AWSWeißbuch

Bewährte Methoden für das Taggen von AWS-Ressourcen

Bewährte Methoden für das Taggen von AWS-Ressourcen: AWSWeißbuch

Table of Contents

Bewährte Methoden für das Markieren von AWS-Ressourcen

Datum der Veröffentlichung: 30. März 2023 () Dokumentversionen

Amazon Web Services (AWS) können Sie vielen Ihrer AWS Ressourcen in Form von Tags zuweisen. Jedes Tag ist eine einfache Bezeichnung, die aus einem Schlüssel und einem optionalen Wert besteht, um Informationen über die Ressource oder Daten, die auf dieser Ressource gespeichert sind, zu speichern. Dieses Whitepaper konzentriert sich auf die Kennzeichnung von Anwendungsfällen, Strategien, Techniken und Tools, die Ihnen helfen können, Ressourcen nach Zweck, Team, Umgebung oder anderen für Ihr Unternehmen relevanten Kriterien zu kategorisieren. Durch die Implementierung einer konsistenten Tagging-Strategie können Sie Ressourcen leichter filtern und suchen, Kosten und Nutzung überwachen und Ihre Umgebung verwalten. AWS

Dieses paper baut auf den Praktiken und Anleitungen auf, die im Whitepaper Organizing Your AWS Environment Using Multiple Accounts beschrieben wurden. Es wird empfohlen, dieses Whitepaper vor diesem zu lesen. AWSempfiehlt, dass Sie Ihr Cloud-Fundament auf ganzheitliche Weise einrichten. Weitere Informationen finden Sie unter Establishing your Cloud Foundation on AWS.

Sind Sie Well-Architected?

Das AWSWell-Architected Framework hilft Ihnen dabei, die Vor- und Nachteile der Entscheidungen zu verstehen, die Sie beim Aufbau von Systemen in der Cloud treffen. Die sechs Säulen des Frameworks ermöglichen es Ihnen, bewährte Architekturpraktiken für den Entwurf und Betrieb zuverlässiger, sicherer, effizienter, kostengünstiger und nachhaltiger Systeme kennenzulernen. Mithilfe des AWS Well-Architected Tool, das kostenlos im verfügbar ist AWS Management Console, können Sie Ihre Workloads anhand dieser bewährten Methoden überprüfen, indem Sie für jede Säule eine Reihe von Fragen beantworten.

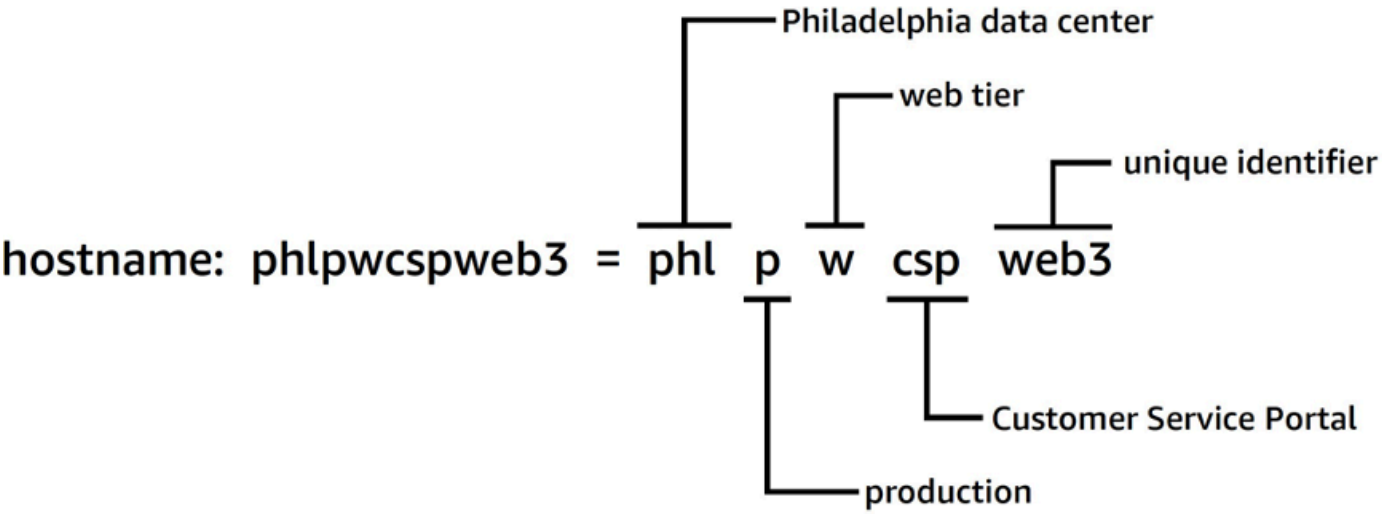
Weitere Expertentipps und bewährte Methoden für Ihre Cloud-Architektur — Referenzarchitekturbereitstellungen, Diagramme und Whitepapers — finden Sie im Architecture Center. AWS

Einführung

AWSmacht es einfach, Ihre Workloads bereitzustellen, AWS indem Ressourcen wie Amazon EC2 EC2-Instances, AmazonEBS-Volumes, Sicherheitsgruppen und Funktionen erstellt werden. AWS

Lambda Sie können auch die AWS Ressourcenflotte, die Ihre Anwendungen hostet, Ihre Daten speichert und Ihre Infrastruktur im Laufe der Zeit erweitert, skalieren und erweitern. AWS Da Ihre AWS Nutzung auf viele Ressourcentypen zunimmt, die sich über mehrere Anwendungen erstrecken, benötigen Sie einen Mechanismus, mit dem Sie nachverfolgen können, welche Ressourcen welcher Anwendung zugewiesen sind. Verwenden Sie diesen Mechanismus, um Ihre betrieblichen Aktivitäten wie Kostenüberwachung, Vorfallmanagement, Patching, Backup und Zugriffskontrolle zu unterstützen.

In lokalen Umgebungen wird dieses Wissen häufig in Wissensmanagementsystemen, Dokumentenverwaltungssystemen und auf internen Wiki-Seiten erfasst. Mit einer Configuration Management Database (CMDB) können Sie die relevanten detaillierten Metadaten mithilfe von Standardprozessen zur Änderungskontrolle speichern und verwalten. Dieser Ansatz bietet Kontrolle, erfordert jedoch zusätzlichen Entwicklungs- und Wartungsaufwand. Sie können bei der Benennung von Ressourcen einen strukturierten Ansatz wählen, aber ein Ressourcenname kann nur eine begrenzte Menge an Informationen enthalten.



Strukturierter Ansatz zur Benennung von Ressourcen

EC2-Instances verfügen beispielsweise über ein vordefiniertes Tag namens Name, das ähnliche Funktionen bietet und es Ihnen ermöglicht, Workloads so zu benennen, wie sie verschoben werden. AWS

2010 AWS führte ich Resource Tags ein, um einen flexiblen und skalierbaren Mechanismus zum Anhängen von Metadaten an Ihre Ressourcen bereitzustellen. Dieses Whitepaper führt Sie durch den Prozess der Entwicklung und Implementierung einer robusten Tagging-Strategie in Ihrer gesamten

Umgebung. AWS Diese Anleitung hilft Ihnen dabei, die Konsistenz und Reichweite der Tagging sicherzustellen, was Ihre Entscheidungsfindung und Ihre betrieblichen Aktivitäten unterstützt

Was sind Tags?

Ein Tag ist ein Schlüssel-Wert-Paar, das auf eine Ressource angewendet wird und Metadaten zu dieser Ressource enthält. Jedes Tag ist ein Label, das aus einem Schlüssel und einem optionalen Wert besteht. Derzeit unterstützen nicht alle Dienste und Ressourcentypen Tags (siehe Dienste, die die Resource Groups Tagging API unterstützen). Andere Dienste unterstützen möglicherweise Tags über ihre eigenen APIs. Es ist zu beachten, dass Tags nicht verschlüsselt sind und nicht zum Speichern sensibler Daten (PII) verwendet werden sollten (z. B. personenbezogene Informationen (PII)).

Tags, die ein Benutzer mithilfe derAWS CLI, API oder der erstellt und auf AWS Ressourcen anwendet, AWS Management Console werden als benutzerdefinierte Tags bezeichnet. Verschiedene AWS DiensteAWS CloudFormation, wie Elastic Beanstalk und Auto Scaling, weisen Ressourcen, die sie erstellen und verwalten, automatisch Tags zu. Diese Schlüssel werden als AWSgenerierte Tags bezeichnet und haben in der Regel ein Präfix. `aws` Dieses Präfix kann nicht in benutzerdefinierten Tag-Schlüsseln verwendet werden.

Es gibt Nutzungsanforderungen und Beschränkungen für die Anzahl der benutzerdefinierten Tags, die einer AWS Ressource hinzugefügt werden können. Weitere Informationen finden Sie unter Beschränkungen und Anforderungen für die Benennung von Tags im AWSAllgemeinen Referenzhandbuch. AWSgenerierte Tags werden nicht auf diese benutzerdefinierten Tag-Limits angerechnet.

Tabelle 1 — Beispiele für benutzerdefinierte Tag-Schlüssel und -Werte

Instance-ID	Tag-Schlüssel	Tag-Wert
`i-01234567abcdef89a`	`CostCenter`	`98765`
	`Stack`	`Test`
i-12345678abcdef90b	`CostCenter`	`98765`
	`Stack`	`Production`

Tabelle 2 — Beispiele für generierte Tags AWS

AWSGenerierte Tag-Schlüssel	Begründung
`aws:ec2spot:fleet-request-id`	Identifiziert die Amazon EC2 Spot-Instance-Anfrage, mit der die Instance gestartet wurde
`aws:cloudformation:stack-name`	Identifiziert den AWS CloudFormation Stack, der die Ressource erstellt hat
`lambda-console:blueprint`	Identifiziert den Blueprint, der als Vorlage für eine AWS Lambda Funktion verwendet wird
`elasticbeanstalk:environment-name`	Identifiziert die Anwendung, die die Ressource erstellt hat
`aws:servicecatalog: provisionedProductArn`	Das bereitgestellte Produkt Amazon-Sachname (ARN)
`aws:servicecatalog:productArn`	Der ARN des Produkts, von dem aus das bereitgestellte Produkt gestartet wurde

AWSgenerierte Tags bilden einen Namespace. In einer AWS CloudFormation Vorlage definieren Sie beispielsweise eine Gruppe von Ressourcen, die zusammen bereitgestellt werden sollen. Dabei `stack-name` handelt es sich um einen aussagekräftigen Namen`stack`, den Sie zu ihrer Identifizierung zuweisen. Wenn Sie einen Schlüssel wie untersuchen, können Sie feststellen*`aws:cloudformation:stack-name`*, dass der Namespace, der für den Gültigkeitsbereich des Parameters verwendet wird, drei Elemente verwendet: aws die Organisation, cloudformation der Dienst und stack-name der Parameter.

Benutzerdefinierte Tags können auch Namespaces verwenden, und es wird empfohlen, eine Organisations-ID als Präfix zu verwenden. Auf diese Weise können Sie schnell erkennen, ob es sich bei einem Tag um etwas aus Ihrem verwalteten Schema oder um etwas handelt, das durch einen Dienst oder ein Tool definiert ist, das Sie in Ihrer Umgebung verwenden.

Im AWSWhitepaper Establishing Your Cloud Foundation on empfehlen wir eine Reihe von Tags, die implementiert werden sollten. Es ist sehr wahrscheinlich, dass verschiedene Unternehmen unterschiedliche zulässige Muster und unterschiedliche Listen für ein bestimmtes Tag verwenden. Schauen wir uns das Beispiel in Tabelle 3 an:

Tabelle 3 — Derselbe Tag-Schlüssel, unterschiedliche Regeln für die Wertevalidierung

Organisation	Tag-Schlüssel	Validierung von Tag-Werten	Beispiel für einen Tag-Wert
Firma A	`CostCenter`	`5432, 5422, 5499`	`5432`
Firma B	`CostCenter`	`ABC*`	`ABC123`

Wenn sich diese beiden Schemas in unterschiedlichen Organisationen befinden, liegt kein Problem mit Tag-Konflikten vor. Sollten diese beiden Umgebungen jedoch zusammengeführt werden, kann es zu Konflikten zwischen den Namespaces kommen und die Validierung wird komplexer. Dieses Szenario mag unwahrscheinlich erscheinen, aber Unternehmen werden übernommen oder fusioniert, und es gibt andere Szenarien, wie z. B. Kunden, die mit einem Managed Service Provider, einem Spieleverlag oder einem Risikokapitalunternehmen zusammenarbeiten, bei dem Konten verschiedener Organisationen Teil einer gemeinsamen Organisation sind. AWS Durch die Verwendung des Firmennamens als Präfix zur Definition eines eindeutigen Namespaces können diese Probleme vermieden werden, wie in Tabelle 4 dargestellt:

Tabelle 4 — Verwendung von Namespaces in Tag-Schlüsseln

Organisation	Tag-Schlüssel	Validierung von Tag-Werten	Beispiel für einen Tag-Wert
Firma A	`company-a :CostCenter`	`5432, 5422, 5499`	`5432`
Firma B	`company-b :CostCenter`	`ABC*`	`ABC123`

In großen und komplexen Organisationen, in denen Unternehmen regelmäßig erworben und veräußert werden, wird diese Situation häufiger auftreten. Da die Prozesse und Praktiken der neuen Akquisition in der gesamten Gruppe harmonisiert sind, ist die Situation gelöst. Es ist hilfreich, klare Namespaces zu haben, da über die Verwendung der älteren Tags berichtet werden kann und die zuständigen Teams kontaktiert werden können, um das neue Schema zu übernehmen. Ein Namespace kann auch verwendet werden, um einen Geltungsbereich anzugeben oder einen

Anwendungsfall oder einen Verantwortungsbereich darzustellen, der auf die Eigentümer der Organisation zugeschnitten ist.

