbuch nicht behandelt werden. Als nächsten Schritt und für weitere Informationen empfehlen wir Ihnen, die folgenden Themen im Zusammenhang mit den geringsten Rechten und der Konfiguration von Zugriff und Berechtigungen zu lesen:

- Berechtigungsgrenzen für IAM-Entitäten
- Richtlinien zur Dienststeuerung (SCP)
- Rollen für kontoübergreifenden Zugriff
- Identitätsverbund
- Informationen, auf die zuletzt zugegriffen wurde, für IAM anzeigen

Mit den folgenden Tools können Sie den Zugriff und die Berechtigungen mit den geringsten Rechten überwachen für: CloudFormation

- AWS Identity and Access Management Access Analyzer
- Sie können die Registerkarte Access Advisor in der AWS Identity and Access Management (IAM-) Konsole verwenden, um zu viele Berechtigungen für IAM-Identitäten zu identifizieren. Ein Beispiel finden Sie unter Verschärfung der S3-Berechtigungen für Ihre IAM-Benutzer und -Rollen mithilfe des Zugriffsverlaufs von S3-Aktionen (Blogbeitrag).AWS
- Sie können ein Linting-Tool wie cfn-policy-validator(GitHub) verwenden, um zu viele Berechtigungen zu identifizieren.

Wenn Sie mit der Erstellung und Verwaltung von CloudFormation Berechtigungen vertraut sind, empfiehlt es sich, zur Bereitstellung Ihrer Vorlagen CI/CD-Pipelines (Continuous Integration and

Continuous Delivery) zu verwenden. CloudFormation Dies reduziert das Risiko menschlicher Fehler und beschleunigt Ihren Bereitstellungsprozess.

Ressourcen

AWS CloudFormation Dokumentation

- Steuerung des Zugriffs mit AWS Identity and Access Management
- AWS Referenz zu Ressourcen- und Eigenschaftstypen
- AWS CloudFormation Stack-Optionen einstellen
- AWS CloudFormation Servicerolle

AWS Identity and Access Management (IAM) -Dokumentation

- Richtlinien und Berechtigungen in IAM
- IAM-JSON-Richtlinienelementreferenz
- Auswertungslogik für Richtlinien
- AWS-Services die mit IAM funktionieren
- Erstellen einer Rolle zur Delegierung von Berechtigungen an eine AWS-Service
- Das Confused-Deputy-Problem
- Bewährte Methoden für die Sicherheit in IAM

Andere Referenzen AWS

- Aktionen, Ressourcen und Bedingungsschlüssel für AWS-Services (Service Authorization Reference)
- Zugriff mit den geringsten Rechten gewähren (AWS Well-Architected Framework)
- Techniken für das Schreiben von IAM-Richtlinien mit den geringsten Rechten (Blogbeitrag)AWS

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
Signifikante Aktualisierungen	Wir haben die Leitlinien und die Muster der Grundsatz erklärungen erheblich überarbeitet und verfeinert, um allgemeine Anwendungsfälle in Unternehmen zu berücksic htigen.	5. Mai 2023
Erste Veröffentlichung	—	9. März 2023

AWS Glossar zu präskriptiven Leitlinien

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

Zahlen

7 Rs

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

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

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

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

A

ABAC

Siehe attributbasierte Zugriffskontrolle.

abstrahierte Dienste

Siehe Managed Services.

ACID

Siehe Atomarität, Konsistenz, Isolierung und Haltbarkeit.

Aktiv-Aktiv-Migration

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

Aktiv-Passiv-Migration

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

Aggregatfunktion

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

AI

Siehe künstliche Intelligenz.

AIOps

Siehe Operationen im Bereich künstliche Intelligenz.

Anonymisierung

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

Anti-Muster

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

Anwendungssteuerung

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

Anwendungsportfolio

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

künstliche Intelligenz (KI)

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

Operationen mit künstlicher Intelligenz (AIOps)

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

Asymmetrische Verschlüsselung

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

Atomizität, Konsistenz, Isolierung, Haltbarkeit (ACID)

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

Attributbasierte Zugriffskontrolle (ABAC)

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

maßgebliche Datenquelle

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

Availability Zone

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

AWS Framework für die Einführung der Cloud (AWS CAF)

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

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

AWS Workload-Qualifizierungsrahmen (AWS WQF)

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

B

schlechter Bot

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

BCP

Siehe Planung der Geschäftskontinuität.