Tabelle 5 — Beispiel für einen Geltungsbereich oder einen Anwendungsfallbereich innerhalb von Tag-Schlüsseln

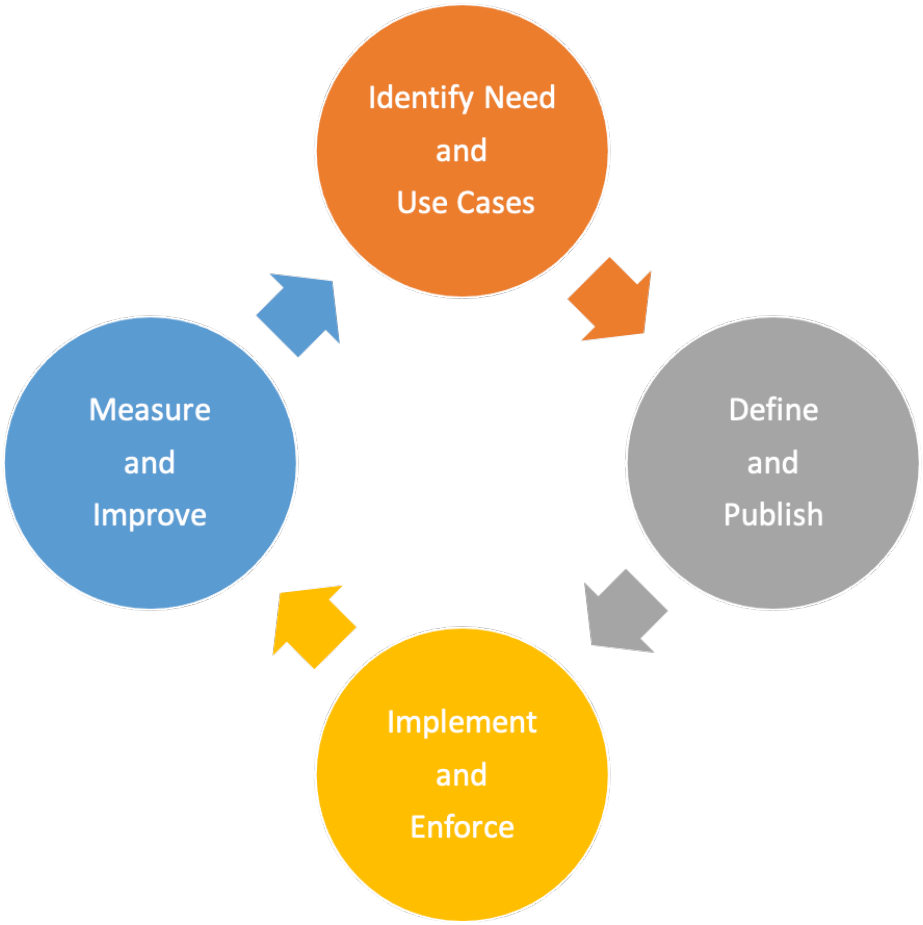
Anwendungsfall	Tag-Schlüssel	Begründung	Zulässige Werte
Klassifizierung von Daten	`example-inc:info-sec:data-classification`	Definierter Satz zur Datenklassifizierung im Bereich Informationssicherheit	`sensitive`, `company-confidential`, `customer-identifiable`
Operationen	`example-inc:dev-ops:environment`	Implementieren Sie die Planung von Test- und Entwicklungsumgebungen	`development`, `staging`, `quality-assurance`, `production`
Notfallwiederherstellung	`example-inc:disaster-recovery:rpo`	Definieren Sie das Recovery Point Objective (RPO) für eine Ressource	6h, 24h
Kostenzuweisung	`example-inc:cost-allocation:business-unit`	Finanzteams benötigen Kostenberichte über die Nutzung und die Ausgaben der einzelnen Teams	`corporate`, `recruitment`, `support`, `engineering`

Tags sind einfach und flexibel. Sowohl der Schlüssel als auch der Wert des Tags sind Zeichenketten variabler Länge und können einen breiten Zeichensatz unterstützen. Weitere Informationen zu Längen und Zeichensätzen finden Sie unter AWSRessourcen mit Tags versehen in der Allgemeinen Referenz. AWS Bei Tags wird zwischen Groß- und Kleinschreibung unterschieden, was bedeutet, dass `costcenter` es sich bei `costCenter` und um unterschiedliche Tagschlüssel handelt. In verschiedenen Ländern kann die Schreibweise eines Wortes unterschiedlich sein, was sich auf Ihre

Schlüssel auswirken kann. In den Vereinigten Staaten könnte man einen Schlüssel beispielsweise als definieren`costcenter`, aber im Vereinigten Königreich `costcentre` könnte dies bevorzugt werden. Aus Sicht der Ressourcen-Tagging handelt es sich dabei um unterschiedliche Schlüssel. Definieren Sie Rechtschreibung, Groß- und Kleinschreibung und Zeichensetzung als Teil Ihrer Tagging-Strategie. Verwenden Sie diese Definitionen als Referenz für alle, die Ressourcen erstellen oder verwalten. Dieses Thema wird im nächsten Abschnitt ausführlicher behandeltEntwickeln Sie Ihre Tagging-Strategie.

Entwickeln Sie Ihre Tagging-Strategie

Wie bei vielen betrieblichen Praktiken ist die Implementierung einer Tagging-Strategie ein Prozess der Iteration und Verbesserung. Fangen Sie klein mit Ihrer unmittelbaren Priorität an und erweitern Sie das Tagging-Schema nach Bedarf.



Iterations- und Verbesserungszyklus der Tagging-Strategie

Während dieses gesamten Prozesses ist Eigenverantwortung der Schlüssel zu Rechenschaftspflicht und Fortschritt. Da Tags für eine Vielzahl von Zwecken verwendet werden können, kann die gesamte Tagging-Strategie in Verantwortungsbereiche innerhalb einer Organisation aufgeteilt werden. Tagging ermöglicht einen programmatischen Ansatz für Aktivitäten, die von der Charakterisierung der Ressourcen abhängen. Die Anzahl der Interessengruppen, die von der Kennzeichnung profitieren können, hängt von der Größe der Organisation und den betrieblichen Praktiken ab. Größere Organisationen können von einer klaren Definition der Verantwortlichkeiten der Teams profitieren, die an der Entwicklung und Umsetzung einer Tagging-Strategie beteiligt sind. Einige Stakeholder können dafür verantwortlich sein, den Bedarf an Tagging zu ermitteln (Anwendungsfälle zu definieren);

andere wiederum können für die Pflege, Implementierung und Verbesserung der Tagging-Strategie verantwortlich sein.

Durch die Übertragung der Verantwortung sind Sie in einer guten Position, um einzelne Aspekte der Strategie umzusetzen. Gegebenenfalls kann diese Eigenverantwortung als Richtlinie formalisiert und in einer Verantwortungsmatrix (z. B. RACI: Responsible, Accountable, Consulted, Informed) oder in einem Modell der gemeinsamen Verantwortung dokumentiert werden. In kleineren Organisationen können Teams in einer Tagging-Strategie mehrere Rollen spielen, von der Definition der Anforderungen bis hin zur Implementierung und Durchsetzung.

Definition von Bedürfnissen und Anwendungsfällen

Beginnen Sie mit der Entwicklung Ihrer Strategie, indem Sie mit Stakeholdern zusammenarbeiten, die ein grundlegendes Bedürfnis haben, Metadaten zu nutzen. Diese Teams definieren die Metadaten, mit denen Ressourcen gekennzeichnet werden müssen, um ihre Aktivitäten wie Berichterstattung, Automatisierung und Datenklassifizierung zu unterstützen. Sie beschreiben, wie die Ressourcen organisiert werden müssen und welchen Richtlinien sie zugeordnet werden müssen. Zu den Rollen und Funktionen, die diese Interessengruppen in Organisationen haben können, gehören unter anderem:

- Finanzen und Geschäftsbereiche müssen den Wert von Investitionen verstehen, indem sie sie den Kosten zuordnen, um Maßnahmen zu priorisieren, die zur Behebung von Unzulänglichkeiten ergriffen werden müssen. Das Verständnis der Kosten im Vergleich zum generierten Wert hilft dabei, erfolglose Geschäftsbereiche oder Produktangebote zu identifizieren. Dies führt zu fundierten Entscheidungen über die Fortsetzung des Supports, die Einführung einer Alternative (z. B. die Nutzung eines SaaS-Angebots oder eines verwalteten Dienstes) oder die Einstellung eines unrentablen Geschäftsangebots.
- Unternehmensführung und Compliance müssen die Kategorisierung von Daten (z. B. öffentlich, sensibel oder vertraulich) verstehen, wissen, ob ein bestimmter Workload anhand eines bestimmten Standards oder einer bestimmten Vorschrift geprüft werden kann oder nicht, und die Wichtigkeit des Dienstes (unabhängig davon, ob der Service oder die Anwendung geschäftskritisch ist), um angemessene Kontrollen und Kontrollen wie Genehmigungen, Richtlinien und Überwachung anwenden zu können.
- Betrieb und Entwicklung müssen den Workload-Lebenszyklus, die Implementierungsphasen ihrer unterstützten Produkte und das Management der Release-Phasen (z. B. Entwicklung, Test, Produktionsaufteilung) sowie die damit verbundenen Support-Priorisierungen und die

Anforderungen an das Stakeholder-Management verstehen. Aufgaben wie Backups, Patches, Observability und Deprecation müssen ebenfalls definiert und verstanden werden.

- Informationssicherheit (InfoSec) und Sicherheitsoperationen (SecOps) beschreiben, welche Kontrollen angewendet werden müssen und welche empfohlen werden. InfoSec definiert normalerweise die Implementierung der Kontrollen und SecOps ist im Allgemeinen für die Verwaltung dieser Kontrollen verantwortlich.

Abhängig von Ihrem Anwendungsfall, Ihren Prioritäten, der Größe Ihres Unternehmens und den betrieblichen Abläufen benötigen Sie möglicherweise Unterstützung durch verschiedene Teams innerhalb der Organisation, z. B. in den Bereichen Finanzen (einschließlich Beschaffung), Informationssicherheit, Cloud-Aktivierung und Cloud-Betrieb. Für Funktionen wie Patchen, Sicherung und Wiederherstellung, Überwachung, Jobplanung und Disaster Recovery benötigen Sie außerdem die Unterstützung der Anwendungs- und Prozessverantwortlichen. Diese Mitarbeiter unterstützen Sie bei der Definition und Implementierung der Tagging-Strategie und messen deren Wirksamkeit. Sie sollten ausgehend von den Interessengruppen und ihren Anwendungsfällen einen funktionsübergreifenden Workshop durchführen. In dem Workshop haben sie die Möglichkeit, ihre Sichtweisen und Bedürfnisse auszutauschen und zur Entwicklung einer Gesamtstrategie beizutragen. Beispiele von Teilnehmern und ihre Beteiligung an verschiedenen Anwendungsfällen werden später in diesem Whitepaper beschrieben.

Die Beteiligten definieren und validieren auch die Schlüssel für obligatorische Tags und können den Geltungsbereich für optionale Tags empfehlen. Beispielsweise müssen Finanzteams eine Ressource möglicherweise einer internen Kostenstelle, einer Geschäftseinheit oder beidem zuordnen. Daher können sie verlangen, dass bestimmte Tag-Schlüssel, wie z. B. `CostCenter` und`BusinessUnit`, verpflichtend sind. Einzelne Entwicklungsteams könnten beschließen, zusätzliche Tags für Automatisierungszwecke zu verwenden, z. B. `EnvironmentName`, `OptIn`, oder`OptOut`.

Die wichtigsten Interessengruppen müssen sich auf den Ansatz der Tagging-Strategie einigen und die Antworten auf Fragen im Zusammenhang mit Compliance und Unternehmensführung dokumentieren, wie z. B.:

- Welche Anwendungsfälle müssen angegangen werden?
- Wer ist für die Kennzeichnung von Ressourcen verantwortlich (Implementierung)?
- Wie werden Tags durchgesetzt und welche Methoden und Automatisierungen werden eingesetzt (proaktiv oder reaktiv)?
- Wie werden die Effektivität und die Ziele von Tagging gemessen?

- Wie oft sollte die Tagging-Strategie überprüft werden?
- Wer treibt Verbesserungen voran? Wie wird das gemacht?

Geschäftsfunktionen wie Cloud Enablement, Cloud Business Office und Cloud Platform Engineering können dann eine Rolle als Vermittler bei der Entwicklung der Tagging-Strategie übernehmen, deren Einführung vorantreiben und die Konsistenz der Anwendung sicherstellen, indem sie den Fortschritt messen, Hindernisse beseitigen und Doppelarbeit reduzieren.

Definition und Veröffentlichung eines Tagging-Schemas

Verwenden Sie beim Taggen Ihrer AWS Ressourcen einen konsistenten Ansatz, sowohl für obligatorische als auch für optionale Tags. Ein umfassendes Tagging-Schema hilft Ihnen dabei, diese Konsistenz zu erreichen. Die folgenden Beispiele können Ihnen den Einstieg erleichtern:

- Vereinbaren Sie die obligatorischen Tag-Schlüssel
- Definieren Sie akzeptable Werte und Benennungskonventionen für Tags (Groß- oder Kleinschreibung, Bindestriche oder Unterstriche, Hierarchie usw.)
- Bestätigen Sie, dass es sich bei den Werten nicht um persönlich identifizierbare Informationen (PII) handelt.
- Entscheiden Sie, wer neue Tag-Schlüssel definieren und erstellen kann
- Vereinbaren Sie, wie Sie neue obligatorische Tag-Werte hinzufügen und wie optionale Tags verwaltet werden

Sehen Sie sich die folgende Tabelle mit den Tag-Kategorien an, die als Grundlage dafür dienen kann, was Sie in Ihr Tagging-Schema aufnehmen könnten. Sie müssen noch festlegen, welche Konvention Sie für den Tag-Schlüssel verwenden werden und welche Werte jeweils zulässig sind. Das Tagging-Schema ist das Dokument, in dem Sie dies für Ihre Umgebung definieren.