Verhaltensdiagramm

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

Big-Endian-System

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

Binäre Klassifikation

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

Bloom-Filter

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

Blau/Grün-Bereitstellung

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

Bot

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

Botnetz

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

branch

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

Zugang durch Glasbruch

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

Brownfield-Strategie

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

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

Puffer-Cache

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

Geschäftsfähigkeit

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

Planung der Geschäftskontinuität (BCP)

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

C

CAF

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

Bereitstellung auf Kanaren

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

CCoE

Weitere Informationen finden Sie im Cloud Center of Excellence.

CDC

Siehe Erfassung von Änderungsdaten.

Erfassung von Datenänderungen (CDC)

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

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

Chaos-Technik

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

CI/CD

Siehe Continuous Integration und Continuous Delivery.

Klassifizierung

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

clientseitige Verschlüsselung

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

Cloud-Exzellenzzentrum (CCoE)

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

Cloud Computing

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

Cloud-Betriebsmodell

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

Phasen der Einführung der Cloud

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

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

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

CMDB

Siehe Datenbank für das Konfigurationsmanagement.

Code-Repository

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

Kalter Cache

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

Kalte Daten

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

Computer Vision (CV)

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

Drift in der Konfiguration

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

Verwaltung der Datenbankkonfiguration (CMDB)

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

Konformitätspaket

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

Kontinuierliche Bereitstellung und kontinuierliche Integration (CI/CD)

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

CV

Siehe Computer Vision.

D

Daten im Ruhezustand

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

Datenklassifizierung

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

Datendrift

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

Daten während der Übertragung

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

Datennetz

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

Datenminimierung

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

Datenperimeter

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

Vorverarbeitung der Daten

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

Herkunft der Daten

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

betroffene Person

Eine Person, deren Daten gesammelt und verarbeitet werden.

Data Warehouse

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

Datenbankdefinitionssprache (DDL)

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

Datenbankmanipulationssprache (DML)

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

DDL

Siehe Datenbankdefinitionssprache.

Deep-Ensemble

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

Deep Learning

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

defense-in-depth

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

delegierter Administrator

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

Einsatz

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

Entwicklungsumgebung

Siehe Umgebung.

Detektivische Kontrolle

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

Abbildung des Wertstroms in der Entwicklung (DVSM)

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

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

digitaler Zwilling

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

Maßtabelle

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

Katastrophe

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

Disaster Recovery (DR)

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

DML

Siehe Sprache zur Datenbankmanipulation.

Domainorientiertes Design

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

DR

Siehe Disaster Recovery.

Erkennung von Driften

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

DVSM

Siehe Abbildung des Wertstroms in der Entwicklung.

E

EDA

Siehe explorative Datenanalyse.

EDI

Siehe elektronischer Datenaustausch.

Edge-Computing

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

elektronischer Datenaustausch (EDI)

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

Verschlüsselung

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

Verschlüsselungsschlüssel

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

Endianismus

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

Endpunkt

Siehe Service-Endpunkt.

Endpunkt-Services

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

Unternehmensressourcenplanung (ERP)

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

Envelope-Verschlüsselung

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

Umgebung

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

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

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

Epics

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

ERP

Siehe Enterprise Resource Planning.

Explorative Datenanalyse (EDA)

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

F

Faktentabelle

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

schnell scheitern

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

Grenze zur Fehlerisolierung

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

Feature-Zweig

Siehe Zweig.

Features

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

Bedeutung der Feature

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

Featuretransformation

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

Eingabeaufforderung mit wenigen Klicks

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

FGAC

Siehe detaillierte Zugriffskontrolle.

Feinkörnige Zugriffskontrolle (FGAC)

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

Flash-Cut-Migration

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

FM

Siehe Fundamentmodell.

Fundamentmodell (FM)

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

G

Generative KI

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

Geoblocking

Siehe geografische Einschränkungen.

Geografische Einschränkungen (Geoblocking)

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

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

Gitflow-Workflow

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

goldenes Bild

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

Greenfield-Strategie

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

Integritätsschutz

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

H

HEKTAR

Siehe Hochverfügbarkeit.

Heterogene Datenbankmigration

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

hohe Verfügbarkeit (HA)

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

historische Modernisierung

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

Daten zurückhalten

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

Homogene Datenbankmigration

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

heiße Daten

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

Hotfix

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

Hypercare-Phase

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

I

IaC

Sehen Sie Infrastruktur als Code.

Identitätsbasierte Richtlinie

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

Leerlaufanwendung

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

IIoT

Siehe Industrielles Internet der Dinge.

unveränderliche Infrastruktur

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

Eingehende (ingress) VPC

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

Inkrementelle Migration

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

Industrie 4.0

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

Infrastruktur

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

Infrastructure as Code (IaC)

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

industrielles Internet der Dinge (T) IIo

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

Inspektions-VPC

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

Internet of Things (IoT)

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

Interpretierbarkeit

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

IoT

Siehe Internet der Dinge.

IT information library (ITIL, IT-Informationsbibliothek)

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

T service management (ITSM, IT-Servicemanagement)

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

BIS

Siehe IT-Informationsbibliothek.

ITSM

Siehe IT-Servicemanagement.

L

Labelbasierte Zugangskontrolle (LBAC)

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

Landing Zone

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

großes Sprachmodell (LLM)

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

Große Migration

Eine Migration von 300 oder mehr Servern.

SCHWARZ

Siehe Labelbasierte Zugriffskontrolle.

Geringste Berechtigung

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

Lift and Shift

Siehe 7 Rs.

Little-Endian-System

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

LLM

Siehe großes Sprachmodell.

Niedrigere Umgebungen

Siehe Umgebung.

M

Machine Learning (ML)

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

Hauptzweig

Siehe Filiale.

Malware

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

verwaltete Dienste

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

Manufacturing Execution System (MES)

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

MAP

Siehe Migration Acceleration Program.

Mechanismus

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

Mitgliedskonto

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

MES

Siehe Manufacturing Execution System.

Message Queuing-Telemetrietransport (MQTT)

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

Microservice

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

Microservices-Architekturen

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

Migration Acceleration Program (MAP)

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

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

Migration in großem Maßstab

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

Migrationsfabrik

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

Migrationsmetadaten

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

Migrationsmuster

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

Migration Portfolio Assessment (MPA)

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

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

Migration Readiness Assessment (MRA)

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

Migrationsstrategie

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

ML

Siehe maschinelles Lernen.

Modernisierung

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

Bewertung der Modernisierungsfähigkeit

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

Monolithische Anwendungen (Monolithen)

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

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

MPA

Siehe Bewertung des Migrationsportfolios.

MQTT

Siehe Message Queuing-Telemetrietransport.

Mehrklassen-Klassifizierung

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

veränderbare Infrastruktur

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

O

OAC

Weitere Informationen finden Sie unter Origin Access Control.

EICHE

Siehe Zugriffsidentität von Origin.

COM

Siehe organisatorisches Change-Management.

Offline-Migration

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

OI

Siehe Betriebsintegration.

OLA

Siehe Vereinbarung auf operativer Ebene.

Online-Migration

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

OPC-UA

Siehe Open Process Communications — Unified Architecture.

Offene Prozesskommunikation — Einheitliche Architektur (OPC-UA)

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

Vereinbarung auf Betriebsebene (OLA)

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

Überprüfung der Betriebsbereitschaft (ORR)

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

Betriebstechnologie (OT)

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

Betriebsintegration (OI)

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

Organisationspfad

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

Organisatorisches Veränderungsmanagement (OCM)

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

Ursprungszugriffskontrolle (OAC)

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

Ursprungszugriffsidentität (OAI)

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

ORR

Weitere Informationen finden Sie unter Überprüfung der Betriebsbereitschaft.

NICHT

Siehe Betriebstechnologie.

Ausgehende (egress) VPC

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

P

Berechtigungsgrenze

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

persönlich identifizierbare Informationen (PII)

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

Personenbezogene Daten

Siehe persönlich identifizierbare Informationen.