Tabelle 6 — Beispiel für ein definitives Tagging-Schema (Teil 1)

Anwendungsfall	Tag-Schlüssel	Begründung	Zulässige Werte (Aufgeführt oder Wertepräfix/ Sujecx)	Wird für die Kostenzuweisung verwendet	Ressourcentypen	Scope	Erforderlich
Kostenverteilung	`example-inc:cost-allocation: ApplicationId`	Verfolgen Sie die Kosten im Vergleich zum in den einzelnen Geschäftsbereichen generierten Wert	`DataLakeX` , `RetailSiteX`	Y	Alle	Alle	zwingend erforderlich
Kostenverteilung	`example-inc:cost-allocation: BusinessUnitId`	Überwachen Sie die Kosten nach Geschäftsbereichen	`Architecture` , `DevOps`, `Finance`	Y	Alle	Alle	zwingend erforderlich
Kostenverteilung	`example-inc:cost-allocation:CostCenter`	Überwachen Sie die Kosten nach Kostenstellen	`123-*`	Y	Alle	Alle	zwingend erforderlich
Kostenverteilung	`example-inc:cost-allocation:Owner`	Welcher Haushaltsinhaber ist für diesen Arbeitsaufwand	`Marketing` , `RetailSupport`	Y	Alle	Alle	zwingend erforderlich

Tabelle 6 — Beispiel für ein definitives Tagging-Schema (Teil 2)

Anwendungsfall	Tag-Schlüssel	Begründung	Zulässige Werte (Aufgeführt oder Wertepräfix/ Sujecx)	Wird für die Kostenzuweisung verwendet	Ressourcentypen	Scope	Erforderlich
DevOps	`example-inc:operations: Owner`	Welches Team/ welcher Kader ist für die Erstellung und Wartung der Ressource verantwortlich	`Squad01`	N	Alle	Alle	zwingend erforderlich
Notfallwiederherstellung	`example-inc:disaster-recovery:rpo`	Definieren Sie das Recovery Point Objective (RPO) für eine Ressource	`6h`, `24h`	N	S3, EBS	Prod	zwingend erforderlich
Datenklassifizierung	`example-inc:data: classification`	Klassifizieren Sie Daten aus Gründen der Einhaltung von Vorschriften und Unternehmensführung	`Public`, `Private`, `Confidential` , `Restricted`	N	S3, EBS	Alle	zwingend erforderlich
- Compliance	`example-inc:compliance: framework`	Identifiziert das Compliance-Framework, dem die	`PCI-DSS`, `HIPAA`	N	Alle	Prod	zwingend erforderlich

Nachdem das Tagging-Schema definiert wurde, verwalten Sie das Schema in einem versionskontrollierten Repository, auf das alle relevanten Beteiligten zugreifen können, sodass sie leicht nachschlagen und Aktualisierungen nachverfolgen können. Dieser Ansatz verbessert die Effizienz und ermöglicht Agilität.

AWS Organizations— Tag-Richtlinien

AWS OrganizationsMit den Richtlinien können Sie zusätzliche Arten der Unternehmensführung anwenden. AWS-Konten Mithilfe einer Tag-Richtlinie können Sie Ihr Tagging-Schema in JSON-Form ausdrücken, sodass die Plattform das Schema in Ihrer AWS Umgebung melden und optional durchsetzen kann. Die Tag-Richtlinie definiert die Werte, die für einen Tag-Schlüssel bei bestimmten Ressourcentypen zulässig sind. Diese Richtlinie kann in Form einer Werteliste oder eines Präfixes, gefolgt von einem Platzhalterzeichen (*), vorliegen. Der einfache Präfix-Ansatz ist weniger streng als eine diskrete Werteliste, erfordert jedoch weniger Wartung.

Die folgenden Beispiele zeigen, wie eine Tagging-Richtlinie definiert wird, um die Werte zu überprüfen, die für einen bestimmten Schlüssel akzeptabel sind. Ausgehend von der benutzerfreundlichen tabellarischen Definition des Schemas können Sie diese Informationen in eine oder mehrere Tag-Richtlinien umwandeln. Separate Richtlinien können verwendet werden, um delegiertes Eigentum zu unterstützen, oder einige Richtlinien gelten möglicherweise nur in bestimmten Szenarien.

ExampleInc- .json CostAllocation

Im Folgenden finden Sie ein Beispiel für eine Tag-Richtlinie, die über Tags zur Kostenzuweisung berichtet:

```
{
  "tags": {
    "example-inc:cost-allocation:ApplicationId": {
      "tag_key": {
        "@@assign": "example-inc:cost-allocation:ApplicationId"
      },
      "tag_value": {
        "@@assign": [
          "DataLakeX",
          "RetailSiteX"
        ]
      }
```

```
    },
    "example-inc:cost-allocation:BusinessUnitId": {
      "tag_key": {
        "@@assign": "example-inc:cost-allocation:BusinessUnitId"
      },
      "tag_value": {
        "@@assign": [
          "Architecture",
          "DevOps",
          "FinanceDataLakeX"
        ]
      }
    },
    "example-inc:cost-allocation:CostCenter": {
      "tag_key": {
        "@@assign": "example-inc:cost-allocation:CostCenter"
      },
      "tag_value": {
        "@@assign": [
          "123-*"
        ]
      }
    }
  }
}
```

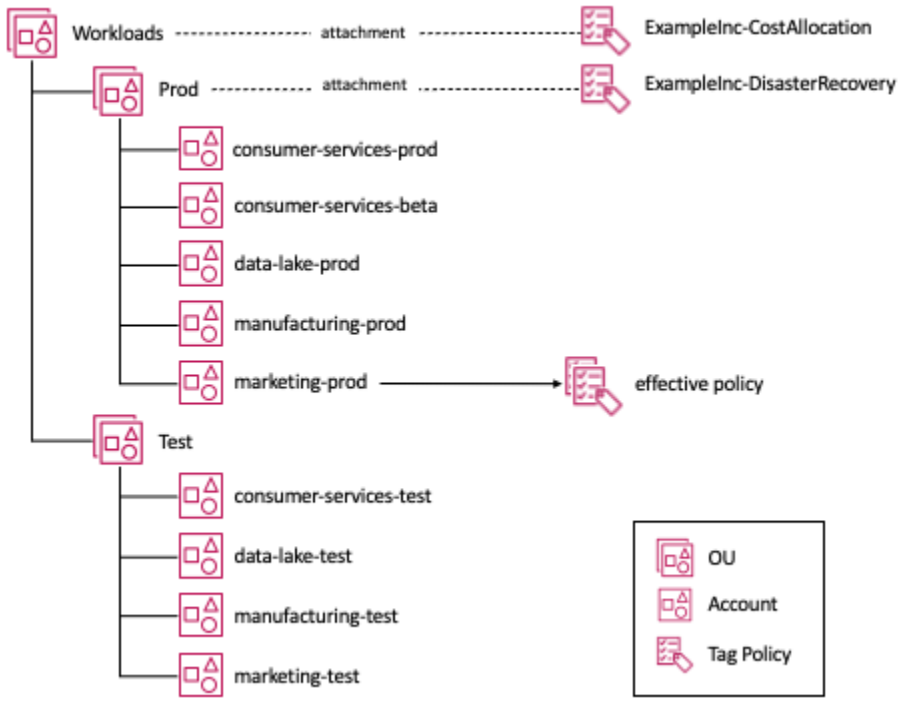
ExampleInc- DisasterRecovery .json

Im Folgenden finden Sie ein Beispiel für eine Tag-Richtlinie, die über Disaster Recovery-Tags berichtet:

```
{
    "tags": {
        "example-inc:disaster-recovery:rpo": {
            "tag_key": {
                "@@assign": "example-inc:disaster-recovery:rpo"
            },
            "tag_value": {
                "@@assign": [
                    "6h",
                    "24h"
                ]
            }
```

```
        }
    }
}
```

In diesem Beispiel ist die `ExampleInc-CostAllocation` Tag-Richtlinie an die `Workloads` Organisationseinheit angehängt und gilt daher für alle Konten sowohl in der Organisationseinheit als auch in den `Prod` `Test` untergeordneten Organisationseinheiten. In ähnlicher Weise ist die `ExampleInc-DisasterRecovery` Tag-Richtlinie an die `Prod` Organisationseinheit angehängt und gilt daher nur für Konten unter dieser Organisationseinheit. Das Whitepaper Organizing Your Environment Using Multiple Accounts befasst sich eingehender mit den empfohlenen OU-Strukturen.



Zuordnung von Tag-Richtlinien zu einer OU-Struktur

Betrachtet man das `marketing-prod` Konto im Diagramm, so gelten beide Tag-Richtlinien für dieses Konto. Wir haben also das Konzept einer effektiven Richtlinie, d. h. die Zusammenfassung der Richtlinien eines bestimmten Typs, die für ein Konto gelten. Wenn Sie Ihre Ressourcen hauptsächlich manuell verwalten, können Sie die geltende Richtlinie überprüfen, indem Sie in der Konsole den Resource Groups- und Tag-Editor: Tag-Richtlinien aufrufen. Wenn Sie Infrastructure as Code (IaC) oder Scripting zur Verwaltung Ihrer Ressourcen verwenden, können Sie den API-Aufruf verwenden. `AWS::Organizations::DescribeEffectivePolicy`

Implementierung und Durchsetzung von Tagging

In diesem Abschnitt stellen wir Ihnen die Tools vor, die für die folgenden Ressourcenmanagement-Strategien verfügbar sind: manuell, Infrastructure as Code (IaC) und Continuous Integration/Continuous Delivery (CI/CD). Die Schlüsseldimension dieser Ansätze ist eine immer häufigere Implementierungsrate.

Manuell verwaltete Ressourcen

Dabei handelt es sich in der Regel um Workloads, die in die Grundlagen- oder Migrationsphase der Einführung fallen. Oft handelt es sich dabei um einfache, weitgehend statische Workloads, die mithilfe herkömmlicher schriftlicher Verfahren erstellt wurden, oder um Workloads, die nach Bedarf mithilfe von Tools migriert wurden, z. B. CloudEndure aus einer lokalen Umgebung. Migrationstools wie Migration Hub und CloudEndure können im Rahmen des Migrationsprozesses Tags anwenden. Wenn jedoch bei der ursprünglichen Migration keine Tags angewendet wurden oder sich das Tagging-Schema seitdem geändert hat, können Sie mit dem Tag-Editor (eine Funktion vonAWS Management Console) anhand einer Vielzahl von Suchkriterien nach Ressourcen suchen und Tags gleichzeitig hinzufügen, ändern oder löschen. Zu den Suchkriterien können Ressourcen mit oder ohne das Vorhandensein eines bestimmten Tags oder Werts gehören. Mit der AWS Resource Tagging API können Sie diese Funktionen programmgesteuert ausführen.

Im Zuge der Modernisierung dieser Workloads werden Ressourcentypen wie Auto Scaling Scaling-Gruppen eingeführt. Diese Ressourcentypen ermöglichen eine höhere Elastizität und eine verbesserte Widerstandsfähigkeit. Die Auto Scaling-Gruppe verwaltet Amazon EC2 EC2-Instances in Ihrem Namen. Möglicherweise möchten Sie jedoch trotzdem, dass die EC2-Instances konsistent mit den manuell erstellten Ressourcen gekennzeichnet werden. Eine Amazon EC2 EC2-Startvorlage bietet die Möglichkeit, die Tags anzugeben, die Auto Scaling auf die von ihm erstellten Instances anwenden soll.

Wenn die Ressourcen eines Workloads manuell verwaltet werden, kann es hilfreich sein, das Tagging von Ressourcen zu automatisieren. Es stehen verschiedene Lösungen zur Verfügung. Ein Ansatz ist die VerwendungAWS-Config-Regeln, mit der nach einer Lambda-Funktion gesucht `required_tags` und diese dann gestartet werden kann, um sie anzuwenden. AWS-Config-Regelnwird später in diesem Whitepaper genauer beschrieben.

Verwaltete Ressourcen mit Infrastruktur als Code (IaC)

AWS CloudFormationbietet eine gemeinsame Sprache für die Bereitstellung aller Infrastrukturressourcen in Ihrer AWS Umgebung. CloudFormation Vorlagen sind JSON- oder YAML-

Dateien, mit denen AWS Ressourcen automatisiert erstellt werden. Wenn Sie AWS Ressourcen mithilfe von CloudFormation Vorlagen erstellen, können Sie die Eigenschaft CloudFormation Resource Tags verwenden, um bei der Erstellung Tags auf unterstützte Ressourcentypen anzuwenden. Die Verwaltung der Tags sowie der Ressourcen mit IaC trägt zur Sicherstellung der Konsistenz bei.

Wenn Ressourcen von erstellt werdenAWS CloudFormation, wendet der Service automatisch eine Reihe AWS definierter Tags auf die mit der AWS CloudFormation Vorlage erstellten Ressourcen an. Dies sind:

```
aws:cloudformation:stack-name
aws:cloudformation:stack-id
aws:cloudformation:logical-id
```

Sie können auf einfache Weise eine Ressourcengruppe auf der Grundlage des AWS CloudFormation Stacks definieren. Diese AWS definierten Tags werden von den Ressourcen vererbt, die vom Stack erstellt wurden. Für Amazon EC2 EC2-Instances innerhalb einer Auto Scaling Scaling-Gruppe `AWS::AutoScaling::AutoScalingGroup TagProperty`muss dies jedoch in der Definition der Auto Scaling Scaling-Gruppe in Ihrer AWS CloudFormation Vorlage festgelegt werden. Wenn Sie eine EC2-Startvorlage mit der Auto Scaling Scaling-Gruppe verwenden, können Sie die Tags alternativ in ihrer Definition definieren. Es wird empfohlen, EC2 Launch Templates mit Auto Scaling Scaling-Gruppen oder mit einem AWS Container-Service zu verwenden. Diese Services können dazu beitragen, dass Ihre Amazon EC2 EC2-Instances konsistent gekennzeichnet werden. Außerdem unterstützen sie Auto Scaling für mehrere Instance-Typen und Kaufoptionen, wodurch die Ausfallsicherheit verbessert und Ihre Rechenkosten optimiert werden können.

AWS CloudFormationHooks bieten Entwicklern die Möglichkeit, wichtige Aspekte ihrer Anwendung mit den Standards ihrer Organisation in Einklang zu bringen. Hooks können so konfiguriert werden, dass sie eine Warnung ausgeben oder die Bereitstellung verhindern. Diese Funktion eignet sich am besten, um wichtige Konfigurationselemente in Ihren Vorlagen zu überprüfen, z. B. ob eine Auto Scaling Scaling-Gruppe so konfiguriert ist, dass sie kundenspezifische Tags auf alle Amazon EC2 EC2-Instances anwendet, die sie startet, oder um sicherzustellen, dass alle Amazon S3 S3-Buckets mit den erforderlichen Verschlüsselungseinstellungen erstellt werden. In beiden Fällen wird die Bewertung dieser Konformität auf die frühere Phase des Implementierungsprozesses verschoben, wobei vor der Bereitstellung ein AWS CloudFormation Haken gesetzt wird.

AWS CloudFormationbietet die Möglichkeit zu erkennen, wenn eine über eine Vorlage bereitgestellte Ressource (siehe Ressourcen, die Drift-Erkennung unterstützen) geändert wurde und Ressourcen

nicht mehr ihren erwarteten Vorlagenkonfigurationen entsprechen. Dies wird als Drift bezeichnet. Wenn Sie mithilfe von Automatisierung Tags auf Ressourcen anwenden, die über IaC verwaltet werden, ändern Sie sie und führen zu Drift. Bei der Verwendung von IaC wird derzeit empfohlen, alle Tagging-Anforderungen als Teil der IaC-Vorlagen zu verwalten, AWS CloudFormation Hooks zu implementieren und AWS CloudFormation Guard-Regelsätze zu veröffentlichen, die für die Automatisierung verwendet werden können.

Mit CI/CD-Pipeline verwaltete Ressourcen

Je ausgereifter ein Workload wird, desto wahrscheinlicher ist es, dass Techniken wie Continuous Integration und Continuous Deployment (CI/CD) eingeführt werden. Diese Techniken tragen dazu bei, das Implementierungsrisiko zu verringern, indem sie es einfacher machen, kleine Änderungen häufiger zu implementieren und die Tests stärker zu automatisieren. Eine Beobachtungsstrategie, die unerwartetes, durch eine Bereitstellung verursachtes Verhalten erkennt, kann die Bereitstellung automatisch und mit minimaler Auswirkung auf die Benutzer rückgängig machen. In der Phase, in der Sie täglich zehnmal am Tag bereitstellen müssen, ist die rückwirkende Anwendung von Tags einfach nicht mehr praktikabel. Alles muss als Code oder Konfiguration ausgedrückt, versionskontrolliert und, wo immer möglich, getestet und bewertet werden, bevor es in der Produktion eingesetzt wird. Beim kombinierten Modell für Entwicklung und Betrieb (DevOps) behandeln viele der Methoden betriebliche Überlegungen in Form von Code und validieren sie zu Beginn des Bereitstellungszyklus.

Idealerweise sollten Sie diese Prüfungen so früh wie möglich durchführen (wie mit AWS CloudFormation Hooks dargestellt), sodass Sie sicher sein können, dass Ihre AWS CloudFormation Vorlage Ihren Richtlinien entspricht, bevor sie den Computer des Entwicklers verlassen.

AWS CloudFormationGuard 2.0 bietet die Möglichkeit, präventive Compliance-Regeln für alles, was Sie definieren können, zu CloudFormation schreiben. Die Vorlage wird anhand der Regeln in der Entwicklungsumgebung validiert. Natürlich hat diese Funktion eine Reihe von Anwendungen, aber in diesem Whitepaper werden wir uns nur einige Beispiele ansehen, um sicherzustellen, dass sie immer verwendet wird. `AWS::AutoScaling::AutoScalingGroup TagProperty`

Im Folgenden finden Sie ein Beispiel für eine CloudFormation Guard-Regel:

```
let all_asgs = Resources.*[ Type == 'AWS::AutoScaling::AutoScalingGroup' ]

rule tags_asg_automation_EnvironmentId when %all_asgs !empty {
    let required_tags = %all_asgs.Properties.Tags.*[
        Key == 'example-inc:automation:EnvironmentId' ]
    %required_tags[*] {
```

```
        PropagateAtLaunch == 'true'
        Value IN ['Prod', 'Dev', 'Test', 'Sandbox']
        <<Tag must have a permitted value
          Tag must have PropagateAtLaunch set to 'true'>>
    }
}

rule tags_asg_costAllocation_CostCenter when %all_asgs !empty {
    let required_tags = %all_asgs.Properties.Tags.*[
        Key == 'example-inc:cost-allocation:CostCenter' ]
    %required_tags[*] {
        PropagateAtLaunch == 'true'
        Value == /^123-/
        <<Tag must have a permitted value
          Tag must have PropagateAtLaunch set to 'true'>>
    }
}
```

Im Codebeispiel filtern wir die Vorlage nach allen Ressourcen dieses Typs `AutoScalingGroup` und haben dann zwei Regeln:

- **`tags_asg_automation_EnvironmentId`**- Überprüft, ob ein Tag mit diesem Schlüssel existiert, dass es einen Wert in der Liste der zulässigen Werte gibt und dass dieser Wert auf gesetzt `PropagateAtLaunch` ist `true`
- **`tags_asg_costAllocation_CostCenter`**- Überprüft, ob ein Tag mit diesem Schlüssel existiert, dass es einen Wert hat, der mit dem definierten Präfixwert beginnt und auf gesetzt `PropagateAtLaunch` ist `true`

Durchsetzung

Wie bereits beschrieben, bietet Resource Groups & Tag Editor die Möglichkeit, festzustellen, wo Ihre Ressourcen die Tagging-Anforderungen nicht erfüllen, die in den Tag-Richtlinien für die Organisationseinheiten der Organisation definiert sind. Wenn Sie von einem Mitgliedskonto einer Organisation aus auf das Konsolentool Resource Groups & Tag Editor zugreifen, werden Ihnen die Richtlinien angezeigt, die für dieses Konto gelten, und die Ressourcen innerhalb des Kontos, die die Anforderungen der Tag-Richtlinie nicht erfüllen. Wenn der Zugriff über das Verwaltungskonto erfolgt (und wenn für Tag-Richtlinien der Zugriff in den Diensten unter aktiviert istAWS Organizations), ist es möglich, die Einhaltung der Tag-Richtlinien für alle verknüpften Konten in der Organisation einzusehen.

In der Tag-Richtlinie selbst können Sie die Durchsetzung für bestimmte Ressourcentypen aktivieren. Im folgenden Richtlinienbeispiel haben wir die Durchsetzung hinzugefügt, sodass alle Ressourcen der `ec2:volume` Typen `ec2:instance` und der Richtlinie entsprechen müssen. Es gibt einige bekannte Einschränkungen, z. B. muss eine Ressource mit einem Tag versehen sein, damit sie anhand der Tag-Richtlinie ausgewertet werden kann. Eine Liste finden Sie unter Ressourcen, die die Durchsetzung von Tag-Richtlinien unterstützen.

ExampleInc-cost-allocation.json

Im Folgenden finden Sie ein Beispiel für eine Tag-Richtlinie, mit der Kostenzuweisungs-Tags gemeldet und/oder durchgesetzt werden:

```
{
  "tags": {
    "example-inc:cost-allocation:ApplicationId": {
      "tag_key": {
        "@@assign": "example-inc:cost-allocation:ApplicationId"
      },
      "tag_value": {
        "@@assign": [
          "DataLakeX",
          "RetailSiteX"
        ]
      },
      "enforced_for": {
        "@@assign": [
          "ec2:instance",
          "ec2:volume"
        ]
      }
    },
    "example-inc:cost-allocation:BusinessUnitId": {
      "tag_key": {
        "@@assign": "example-inc:cost-allocation:BusinessUnitId"
      },
      "tag_value": {
        "@@assign": [
          "Architecture",
          "DevOps",
          "FinanceDataLakeX"
        ]
      },
```

```
      "enforced_for": {
        "@@assign": [
          "ec2:instance",
          "ec2:volume"
        ]
      }
    },
    "example-inc:cost-allocation:CostCenter": {
      "tag_key": {
        "@@assign": "example-inc:cost-allocation:CostCenter"
      },
      "tag_value": {
        "@@assign": [
          "123-*"
        ]
      },
      "enforced_for": {
        "@@assign": [
          "ec2:instance",
          "ec2:volume"
        ]
      }
    }
  }
}
```

AWS Config (**`required_tag`**)

AWS Configist ein Service, mit können Sie die Konfigurationen Ihrer AWS -Ressourcen bewerten, prüfen und AWS Config beurteilen. Im Fall von Tagging können wir damit mithilfe der `required_tags` Regel Ressourcen identifizieren, denen Tags mit bestimmten Schlüsseln fehlen (siehe Ressourcentypen, die von required_tags unterstützt werden). Ausgehend vom vorherigen Beispiel könnten wir testen, ob der Schlüssel auf allen Amazon EC2 EC2-Instances vorhanden ist. In Fällen, in denen der Schlüssel nicht existiert, wird die Instance als nicht konform registriert. Diese AWS CloudFormation Vorlage beschreibt eine AWS Config Regel, mit der das Vorhandensein der in der Tabelle beschriebenen obligatorischen Schlüssel auf Amazon S3-Buckets, Amazon EC2 EC2-Instances und Amazon EBS-Volumes getestet werden soll.

```
Resources:
 MandatoryTags:
   Type: AWS::Config::ConfigRule
   Properties:
```

```
      ConfigRuleName: ExampleIncMandatoryTags
      Description: These tags should be in place
      InputParameters:
        tag1Key: example-inc:cost-allocation:ApplicationId
        tag2Key: example-inc:cost-allocation:BusinessUnitId
        tag3Key: example-inc:cost-allocation:CostCenter
        tag4Key: example-inc:automation:EnvironmentId
      Scope:
        ComplianceResourceTypes:
        - "AWS::S3::Bucket"
        - "AWS::EC2::Instance"
        - "AWS::EC2::Volume"
      Source:
        Owner: AWS
        SourceIdentifier: REQUIRED_TAGS
```

In Umgebungen, in denen Ressourcen manuell verwaltet werden, kann eine AWS Config Regel dahingehend erweitert werden, dass der fehlende Tag-Schlüssel mithilfe einer automatischen Problembehebung über eine Funktion automatisch zu den Ressourcen hinzugefügt wird. AWS Lambda Das funktioniert zwar gut für statische Workloads, ist aber zunehmend weniger effektiv, wenn Sie beginnen, Ihre Ressourcen über IaC und Deployment-Pipelines zu verwalten.

AWS Organizations— Service Control Policies (SCPs) sind eine Art von Unternehmensrichtlinie, mit können Sie die Berechtigungen in Ihrer Organisation verwalten. SCPs bieten eine zentrale Kontrolle über die maximal verfügbaren Berechtigungen für alle Konten in Ihrer Organisation oder Organisationseinheit (OU). SCPs wirken sich nur auf Benutzer und Rollen aus, die von Konten verwaltet werden, die Teil der Organisation sind. Sie wirken sich zwar nicht direkt auf Ressourcen aus, schränken jedoch die Berechtigungen von Benutzern und Rollen ein, was auch die Berechtigungen für Tagging-Aktionen einschließt. In Bezug auf das Tagging können SCPs zusätzlich zu den Möglichkeiten, die Tag-Richtlinien bieten, zusätzliche Granularität bei der Durchsetzung von Tags bieten.

Im folgenden Beispiel lehnt die Richtlinie `ec2:RunInstances` Anfragen ab, bei denen das `example-inc:cost-allocation:CostCenter` Tag nicht vorhanden ist.

Das Folgende ist ein Deny-SCP:

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

```
      "Sid": "DenyRunInstanceWithNoCostCenterTag",
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:*:*:instance/"
      ],
      "Condition": {
        "Null": {
          "aws:RequestTag/example-inc:cost-allocation:CostCenter": "true"
        }
      }
    }
  ]
}
```

Es ist nicht möglich, die effektive Dienststeuerungsrichtlinie abzurufen, die standardmäßig für ein verknüpftes Konto gilt. Wenn Sie die Kennzeichnung mit SCPs erzwingen, muss den Entwicklern die Dokumentation zur Verfügung stehen, damit sie sicherstellen können, dass ihre Ressourcen den Richtlinien entsprechen, die für ihre Konten gelten. Wenn Sie nur Lesezugriff auf CloudTrail Ereignisse in ihrem Konto gewähren, können Entwickler bei der Aufgabe des Debuggings unterstützt werden, wenn ihre Ressourcen nicht den Anforderungen entsprechen.

Messung der Effektivität von Tagging und Förderung von Verbesserungen

Nachdem Sie eine Tagging-Strategie implementiert haben, ist es wichtig, ihre Wirksamkeit anhand der Zielanwendungsfälle zu messen. Das Maß der Effektivität wird je nach Anwendungsfall variieren. Beispiele:

- Kostenzuweisung — Mithilfe von Tools wie dem Kosten- und Nutzungsbericht könnten Sie den Umfang der Tagging von Ressourcen anhand der Ausgaben messen. AWS Cost ExplorerAWS Sie könnten beispielsweise den Prozentsatz der Ressourcen mit oder ohne Tags verfolgen, für die Gebühren anfallen, insbesondere durch die Überwachung bestimmter Tag-Schlüssel.
- Automatisierung — Möglicherweise möchten Sie überprüfen, ob das gewünschte Ergebnis erzielt wurde. Zum Beispiel, ob Amazon EC2 EC2-Instances außerhalb der Geschäftszeiten angehalten werden, ob die Start- und Stoppzeiten von Instances geprüft werden.