Playbook

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

PLC

Siehe programmierbare Logiksteuerung.

PLM

Siehe Produktlebenszyklusmanagement.

policy

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

Polyglotte Beharrlichkeit

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

Portfoliobewertung

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

predicate

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

Prädikat Pushdown

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

Präventive Kontrolle

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

Prinzipal

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

Datenschutz von Natur aus

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

Privat gehostete Zonen

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

proaktive Steuerung

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

Produktlebenszyklusmanagement (PLM)

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

Produktionsumgebung

Siehe Umgebung.

Speicherprogrammierbare Steuerung (SPS)

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

schnelle Verkettung

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

Pseudonymisierung

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

publish/subscribe (pub/sub)

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

Q

Abfrageplan

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

Abfrageplanregression

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

R

RACI-Matrix

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

RAG

Siehe Erweiterte Generierung beim Abrufen.

Ransomware

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

RASCI-Matrix

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

RCAC

Siehe Zugriffskontrolle für Zeilen und Spalten.

Read Replica

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

neu strukturieren

Siehe 7 Rs.

Recovery Point Objective (RPO)

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

Wiederherstellungszeitziel (RTO)

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

Refaktorierung

Siehe 7 Rs.

Region

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

Regression

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

rehosten

Siehe 7 Rs.

Veröffentlichung

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

umziehen

Siehe 7 Rs.

neue Plattform

Siehe 7 Rs.

Rückkauf

Siehe 7 Rs.

Ausfallsicherheit

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

Ressourcenbasierte Richtlinie

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

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

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

Reaktive Kontrolle

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

Beibehaltung

Siehe 7 Rs.

zurückziehen

Siehe 7 Rs.

Retrieval Augmented Generation (RAG)

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

Drehung

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

Zugriffskontrolle für Zeilen und Spalten (RCAC)

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

RPO

Siehe Recovery Point Objective.

RTO

Siehe Ziel für die Erholungszeit.

Runbook

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

S

SAML 2.0

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

SCADA

Siehe Aufsichtskontrolle und Datenerfassung.

SCP

Siehe Richtlinie zur Dienstkontrolle.

Secret

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

Sicherheit durch Design

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

Sicherheitskontrolle

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

Härtung der Sicherheit

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

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

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

Automatisierung von Sicherheitsreaktionen

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

Serverseitige Verschlüsselung

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

Service-Kontrollrichtlinie (SCP)

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

Service-Endpunkt

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

Service Level Agreement (SLA)

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

Service-Level-Indikator (SLI)

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

Service-Level-Ziel (SLO)

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

Modell der geteilten Verantwortung

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

SIEM

Siehe Sicherheitsinformations- und Event-Management-System.

Single Point of Failure (SPOF)

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

SLA

Siehe Service Level Agreement.

SLI

Siehe Service-Level-Indikator.

ALSO

Siehe Service-Level-Ziel.

split-and-seed Modell

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

SPOTTEN

Siehe Single Point of Failure.

Sternschema

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

Strangler-Fig-Muster

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

Subnetz

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

Aufsichtskontrolle und Datenerfassung (SCADA)

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

Symmetrische Verschlüsselung

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

synthetisches Testen

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

Systemaufforderung

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

T

tags

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

Zielvariable

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

Aufgabenliste

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

Testumgebungen

Siehe Umgebung.

Training

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

Transit-Gateway

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

Stammbasierter Workflow

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

Vertrauenswürdiger Zugriff

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

Optimieren

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

Zwei-Pizzen-Team

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

U

Unsicherheit

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

undifferenzierte Aufgaben

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

höhere Umgebungen

Siehe Umgebung.

V

Vacuuming

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

Versionskontrolle

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

VPC-Peering

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

Schwachstelle

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

W

Warmer Cache

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

warme Daten

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

Fensterfunktion

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

Workload

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

Workstream

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

WURM

Sehen Sie einmal schreiben, viele lesen.

WQF

Siehe AWS Workload-Qualifizierungsrahmen.

einmal schreiben, viele lesen (WORM)

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

Z

Zero-Day-Exploit

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

Zero-Day-Sicherheitslücke

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

Eingabeaufforderung ohne Zwischenfälle

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

Zombie-Anwendung

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

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