Der Resource Groups & Tag Editor innerhalb des Verwaltungskontos bietet zusätzliche Funktionen zur Analyse der Einhaltung der Tag-Richtlinien für alle verknüpften Konten in Ihrer Organisation.

Ermitteln Sie anhand der Ergebnisse der Messung Ihrer Tagging-Effektivität, ob bei einem der Schritte, z. B. bei der Definition eines Anwendungsfalls, der Implementierung oder Durchsetzung des Tagging-Schemas, Verbesserungen oder Änderungen erforderlich sind. Nehmen Sie die erforderlichen Änderungen vor und wiederholen Sie den Zyklus, bis die gewünschte Effektivität erreicht ist. Im Beispiel mit der Kostenzuweisung können Sie sich die prozentuale Verbesserung ansehen.

Da es die Entwickler und Betreiber sind, die das eigentliche Tagging von Ressourcen durchführen müssen, ist es wichtig, dass sie die Verantwortung dafür übernehmen. Dies ist nicht die einzige zusätzliche Verantwortung, die Teams normalerweise auf ihrem Weg AWS zur Einführung übernehmen. Eine größere Verantwortung für die Sicherheit und die Kosten für die Entwicklung und den Betrieb ihrer Anwendung sind ebenfalls wichtig. Organizations verwenden häufig Ziele und Vorgaben, um die Einführung neuer Praktiken zu motivieren, sodass dies auch hier zutreffen kann.

Anwendungsfälle taggen

Themen

Tags für die Kostenzuweisung und das Finanzmanagement

Einer der ersten Anwendungsfälle, mit denen sich Unternehmen häufig befassen, ist die Transparenz und Verwaltung von Kosten und Nutzung. In der Regel gibt es dafür mehrere Gründe:

- In der Regel handelt es sich um ein gut verstandenes Szenario, und die Anforderungen sind allgemein bekannt. Finanzteams möchten beispielsweise die Gesamtkosten von Workloads und Infrastruktur sehen, die sich über mehrere Dienste, Funktionen, Konten oder Teams erstrecken. Eine Möglichkeit, diese Kostentransparenz zu erreichen, ist die konsistente Kennzeichnung von Ressourcen.
- Tags und ihre Werte sind klar definiert. In der Regel gibt es in den Finanzsystemen einer Organisation bereits Mechanismen zur Kostenverteilung, z. B. die Erfassung nach Kostenstelle, Geschäftseinheit, Team oder Organisationsfunktion.
- Schnelle, nachweisbare Kapitalrendite. Es ist möglich, Trends zur Kostenoptimierung im Laufe der Zeit zu verfolgen, wenn Ressourcen einheitlich gekennzeichnet werden, z. B. für Ressourcen, die richtig dimensioniert, automatisch skaliert oder in einen Zeitplan aufgenommen wurden.

Wenn Sie wissen, wie Ihnen Kosten entstehen, AWS können Sie fundierte finanzielle Entscheidungen treffen. Wenn Sie wissen, wo Ihnen Kosten auf Ressourcen-, Arbeitslast-, Team- oder Organisationsebene entstanden sind, können Sie besser verstehen, welchen Nutzen Sie auf der jeweiligen Ebene im Vergleich zu den erzielten Geschäftsergebnissen erzielt haben.

Die Entwicklungsteams haben möglicherweise keine Erfahrung mit dem Finanzmanagement ihrer Ressourcen. Die Einstellung einer Person mit Spezialkenntnissen im AWS Finanzmanagement, die Ingenieur- und Entwicklungsteams in den Grundlagen des AWS Finanzmanagements schulen und eine Beziehung zwischen Finanzen und Technik herstellen kann, um die Unternehmenskultur zu fördern, trägt FinOps dazu bei, messbare Ergebnisse für das Unternehmen zu erzielen und

Teams zu ermutigen, kostenbewusst zu bauen. Die Festlegung guter Finanzpraktiken wird in der Säule Kostenoptimierung des Well-Architected Framework ausführlich behandelt, aber wir werden in diesem Whitepaper auf einige der grundlegenden Prinzipien eingehen.

Kostenzuordnungs-Tags

Die Kostenzuweisung bezieht sich auf die Zuweisung oder Verteilung der angefallenen Kosten an die Nutzer oder Begünstigten dieser Kosten nach einem festgelegten Prozess. Im Rahmen dieses Whitepapers unterteilen wir die Kostenzuweisung in zwei Typen: Showback und Chargeback.

Showback-Tools und -Mechanismen tragen dazu bei, das Kostenbewusstsein zu stärken. Chargeback hilft bei der Kostendeckung und fördert das Kostenbewusstsein. Bei Showback geht es um die Darstellung, Berechnung und Meldung der Gebühren, die für eine bestimmte Einheit anfallen, z. B. für eine Geschäftseinheit, eine Anwendung, einen Benutzer oder eine Kostenstelle. Zum Beispiel: „Das Team für Infrastrukturtechnik war im letzten Monat für AWS Ausgaben in Höhe von X $ verantwortlich“. Bei der Rückbuchung geht es um die tatsächliche Verbuchung der entstandenen Kosten an diese Unternehmen über die internen Buchhaltungsprozesse eines Unternehmens, wie z. B. Finanzsysteme oder Journalbelege. Zum Beispiel: „X $ wurden vom Budget des Infrastruktur-Engineering-Teams abgezogen.“ AWS In beiden Fällen kann eine angemessene Kennzeichnung der Ressourcen dazu beitragen, die Kosten einer Entität zuzuweisen. Der einzige Unterschied besteht darin, ob von jemandem eine Zahlung erwartet wird oder nicht.

Die Finanzverwaltung Ihres Unternehmens erfordert möglicherweise eine transparente Abrechnung der anfallenden Kosten auf Anwendungs-, Geschäftsbereichs-, Kostenstellen- und Teamebene. Die durch Cost Allocation Tags unterstützte Kostenzuweisung liefert Ihnen die Daten, die Sie benötigen, um die Kosten, die einer Entität entstanden sind, anhand entsprechend gekennzeichneter Ressourcen genau zuzuordnen.

- Rechenschaftspflicht — Stellen Sie sicher, dass die Kosten denjenigen zugewiesen werden, die für die Ressourcennutzung verantwortlich sind. Eine einzige Servicestelle oder Gruppe kann für Ausgabenprüfungen und Berichte verantwortlich sein.
- Finanzielle Transparenz — Verschaffen Sie sich einen klaren Überblick über die Mittelzuweisungen für die IT, indem Sie effektive Dashboards und aussagekräftige Kostenanalysen für Führungskräfte erstellen.
- Informierte IT-Investitionen — Verfolgen Sie den ROI je nach Projekt, Anwendung oder Geschäftsbereich und versetzen Sie Teams in die Lage, bessere Geschäftsentscheidungen zu treffen, z. B. mehr Mittel für umsatzgenerierende Anwendungen bereitzustellen.

Zusammenfassend können Ihnen die Tags zur Kostenzuweisung dabei helfen, Ihnen folgende Informationen zu geben:

- Wem gehören die Ausgaben und wer ist für deren Optimierung verantwortlich?
- Für welchen Workload, welche Anwendung oder welches Produkt fallen die Ausgaben an? Welche Umgebung oder Phase?
- Welche Ausgabenbereiche wachsen am schnellsten?
- Wie viele Ausgaben können aufgrund vergangener Trends von einem AWS Budget abgezogen werden?
- Wie wirkten sich die Bemühungen zur Kostenoptimierung bei bestimmten Workloads, Anwendungen oder Produkten aus?

Die Aktivierung von Ressourcen-Tags für die Kostenzuweisung hilft bei der Definition von Messmethoden innerhalb der Organisation, anhand derer die AWS Nutzung transparent gemacht und die Rechenschaftspflicht für Ausgaben erhöht wird. Ein weiterer Schwerpunkt liegt auf der Schaffung eines angemessenen Grads an Granularität in Bezug auf Kosten- und Nutzungstransparenz sowie auf der Beeinflussung des Cloud-Nutzungsverhaltens durch Berichte zur Kostenzuweisung und KPI-Tracking.

Aufbau einer Strategie zur Kostenverteilung

Definition und Implementierung eines Kostenverteilungsmodells

Erstellen Sie eine Konto- und Kostenstruktur für die Ressourcen, in denen sie eingesetzt werdenAWS. Stellen Sie das Verhältnis zwischen den AWS Ausgaben, der Art und Weise, wie diese Kosten entstanden sind, und der Person oder dem, was diese Kosten verursacht hat, fest. Gängige Kostenstrukturen basieren auf AWS Organizations Umgebungen und Entitäten innerhalb Ihrer Organisation, z. B. einem Geschäftsbereich oder einer Arbeitslast. AWS-Konten Kostenstrukturen können auf mehreren Attributen basieren, sodass die Kosten auf unterschiedliche Weise oder mit unterschiedlichen Granularitätsebenen untersucht werden können, z. B. indem die Kosten einzelner Workloads auf den Geschäftsbereich, für den sie verwendet werden, zusammengefasst werden.

Bei der Auswahl einer Kostenstruktur, die sich an den gewünschten Ergebnissen orientiert, sollten Sie die Mechanismen zur Kostenverteilung anhand der Einfachheit der Implementierung im Vergleich zur gewünschten Genauigkeit bewerten. Dies könnte Überlegungen in Bezug auf Rechenschaftspflicht, Verfügbarkeit von Tools und kulturelle Veränderungen beinhalten. Drei beliebte Kostenverteilungsmodelle, von denen AWS Kunden in der Regel ausgehen, sind:

- Kontobasiert — Dieses Modell erfordert den geringsten Aufwand und bietet eine hohe Genauigkeit bei Showbacks und Chargebacks. Es eignet sich für Unternehmen mit einer definierten Kontostruktur (und entspricht den Empfehlungen des Whitepapers Organizing Your AWS Environment Using Multiple Accounts). Dies ermöglicht eine klare Kostentransparenz auf Kontobasis. Für Kostentransparenz und Kostenzuweisung können Sie Kosten AWS Cost Explorer- und Nutzungsberichte sowie AWSBudgets für die Kostenüberwachung und -verfolgung verwenden. Diese Tools bieten Filter- und Gruppierungsoptionen nachAWS-Konten. Aus Sicht der Kostenzuweisung muss sich dieses Modell nicht auf eine genaue Kennzeichnung einzelner Ressourcen verlassen.
- Geschäftsbereich- oder teambasiert — Kosten, die Teams, Geschäftseinheiten oder Organisationen innerhalb eines Unternehmens zugewiesen werden können. Dieses Modell erfordert einen moderaten Aufwand, bietet eine hohe Genauigkeit bei Showbacks und Chargebacks und eignet sich für Unternehmen mit einer definierten Kontostruktur (in der Regel mitAWS Organizations), bei der verschiedene Teams, Anwendungen und Workload-Typen getrennt sind. Dies sorgt für eine klare Kostentransparenz zwischen Teams und Anwendungen und reduziert als zusätzlicher Vorteil das Risiko, dass AWSServicequoten innerhalb eines einzigen Pakets erreicht werden. AWS-Konto Beispielsweise kann jedes Team über fünf Konten (`prod`,,`staging`, `testdev`,`sandbox`) verfügen, und keine zwei Teams und Anwendungen teilen sich dasselbe Konto. Mit einer solchen Struktur bieten AWSCost Categories dann die Funktionalität, Konten oder andere Tags („Meta-Tagging“) in Kategorien zu gruppieren, die in den im vorherigen Beispiel genannten Tools nachverfolgt werden können. Es ist wichtig zu beachten, dass dies das Taggen von Konten und Organisationseinheiten (OUs) AWS Organizations ermöglicht. Diese Tags sind jedoch nicht für die Kostenzuweisung und die Fakturierung relevant (das heißt, Sie können Ihre Kosten nicht nach OU gruppieren oder filtern). AWS Cost Explorer AWS Zu diesem Zweck sollten Cost Categories verwendet werden.
- Tag-basiert — Dieses Modell erfordert im Vergleich zu den beiden vorherigen Modellen mehr Aufwand und bietet je nach Anforderungen und Endziel eine hohe Genauigkeit bei Showbacks und Chargebacks. Wir empfehlen Ihnen zwar dringend, die im Whitepaper Organizing Your AWS Environment Using Multiple Accounts beschriebenen Verfahren anzuwenden, aber realistischerweise haben Kunden oft gemischte und komplexe Kontostrukturen, von denen die Migration einige Zeit in Anspruch nimmt. Die Implementierung einer rigorosen und effektiven Tagging-Strategie ist der Schlüssel in diesem Szenario, gefolgt von der Aktivierung relevanter Tags für die Kostenzuweisung in der Billing and Cost Management Kostenmanagement-Konsole (inAWS Organizations, Tags können für die Kostenzuweisung nur über das Management Payer-Konto aktiviert werden). Nachdem die Tags für die Kostenzuweisung aktiviert wurden, können die in den vorherigen Methoden erwähnten Tools für Kostentransparenz und Kostenzuweisung

für Showbacks und Rückbuchungen verwendet werden. Beachten Sie, dass Tags für die Kostenzuweisung nicht rückwirkend sind und erst in den Tools für Rechnungsberichte und Kostenverfolgung angezeigt werden, nachdem sie für die Kostenzuweisung aktiviert wurden.

Zusammenfassend lässt sich sagen, dass Sie, wenn Sie die Kosten nach Geschäftsbereichen verfolgen möchten, AWSCost Categories verwenden können, um verknüpfte Konten innerhalb der AWS Organisation entsprechend zu gruppieren und diese Gruppierung in Abrechnungsberichten anzuzeigen. Wenn Sie separate Konten für Produktions- und Nichtproduktionsumgebungen erstellen, können Sie die Kosten für Umgebungen auch in Tools wie filtern oder diese Kosten AWS Cost Explorermithilfe von Budgets verfolgen. AWS Und wenn Ihr Anwendungsfall eine detailliertere Kostenverfolgung erfordert, z. B. nach einzelnen Workloads oder Anwendungen, können Sie Ressourcen innerhalb dieser Konten entsprechend taggen, diese Tagschlüssel für die Kostenzuweisung auf dem Verwaltungskonto aktivieren und diese Kosten dann in den Tools für die Rechnungsberichterstattung nach Tagschlüsseln filtern.

Einrichtung von Kostenberichterstattungs- und Kontrollprozessen

Identifizieren Sie zunächst die Arten von Kosten, die für interne Stakeholder wichtig sind (z. B. tägliche Ausgaben, Kosten pro Konto, Kosten pro X, amortisierte Kosten). Auf diese Weise können Sie die mit unerwarteten oder ungewöhnlichen Ausgaben verbundenen Haushaltsrisiken schneller mindern, als wenn Sie auf die endgültige Rechnung warten müssen. AWS Tags bieten die Zuordnung, die diese Berichtsszenarien ermöglicht. Die aus der Berichterstattung gewonnenen Erkenntnisse können als Grundlage für Ihre Maßnahmen zur Minderung der Auswirkungen ungewöhnlicher und unerwarteter Ausgaben auf Finanzbudgets dienen. Wenn es zu einem unerwarteten Anstieg der Kosten kommt, ist es wichtig, zu bewerten, ob es zu einem unerwarteten Anstieg des erzielten Nutzens gekommen ist, damit Sie feststellen können, ob und welche Maßnahmen erforderlich sind.

Bei der Entwicklung einer Tagging-Strategie zur Unterstützung der Kostenverteilung sollten Sie die folgenden Elemente berücksichtigen:

- AWS Organizations- Die Kostenzuweisung innerhalb mehrerer Konten kann nach Konten, Kontogruppen oder Gruppen von Stichwörtern erfolgen, die für Ressourcen auf diesen Konten erstellt wurden. Tags, die für Ressourcen erstellt wurden, die sich in einzelnen Konten befinden, AWS Organizations können nur vom Verwaltungskonto aus für die Kostenzuweisung verwendet werden.

- AWSKonto — Die Kostenzuweisung innerhalb eines Kontos AWS-Konto kann durch zusätzliche Dimensionen wie Dienste oder Regionen erfolgen. Es ist möglich, Ressourcen innerhalb eines Accounts weiter zu taggen und mit den Gruppen solcher Ressourcen-Tags zu arbeiten.
- Tags für die Kostenzuweisung — Sowohl von Benutzern erstellte als auch AWS generierte Tags können bei Bedarf für die Kostenzuweisung aktiviert werden. Die Aktivierung von Tags für die Kostenzuweisung in der Abrechnungskonsole (des Verwaltungskontos inAWS Organizations) hilft bei Showbacks und Rückbuchungen.
- Cost AWS Categories — Cost Categories ermöglichen das Gruppieren von Konten und das Gruppieren von Stichwörtern („Metatagging“) innerhalb einer AWS Organisation, wodurch die mit diesen Kategorien verbundenen Kosten mithilfe von Tools wie AWS Cost Explorer AWS Budgets und Kosten- und AWS Nutzungsbericht weiter analysiert werden können.

Durchführung von Showback- und Chargeback-Aktionen für Geschäftsbereiche, Teams oder Organisationen innerhalb des Unternehmens

Ordnen Sie Kosten mithilfe Ihres Kostenzuordnungsprozesses zu, der durch Ihre Kostenstruktur- und Kostenzuweisungs-Tags unterstützt wird. Mithilfe von Stichwörtern können Teams, die zwar nicht direkt für die Bezahlung der Kosten verantwortlich sind, aber dafür verantwortlich sind, dass diese Kosten entstanden sind, als Vorzeigeobjekt dienen. Durch diesen Ansatz wird ein Bewusstsein dafür geschaffen, welchen Beitrag sie zu den Ausgaben leisten und wie diese Kosten entstehen. Führen Sie Rückbuchungen an die Teams durch, die direkt für die Kosten verantwortlich sind, um die Kosten für die verbrauchten Ressourcen zu decken und ihnen bewusst zu machen, welche Kosten und wie sie entstanden sind.

Messung und Verbreitung von Effizienz- oder Wert-KPIs

Vereinbaren Sie eine Reihe von Stückkosten- oder KPI-Metriken, um die Auswirkungen Ihrer Investitionen in das Cloud-Finanzmanagement zu messen. Diese Übung schafft eine gemeinsame Sprache für Technologie- und Geschäftsakteure und erzählt eine Geschichte, die auf der Wissenschaft basiert, und nicht eine Geschichte, die sich ausschließlich auf absolute Gesamtausgaben konzentriert. Weitere Informationen finden Sie in diesem Blog, in dem es darum geht, wie Einheitenkennzahlen dazu beitragen können, die Geschäftsfunktionen aufeinander abzustimmen.

Zuweisung nicht zuweisbarer Ausgaben

Je nach den Rechnungslegungspraktiken der Organisation können unterschiedliche Gebührenarten unterschiedlich behandelt werden müssen. Identifizieren Sie die Ressourcen oder Kostenkategorien, die nicht gekennzeichnet werden können. Vereinbaren Sie je nach den in Anspruch genommenen und geplanten Diensten die Mechanismen, wie solche nicht zuweisbaren Ausgaben behandelt und gemessen werden sollen. Schauen Sie sich zum Beispiel die Liste der Ressourcen an, die von AWS Resource Groupsund Tag Editor unterstützt werden, im AWS Resource Groupsund Tags-Benutzerhandbuch.

Ein gängiges Beispiel für eine Kostenkategorie, die nicht gekennzeichnet werden kann, sind Gebühren für Rabatte auf Basis von Verpflichtungen wie Reserved Instances (RI) und Savings Plans (SP). Abonnementgebühren und ungenutzte SP- und RI-Gebühren können zwar nicht markiert werden, bevor sie in den Tools zur Rechnungsberichterstattung erscheinen, aber Sie können nachträglich verfolgen, wie RI- und SP-Rabatte auf Konten, Ressourcen und deren Tags angewendet werden. AWS Organizations Beispielsweise ist AWS Cost Explorer es möglich, sich die amortisierten Kosten anzusehen, diese Ausgaben nach den entsprechenden Tag-Schlüsseln zu gruppieren und Filter anzuwenden, die für Ihren Anwendungsfall relevant sind. Im AWS Kosten- und Nutzungsbericht (CUR) können Sie Zeilen herausfiltern, die der Nutzung entsprechen, die durch RI- und SP-Rabatte abgedeckt ist (weitere Informationen finden Sie im Abschnitt Anwendungsfälle der CUR-Dokumentation) und die Spalten auswählen, die nur für Sie relevant sind. Jeder für die Kostenzuweisung aktivierte Tagschlüssel wird am Ende des CUR-Berichts in einer eigenen Spalte angezeigt, ähnlich wie er in anderen älteren Abrechnungsberichten, z. B. dem monatlichen Kostenzuordnungsbericht, dargestellt wird. Weitere Informationen finden Sie in den AWSWell-Architected Labs. Dort finden Sie Beispiele für die Gewinnung von Kosten- und Nutzungsinformationen aus CUR-Daten.

Berichterstellung

Zusätzlich zu den verfügbaren AWS Tools zur Unterstützung bei Showbacks und Chargebacks gibt es eine Reihe anderer AWS Lösungen von Drittanbietern, mit denen Sie die Kosten für markierte Ressourcen überwachen und die Effektivität der Tagging-Strategie messen können. Je nach den Anforderungen und dem Endziel des Unternehmens könnte man entweder Zeit und Ressourcen in die Entwicklung maßgeschneiderter Lösungen investieren oder Tools erwerben, die von einem der Kompetenzpartner für AWS CloudManagement-Tools bereitgestellt werden. Wenn Sie sich dafür entscheiden, Ihr eigenes Tool zur Kostenzuweisung mit kontrollierten, für das Unternehmen relevanten Parametern zu erstellen, bietet der AWS Cost and Usage Report (CUR) detaillierteste Kosten- und Nutzungsdaten und ermöglicht die Erstellung benutzerdefinierter

Optimierungs-Dashboards, die das Filtern und Gruppieren nach Konten, Diensten, Kostenkategorien, Kostenzuordnungs-Tags und mehreren anderen Dimensionen ermöglichen. Unter den von That entwickelten CUR-basierten LösungenAWS, die als eines dieser Tools verwendet werden können, finden Sie Cloud Intelligence Dashboards auf der Website von AWS Well-Architected Labs.

Tags für Betrieb und Support

Eine AWS Umgebung wird über mehrere Konten, Ressourcen und Workloads mit unterschiedlichen betrieblichen Anforderungen verfügen. Stichwörter können verwendet werden, um den Betriebsteams Kontext und Anleitungen zur Verfügung zu stellen und die Verwaltung Ihrer Services zu verbessern. Tags können auch verwendet werden, um die betriebliche Steuerung der verwalteten Ressourcen transparent zu machen.

Einige der wichtigsten Faktoren, die für eine einheitliche Definition operativer Tags sprechen, sind:

- Um Ressourcen bei automatisierten Infrastrukturaktivitäten zu filtern. Zum Beispiel beim Bereitstellen, Aktualisieren oder Löschen von Ressourcen. Ein weiterer Grund ist die Skalierung von Ressourcen zur Kostenoptimierung und zur Reduzierung der Nutzung außerhalb der Geschäftszeiten. Ein funktionierendes AWSBeispiel finden Sie in der Instance Scheduler-Lösung.
- Identifizieren isolierter oder veralteter Ressourcen. Ressourcen, die ihre festgelegte Lebensdauer überschritten haben oder die aufgrund interner Mechanismen als isoliert gekennzeichnet wurden, sollten entsprechend gekennzeichnet werden, um das Support-Personal bei der Untersuchung zu unterstützen. Ressourcen, die nicht mehr aktuell sind, sollten vor der Isolierung, Archivierung und Löschung gekennzeichnet werden.
- Support-Anforderungen für eine Gruppe von Ressourcen. Ressourcen haben oft unterschiedliche Support-Anforderungen. Diese Anforderungen können beispielsweise zwischen den Teams ausgehandelt oder als Teil der Wichtigkeit einer Anwendung festgelegt werden. Weitere Hinweise zu Betriebsmodellen finden Sie in der Säule Operational Excellence.
- Verbessern Sie den Prozess des Incident-Managements. Durch die Kennzeichnung von Ressourcen mit Tags, die für mehr Transparenz im Incident-Management-Prozess sorgen, können Support-Teams und Techniker sowie Teams für Major Incident Management (MIM) Ereignisse effektiver verwalten.
- Backups. Mithilfe von Tags können Sie auch ermitteln, wie häufig Ihre Ressourcen gesichert werden müssen und wo die Sicherungskopien abgelegt werden müssen oder wo die Backups wiederhergestellt werden sollen. Präskriptive Leitlinien für Backup- und Wiederherstellungsansätze auf. AWS

- Patchen. Das Patchen veränderlicher Instances, in denen sie ausgeführt werden, AWS ist sowohl für Ihre übergreifende Patch-Strategie als auch für das Patchen von Zero-Day-Schwachstellen von entscheidender Bedeutung. Ausführlichere Hinweise zur umfassenderen Patch-Strategie finden Sie in den präskriptiven Leitlinien. Das Patchen von Zero-Day-Sicherheitslücken wird in diesem Blog behandelt.
- Operative Beobachtbarkeit. Wenn eine operative KPI-Strategie in Ressourcen-Tags übersetzt wird, können die Betriebsteams besser verfolgen, ob die Ziele erreicht werden, um die Geschäftsanforderungen zu verbessern. Die Entwicklung einer KPI-Strategie ist ein eigenständiges Thema, konzentriert sich jedoch in der Regel auf ein Unternehmen, das sich in einem stabilen Zustand befindet, oder darauf, wo die Auswirkungen und Ergebnisse von Veränderungen gemessen werden müssen. Die KPI-Dashboards (AWSWell-Architected Labs) und der Operations KPI Workshop (ein proaktiver Service von AWS Enterprise Support) befassen sich beide mit der Messung der Leistung in einem stabilen Zustand. Der Blogartikel Measuring the Success of Your Transformation zur AWS Unternehmensstrategie befasst sich mit der Messung von KPIs für ein Transformationsprogramm, wie z. B. die IT-Modernisierung oder die Migration von einer lokalen Infrastruktur zu. AWS

Automatisierte Infrastrukturaktivitäten

Tags können für eine Vielzahl von Automatisierungsaktivitäten bei der Verwaltung der Infrastruktur verwendet werden. Mit AWSSystems Manager können Sie beispielsweise Automatisierungen und Runbooks auf Ressourcen verwalten, die durch das definierte Schlüssel-Wert-Paar, das Sie erstellen, spezifiziert sind. Für verwaltete Knoten könnten Sie eine Reihe von Tags definieren, um Knoten nach Betriebssystem und Umgebung zu verfolgen oder als Ziel festzulegen. Sie könnten dann ein Aktualisierungsskript für alle Knoten in einer Gruppe ausführen oder den Status dieser Knoten überprüfen. Systems Manager Manager-Ressourcen können auch mit Tags versehen werden, um Ihre automatisierten Aktivitäten weiter zu verfeinern und zu verfolgen.

Die Automatisierung des Start- und Stopp-Lebenszyklus von Umgebungsressourcen kann für jedes Unternehmen zu einer erheblichen Kostensenkung führen. Instance Scheduler on AWS ist ein Beispiel für eine Lösung, mit der Amazon EC2- und Amazon RDS-Instances gestartet und gestoppt werden können, wenn sie nicht benötigt werden. Beispielsweise nutzen Entwicklerumgebungen, die Amazon EC2- oder Amazon RDS-Instances verwenden und nicht an Wochenenden laufen müssen, das Kosteneinsparpotenzial, das das Herunterfahren dieser Instances bieten kann, nicht aus. Indem Sie die Bedürfnisse der Teams und ihrer Umgebungen analysieren und diese Ressourcen richtig kennzeichnen, um ihr Management zu automatisieren, können Sie Ihr Budget effektiv einsetzen.

Ein Beispiel für ein Schedule-Tag, das vom Instance Scheduler auf einer Amazon EC2 EC2-Instance verwendet wird:

```
{
    "Tags": [
        {
            "Key": "Schedule",
            "ResourceId": "i-1234567890abcdef8",
            "ResourceType": "instance",
            "Value": "mon-9am-fri-5pm"
        }
    ]
}
```

Workload-Lebenszyklus

Überprüfen Sie die Genauigkeit der unterstützenden Betriebsdaten. Stellen Sie sicher, dass die Tags, die mit Ihrem Workload-Lebenszyklus verknüpft sind, regelmäßig überprüft werden und dass die entsprechenden Beteiligten an diesen Überprüfungen beteiligt sind.

Tabelle 7 — Überprüfen Sie die operativen Tags im Rahmen des Workload-Lebenszyklus

Anwendungsfall	Schlüsselwort	Begründung	Beispielwerte
Kontoinhaber	`example-inc:account-owner:owner`	Der Besitzer des Kontos und der darin enthaltenen Ressourcen.	`ops-center` , `dev-ops`, `app-team`
Bewertung des Kontoinhabers	`example-inc:account-owner:review`	Überprüfung der Angaben zur Kontoinhaberschaft auf dem neuesten Stand und korrekt.	<review date in the correct format defined in your tagging library>
Dateneigentümer	`example-inc:data-owner:owner`	Der Dateneigentümer der Konten, in denen Daten gespeichert sind.	`bi-team`, `logistics` , `security`

Anwendungsfall	Schlüsselwort	Begründung	Beispielwerte
Überprüfung durch Dateninhaber	`example-inc:data-owner:review`	Überprüfung der Aktualität und Richtigkeit der Angaben zum Dateneigentum.	<review date in the correct format defined in your tagging library>

Zuweisen von Tags zu gesperrten Konten vor der Migration zur gesperrten Organisationseinheit

Bevor Sie ein Konto sperren und in die gesperrte Organisationseinheit wechseln, wie im Whitepaper Organizing Your AWS Environment Using Multiple Accounts beschrieben, sollten Sie dem Konto Tags hinzufügen, um Sie bei der internen Rückverfolgung und Prüfung des Lebenszyklus eines Accounts zu unterstützen. Zum Beispiel eine relative URL oder Ticketreferenz im ITSM-Ticketsystem einer Organisation, die den Prüfpfad für eine Anwendung anzeigt, die gesperrt wurde.

Tabelle 8 — Fügen Sie Betriebs-Tags hinzu, wenn der Workload-Lebenszyklus in eine neue Phase eintritt

Anwendungsfall	Schlüsselwort	Begründung	Beispielwerte
Kontoinhaber	`example-inc:account-owner:owner`	Der Besitzer des Kontos und der darin enthaltenen Ressourcen.	`ops-center` , `dev-ops`, `app-team`
Dateneigentümer	`example-inc:data-owner:owner`	Der Dateneigentümer der Konten, in denen Daten gespeichert sind.	`bi-team`, `logistics` , `security`
Datum der Sperrung	`example-inc:suspension:date`	Das Datum, an dem das Konto gesperrt wurde	<suspended date in the correct format defined in your tagging library>

Anwendungsfall	Schlüsselwort	Begründung	Beispielwerte
Genehmigung für die Aussetzung	`example-inc:suspension:approval`	Der Link zur Genehmigung der Kontosperrung	`workload/deprecation`

Verwaltung von Zwischenfällen

Tags können in allen Phasen des Vorfallmanagements eine wichtige Rolle spielen, angefangen bei der Protokollierung, Priorisierung, Untersuchung, Kommunikation, Lösung bis hin zur Schließung von Vorfällen.

Mithilfe von Tags können detailliert beschrieben werden, wo ein Vorfall protokolliert werden soll, welches Team oder welche Teams über den Vorfall informiert werden sollen und welche Eskalationspriorität festgelegt wurde. Es ist wichtig, sich daran zu erinnern, dass Tags nicht verschlüsselt sind. Überlegen Sie sich also, welche Informationen Sie darin speichern. Außerdem ändern sich die Zuständigkeiten in Organisationen, Teams und Berichtslinien. Erwägen Sie daher, einen Link zu einem sicheren Portal zu speichern, über das diese Informationen effektiver verwaltet werden können. Diese Tags müssen nicht exklusiv sein. Die Anwendungs-ID könnte beispielsweise verwendet werden, um die Eskalationspfade in einem IT-Servicemanagement-Portal nachzuschlagen. Stellen Sie sicher, dass aus Ihren betrieblichen Definitionen eindeutig hervorgeht, dass dieses Tag für mehrere Zwecke verwendet wird.

Die Tags für betriebliche Anforderungen können ebenfalls detailliert sein, damit Störfallmanager und Betriebspersonal ihre Ziele als Reaktion auf einen Vorfall oder ein Ereignis weiter verfeinern können.

Relative Links (zur Knowledge-System-Basis-URL) für Runbooks und Playbooks können als Tags hinzugefügt werden, um die antwortenden Teams bei der Identifizierung der entsprechenden Prozesse, Verfahren und Unterlagen zu unterstützen.

Tabelle 9 — Verwenden Sie betriebliche Kennzeichnungen als Grundlage für das Incident Management

Anwendungsfall	Schlüsselwort	Begründung	Beispielwerte
Verwaltung von Zwischenfällen	`example-inc:incident-`	Das System, das vom Support-Team zur Protokollierung von	`jira`, `servicenow` , `zendesk`

Anwendungsfall	Schlüsselwort	Begründung	Beispielwerte
	`management:escalationlog`	Vorfällen verwendet wird	
Verwaltung von Zwischenfällen	`example-inc:incident-management:escalationpath`	Weg der Eskalation	`ops-center` , `dev-ops`, `app-team`
Kostenverteilung und Vorfallmanagement	`example-inc:cost-allocation:CostCenter`	Überwachen Sie die Kosten nach Kostenstellen. Dies ist ein Beispiel für ein Tag mit doppeltem Verwendungszweck, bei dem die Kostenstelle als Anwendung scode für die Vorfallprotokollierung verwendet wird	`123-*`
Backup-Zeitplan	`example-inc:backup:schedule`	Backup-Zeitplan der Ressource	`Daily`
Spielbuch//Vorfall management	`example-inc:incident-management:playbook`	Dokumentiertes Playbook	`webapp/incident/playbook`

Patchen

Organizations können ihre Patching-Strategie für veränderliche Computerumgebungen automatisieren und dafür sorgen, dass veränderbare Instanzen mit der definierten Patch-Baseline dieser Anwendungsumgebung Schritt halten, indem sie AWS Systems Manager Patch Manager und verwenden. AWS Lambda Eine Tagging-Strategie für veränderbare Instanzen in diesen Umgebungen

kann verwaltet werden, indem diese Instanzen Patchgruppen und Wartungsfenstern zugewiesen werden. In den folgenden Beispielen finden Sie eine Aufteilung von Dev → Test → Prod. AWSFür das Patch-Management veränderlicher Instances sind präskriptive Anleitungen verfügbar.

Tabelle 10 — Betriebs-Tags können umgebungsspezifisch sein

Entwicklung	Staging	Produktion

{
"Tags": [
{
"Key": "Maintenance Window",
"ResourceId": "i-012345678ab9ab111",
"ResourceType": "instance",
"Value": "cron(30 23 ? * TUE#1 *)"
},
{
"Key": "Name",
"ResourceId": "i-012345678ab9ab222",
"ResourceType": "instance",
"Value": "WEBAPP"
},
{
"Key": "Patch Group",
"ResourceId": "i-012345678ab9ab333",
"ResourceType": "instance",
"Value": "WEBAPP-DEV-AL2"
}
]
	{
	"Tags": [
	{
	"Key": "Maintenance Window",
	"ResourceId": "i-012345678ab9ab444",
	"ResourceType": "instance",
	"Value": "cron(30 23 ? * TUE#2 *)"
	},
	{
	"Key": "Name",
	"ResourceId": "i-012345678ab9ab555",
	"ResourceType": "instance",
	"Value": "WEBAPP"
	},
	{
	"Key": "Patch Group",
	"ResourceId": "i-012345678ab9ab666",
	"ResourceType": "instance",
	"Value": "WEBAPP-TEST-AL2"
	}
	]
		{
		"Tags": [
		{
		"Key": "Maintenance Window",
		"ResourceId": "i-012345678ab9ab777",
		"ResourceType": "instance",
		"Value": "cron(30 23 ? * TUE#3 *)"
		},
		{
		"Key": "Name",
		"ResourceId": "i-012345678ab9ab888",
		"ResourceType": "instance",
		"Value": "WEBAPP"
		},
		{
		"Key": "Patch Group",
		"ResourceId": "i-012345678ab9ab999",
		"ResourceType": "instance",
		"Value": "WEBAPP-PROD-AL2"
		}
		]

Entwicklung	Staging	Produktion
`}`	`}`	`}`

Zero-Day-Schwachstellen können auch behoben werden, indem Tags definiert werden, die Ihre Patch-Strategie ergänzen. Eine ausführliche Anleitung finden Sie unter Vermeiden von Zero-Day-Sicherheitslücken mit Sicherheitspatches am selben Tag mithilfe von AWS Systems Manager.

Operative Beobachtbarkeit

Beobachtbarkeit ist erforderlich, um umsetzbare Erkenntnisse über die Leistung Ihrer Umgebungen zu gewinnen und Probleme zu erkennen und zu untersuchen. Sie hat auch einen sekundären Zweck, der es Ihnen ermöglicht, wichtige Leistungsindikatoren (KPIs) und Service Level Objectives (SLOs) wie die Verfügbarkeit zu definieren und zu messen. Für die meisten Unternehmen sind wichtige Betriebs-KPIs die Mean Time to Detect (MTTD) und die Mean Time to Recovery (MTTR) nach einem Vorfall.

Bei der Beobachtbarkeit ist der Kontext wichtig, da Daten gesammelt und anschließend die zugehörigen Tags gesammelt werden. Unabhängig davon, auf welche Service-, Anwendungs- oder Anwendungsebene Sie sich konzentrieren, können Sie nach diesem bestimmten Datensatz filtern und analysieren. Mithilfe von Stichwörtern können Sie das Onboarding von CloudWatch Alarmen automatisieren, sodass die richtigen Teams benachrichtigt werden können, wenn bestimmte Messwerte überschritten werden. Beispielsweise könnten ein Tag-Schlüssel `example-inc:ops:alarm-tag` und der darauf stehende Wert darauf hinweisen, dass der Alarm ausgelöst wurde. CloudWatch Eine Lösung, die dies demonstriert, ist unter Verwenden von Tags zur Erstellung und Verwaltung von CloudWatch Amazon-Alarmen für Amazon EC2 EC2-Instances beschrieben.

Wenn zu viele Alarme konfiguriert sind, kann dies leicht zu einem Alarmsturm führen — wenn eine große Anzahl von Alarmen oder Benachrichtigungen die Bediener schnell überfordert und ihre Gesamteffektivität beeinträchtigt, während die Bediener einzelne Alarme manuell auswählen und priorisieren. Zusätzlicher Kontext für die Alarme kann in Form von Tags bereitgestellt werden. Das bedeutet, dass innerhalb von Amazon Regeln definiert werden können, EventBridge um sicherzustellen, dass der Schwerpunkt auf dem vorgelagerten Problem liegt und nicht auf nachgelagerten Abhängigkeiten.

Die Rolle des Nebenbetriebs DevOps wird oft übersehen, aber in vielen Unternehmen leisten die zentralen Betriebsteams auch außerhalb der normalen Geschäftszeiten immer noch eine

wichtige Erstreaktion. (Weitere Einzelheiten zu diesem Modell finden Sie im Whitepaper Operational Excellence.) Im Gegensatz zu dem DevOps Team, das für den Workload zuständig ist, verfügen sie in der Regel nicht über die gleiche Wissenstiefe. Der Kontext, den Tags in Dashboards und Warnmeldungen bereitstellen, kann sie zum richtigen Runbook für das Problem weiterleiten oder ein automatisiertes Runbook initiieren (weitere Informationen finden Sie im Blogbeitrag Automating Amazon Alarms with). CloudWatch AWS Systems Manager

Tags für Datensicherheit, Risikomanagement und Zugriffskontrolle

Organizations haben unterschiedliche Bedürfnisse und Verpflichtungen in Bezug auf den angemessenen Umgang mit der Datenspeicherung und -verarbeitung zu erfüllen. Die Datenklassifizierung ist ein wichtiger Vorläufer für verschiedene Anwendungsfälle wie Zugriffskontrolle, Datenspeicherung, Datenanalyse und Einhaltung von Vorschriften.

Datensicherheit und Risikomanagement

In einer AWS Umgebung werden Sie wahrscheinlich Konten mit unterschiedlichen Compliance- und Sicherheitsanforderungen haben. Beispielsweise verfügen Sie möglicherweise über eine Entwickler-Sandbox und ein Konto, das die Produktionsumgebung für stark regulierte Arbeitslasten hostet, z. B. für die Verarbeitung von Zahlungen. Indem Sie sie auf verschiedene Konten isolieren, können Sie unterschiedliche Sicherheitskontrollen anwenden, den Zugriff auf vertrauliche Daten einschränken und den Prüfungsumfang für regulierte Workloads reduzieren.

Die Einführung eines einzigen Standards für alle Workloads kann zu Herausforderungen führen. Während viele Kontrollen in der gesamten Umgebung gleichermaßen gelten, sind einige Kontrollen übertrieben oder irrelevant für Konten, die keine spezifischen rechtlichen Rahmenbedingungen erfüllen müssen, und für Konten, bei denen niemals personenbezogene Daten vorhanden sein werden (z. B. eine Entwickler-Sandbox oder Konten für Workload-Entwicklung). Dies führt in der Regel zu falsch positiven Sicherheitsergebnissen, die geprüft und geschlossen werden müssen, ohne dass Maßnahmen ergriffen werden, was den Aufwand der Ergebnisse, die untersucht werden sollten, überflüssig macht.

Tabelle 11 — Beispiele für Tags für Datensicherheit und Risikomanagement

Anwendungsfall	Schlüsselwort	Begründung	Beispielwerte
Verwaltung von Zwischenfällen	`example-inc:incident-`	Das System, das vom Support-Team zur	`jira`, `servicenow` , `zendesk`

Anwendungsfall	Schlüsselwort	Begründung	Beispielwerte
	`management:escalationlog`	Protokollierung von Vorfällen verwendet wird	
Verwaltung von Zwischenfällen	`example-inc:incident-management:escalationpath`	Weg der Eskalation	`ops-center` , `dev-ops`, `app-team`
Klassifizierung von Daten	`example-inc:data:classification`	Klassifizieren Sie Daten aus Gründen der Einhaltung von Vorschriften und Unternehmensführung	`Public`, `Private`, `Confidential` , `Restricted`
-Compliance	`example-inc:compliance:framework`	Identifiziert das Compliance-Framework, dem die Arbeitslast unterliegt	`PCI-DSS`, `HIPAA`

Die manuelle Verwaltung verschiedener Kontrollen in einer AWS Umgebung ist sowohl zeitaufwändig als auch fehleranfällig. Der nächste Schritt besteht darin, die Implementierung geeigneter Sicherheitskontrollen zu automatisieren und die Überprüfung der Ressourcen auf der Grundlage der Klassifizierung dieses Kontos zu konfigurieren. Durch das Anwenden von Tags auf die Konten und die darin enthaltenen Ressourcen kann die Implementierung von Kontrollen automatisiert und entsprechend der Arbeitslast konfiguriert werden.

Beispiel:

Ein Workload umfasst einen Amazon S3 S3-Bucket mit dem Tag `example-inc:data:classification` mit dem Wert`Private`. Die Automatisierung der Sicherheitstools stellt eine AWS Config Regel bereits`s3-bucket-public-read-prohibited`, die die Block Public Access-Einstellungen des Amazon S3 S3-Buckets, die Bucket-Richtlinie und die Bucket-Zugriffskontrollliste (ACL) überprüft und bestätigt, dass die Konfiguration des Buckets für seine Datenklassifizierung geeignet ist. Um sicherzustellen, dass der Inhalt des Buckets mit der Klassifizierung übereinstimmt, kann Amazon Macie so konfiguriert werden, dass nach

personenbezogenen Daten (PII) gesucht wird. Der Blog Using Amazon Macie to Validate S3 Bucket Data Classification untersucht dieses Muster eingehender.

Bestimmte regulatorische Rahmenbedingungen, wie z. B. Versicherungen und Gesundheitswesen, unterliegen möglicherweise verbindlichen Richtlinien zur Aufbewahrung von Daten. Die Datenspeicherung mithilfe von Tags in Kombination mit Amazon S3 Lifecycle-Richtlinien kann eine effektive und einfache Möglichkeit sein, Objektübergänge auf eine andere Speicherebene zu regeln. Amazon S3 S3-Lebenszyklusregeln können auch verwendet werden, um Objekte für die Datenlöschung nach Ablauf der obligatorischen Aufbewahrungsfrist ablaufen zu lassen. Eine ausführliche Anleitung zu diesem Prozess finden Sie unter Vereinfachen Sie Ihren Datenlebenszyklus durch die Verwendung von Objekt-Tags mit Amazon S3 Lifecycle.

Darüber hinaus können Tags dem Prüfer bei der Suche oder Behebung von Sicherheitslücken wichtigen Kontext liefern, der ihm hilft, das Risiko einzuschätzen, und hilft dabei, die entsprechenden Teams mit der Untersuchung oder Abschwächung der Ergebnisse zu beauftragen.

Tags für Identitätsmanagement und Zugriffskontrolle

Bei der Verwaltung der Zugriffskontrolle in einer AWS Umgebung mit AWS IAM Identity Center können Tags verschiedene Skalierungsmuster ermöglichen. Es gibt mehrere Delegierungsmuster, die angewendet werden können. Einige basieren auf Tagging. Wir werden sie einzeln behandeln und Links zu weiterführenden Informationen zu jedem Thema bereitstellen.

ABAC für einzelne Ressourcen

IAM Identity Center-Benutzer und IAM-Rollen unterstützen die attributebasierte Zugriffssteuerung (ABAC), mit der Sie den Zugriff auf Operationen und Ressourcen anhand von Tags definieren können. ABAC reduziert die Notwendigkeit, die Berechtigungsrichtlinien zu aktualisieren, und unterstützt Sie dabei, den Zugriff auf Mitarbeiterattribute aus Ihrem Unternehmensverzeichnis zu stützen. Wenn Sie bereits eine Strategie für mehrere Konten verwenden, kann ABAC zusätzlich zur rollenbasierten Zugriffskontrolle (RBAC) verwendet werden, um mehreren Teams, die mit demselben Konto arbeiten, granularen Zugriff auf verschiedene Ressourcen zu ermöglichen. Beispielsweise können IAM Identity Center-Benutzer oder IAM-Rollen Bedingungen zur Beschränkung des Zugriffs auf bestimmte Amazon EC2 EC2-Instances enthalten, die andernfalls explizit in jeder Richtlinie aufgeführt werden müssten, um auf sie zugreifen zu können.

Da ein ABAC-Autorisierungsmodell für den Zugriff auf Operationen und Ressourcen von Tags abhängt, ist es wichtig, Schutzmaßnahmen vorzusehen, um unbeabsichtigten Zugriff zu verhindern. SCPs können verwendet werden, um Tags in Ihrer gesamten Organisation zu schützen, indem Tags

nur unter bestimmten Bedingungen geändert werden dürfen. Die Blogs Sichern von Ressourcen-Tags, die für die Autorisierung verwendet werden, mithilfe einer Service-Kontrollrichtlinie in AWS Organizations und Permissions Boundaries für IAM-Entitäten finden Sie Informationen zur Implementierung.

Wenn langlebige Amazon EC2-Instances zur Unterstützung traditionellerer Betriebspraktiken verwendet werden, kann dieser Ansatz verwendet werden. Im Blog Configure IAM Identity Center ABAC for Amazon EC2 Instances and Systems Manager Session Manager wird diese Form der attributbasierten Zugriffskontrolle ausführlicher beschrieben. Wie bereits erwähnt, unterstützen nicht alle Ressourcentypen das Tagging, und von denen, die dies tun, unterstützen nicht alle die Durchsetzung mithilfe von Tag-Richtlinien. Daher ist es ratsam, dies zu überprüfen, bevor Sie mit der Implementierung dieser Strategie auf einem beginnenAWS-Konto.

Informationen zu Diensten, die ABAC unterstützen, finden Sie unter Dienste, die mit IAM funktionieren, mithilfe von AWSServices, die mit IAM funktionieren.

Schlussfolgerung

AWSRessourcen können für eine Vielzahl von Zwecken gekennzeichnet werden, von der Implementierung einer Kostenzuweisungsstrategie über die Unterstützung der Automatisierung bis hin zur Autorisierung des Zugriffs auf Ressourcen. AWS Die Implementierung einer Tagging-Strategie kann für einige Unternehmen aufgrund der Anzahl der beteiligten Interessengruppen und Überlegungen wie Datenbeschaffung und Tag-Governance eine Herausforderung sein.

In diesem Whitepaper haben wir Empfehlungen zur Entwicklung und Implementierung einer Tagging-Strategie in einer Organisation dargelegt, die auf betrieblichen Praktiken, definierten Anwendungsfällen, den am Prozess beteiligten Stakeholdern und den von bereitgestellten Tools und Dienstleistungen basiert. AWS Wenn es um eine Tagging-Strategie geht, handelt es sich um einen Prozess der Iteration und Verbesserung, bei dem Sie von Ihrer unmittelbaren Priorität aus klein beginnen, relevante Anwendungsfälle in Ihrem Unternehmen identifizieren und dann das Tagging-Schema nach Bedarf implementieren und erweitern und gleichzeitig die Effektivität kontinuierlich messen und verbessern. Wir haben darauf hingewiesen, dass Sie mit einem klar definierten Satz von Tags innerhalb Ihres Unternehmens die AWS Nutzung und den Verbrauch den Teams zuordnen können, die für die Ressourcen und den Geschäftszweck verantwortlich sind, für die sie existieren, um sie an der Unternehmensstrategie und dem Unternehmenswert auszurichten.

Beitragende Faktoren

Zu den Mitwirkenden an diesem Dokument gehören:

- Chris Pates, Senior Specialist Technical Account Manager, Amazon Web Services
- Vijay Shekhar Rao, Leiter Unternehmenssupport, Amazon Web Services
- Nataliya Godunok, Senior Specialist Technical Account Manager, Amazon Web Services
- Yogish Kutkunje Pai, leitender Lösungsarchitekt, Amazon Internet Services Private Limited
- Jamie Ibbs, Senior Specialist Technical Account Manager, Amazon Web Services

Weitere Informationen

Weitere Informationen finden Sie unter

- AWSre:Invent 2020: Rückwärts arbeiten: Amazons Innovationsansatz
- AWSPräskriptive Leitlinien: Automatisiertes Patchen für veränderbare Instanzen in der Hybrid Cloud mit Systems Manager AWS
- AWSZentrum für Architektur

AWSWell-Architected

- AWSWell-Architected Framework
- Säule Operational Excellence — AWS Well-Architected Framework
- Plan für Disaster Recovery (DR) — Säule AWS der zuverlässigen Architektur
- Säule der Kostenoptimierung — AWS Well-Architected Framework
- AWSWell-Architected Labs: AWS Generierte Kostenzuweisungs-Tags aktivieren
- AWSWell-Architected Labs: Tag-Richtlinien
- AWSWell-Architected Labs: AWS CUR-Abfragebibliothek

AWSBlogs

- AWS HealthAware — Passen Sie AWS Health Benachrichtigungen für Organisations- und AWS Privatkonten an
- So kennzeichnen Sie Amazon EC2 EC2-Ressourcen automatisch als Reaktion auf API-Ereignisse
- AWSGeneriertes und benutzerdefiniertes Kostenzuweisungs-Tag
- Kostenkennzeichnung und Berichterstattung mit AWS Organizations
- Patchen Ihrer Windows EC2-Instances mithilfe von Patch Manager AWS Systems Manager
- Vermeiden Sie Zero-Day-Schwachstellen mit Sicherheitspatches am selben Tag mithilfe von AWS Systems Manager

AWS-Dokumentation

- Verwendung von Tags für die Kostenzuweisung — AWS Billing and Cost Management und Kostenmanagement und Kostenmanagement

- Was sind AWS Kosten- und Nutzungsberichte
- AWS Resource Groups API Referenz
- Wie kann ich mithilfe von IAM-Policy-Tags einschränken, wie eine EC2-Instance oder ein EBS-Volume erstellt werden kann?
- Veränderliche und unveränderliche Aktualisierungsmodelle

Sonstige

- Bryar, C. und Carr, B. (2021). Rückwärts arbeiten: Einblicke, Geschichten und Geheimnisse aus Amazon. London Macmillan.
- AWS CloudFormationWache () GitHub

Dokumentversionen

Wenn Sie über Aktualisierungen dieses Whitepapers benachrichtigt werden möchten, abonnieren Sie den RSS-Feed.

Änderung	Beschreibung	Datum
Geringfügiges Update	Aktualisierungen des Identität smanagements	30. März 2023
Geringfügige Überarbeitung	Aktualisierte Referenz in ABAC für einzelne Ressource n.	24. Februar 2023
Geringfügige Überarbeitung	Aktualisierter Leitfaden, angepasst an die bewährten IAM-Methoden. Weitere Informationen finden Sie unter Bewährte IAM-Methoden.	6. Februar 2023
Größere Überarbeitung	Es wurde eine genauere Referenz für Ressourcentypen hinzugefügt, die von AWS Config der Regel unterstützt werden`required_tags` .	18. Januar 2023
Größere Revision	Es wurde aktualisiert und enthält nun die neuesten Verfahren und Servicefu nktionen, insbesondere im Bereich Identität.	29. September 2022
Geringfügiges Update	Die Tabellenformatierung in der PDF-Version wurde behoben.	25. April 2022
Größere Überarbeitung	Die Dokumentstruktur wurde aktualisiert und die Abschnitt	22. April 2022

	e „Tagging-Strategie“ und „Anwendungsfälle“ wurden erweitert. Es wurden weitere präskriptive Anleitungen hinzugefügt, die auf den neuesten Tools, Techniken und verfügbaren Ressourcen basieren.	
Erste Veröffentlichung	Erstveröffentlichtes Whitepaper.	1. Dezember 2018

> **Note**
>
> Um RSS-Updates zu abonnieren, muss für den von Ihnen verwendeten Browser ein RSS-Plugin aktiviert sein.

Hinweise

Die Kunden sind dafür verantwortlich, die Informationen in diesem Dokument selbst unabhängig zu beurteilen. Dieses Dokument: (a) dient nur zu Informationszwecken, (b) stellt aktuelle AWS Produktangebote und Praktiken dar, die ohne vorherige Ankündigung geändert werden können, und (c) stellt keine Verpflichtungen oder Zusicherungen von AWS und seinen verbundenen Unternehmen, Lieferanten oder Lizenzgebern dar. AWSProdukte oder Dienstleistungen werden „wie sie sind“ ohne ausdrückliche oder stillschweigende Garantien, Zusicherungen oder Bedingungen jeglicher Art bereitgestellt. Die Verantwortlichkeiten und Verbindlichkeiten AWS gegenüber seinen Kunden werden durch AWS Vereinbarungen geregelt, und dieses Dokument ist weder Teil einer Vereinbarung zwischen AWS und seinen Kunden noch ändert es diese.

AWS-Glossar

Die neueste AWS-Terminologie finden Sie im AWS-Glossar in der AWS-Glossar-Referenz.

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.