Documento técnico de AWS

Prácticas recomendadas para el etiquetado de los recursos de AWS

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Prácticas recomendadas para el etiquetado de los recursos de AWS: Documento técnico de AWS

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Las marcas comerciales y la imagen comercial de Amazon no se pueden utilizar en relación con ningún producto o servicio que no sea de Amazon, de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas comerciales que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, relacionados o patrocinados por Amazon.

Table of Contents

Resumen e introducción i
¿Tiene una buena arquitectura? 1
Introducción 1
¿Qué son las etiquetas? 3
Creación de la estrategia de etiquetado 7
Definición de las necesidades y los casos de uso 8
Definición y publicación de un esquema de etiquetado 10
AWS Organizations: Políticas de etiquetas 13
ExampleInc-CostAllocation.json 13
ExampleInc-DisasterRecovery.json 14
Implementación y aplicación del etiquetado 16
Recursos administrados manualmente 16
Recursos administrados por la infraestructura como código (IaC) 16
Recursos administrados por canalización de CI/CD 18
Cumplimiento 19
Medir la eficacia del etiquetado e impulsar mejoras 23
Etiquetado de casos de uso 25
Etiquetas para la asignación de costos y la administración financiera 25
Etiquetas de asignación de costos 26
Elaboración de una estrategia de asignación de costos 27
Etiquetas para operaciones y ayuda 31
Actividades de infraestructura automatizadas 33
Ciclo de vida de la carga de trabajo 34
Administración de incidentes 35
Aplicación de parches 37
Observabilidad operativa 38
Etiquetas para la seguridad de los datos, la administración de riesgos y el control de acceso 39
Seguridad de datos y administración de riesgos 39
Etiquetas para administración de identidades y control de acceso 41
Conclusión 43
Colaboradores 44
Documentación adicional 45
Revisiones del documento 47
Avisos 49

Glosario de AWS 50

Prácticas recomendadas para el etiquetado de los recursos de AWS

Fecha de publicación: 30 de marzo de 2023 (Revisiones del documento)

Amazon Web Services (AWS) le permite asignar metadatos a muchos de los recursos de AWS en forma de etiquetas. Cada etiqueta es una etiqueta simple que consta de una clave y un valor opcional para almacenar información sobre el recurso o los datos retenidos en ese recurso. Este documento técnico se centra en el etiquetado de casos de uso, estrategias, técnicas y herramientas que le pueden ayudar a clasificar los recursos por propósito, equipo, entorno u otros criterios relevantes para la empresa. La implementación de una estrategia de etiquetado coherente puede facilitar el filtrado y la búsqueda de recursos, el monitoreo del costo y el uso, y la administración del entorno de AWS.

Este documento se basa en las prácticas y la orientación proporcionadas en el documento técnico Organización del entorno de AWS con varias cuentas. Se recomienda que lea ese documento técnico primero y, luego, este. AWS recomienda que establezca la base de la nube de forma holística. Para obtener información adicional, consulte Establecimiento de la base de la nube en AWS.

¿Tiene una buena arquitectura?

El marco de buena arquitectura de AWS le ayuda a entender las ventajas y desventajas de las decisiones que toma al crear sistemas en la nube. Los seis pilares del marco le permitirán aprender las prácticas recomendadas de arquitectura para diseñar y utilizar sistemas fiables, seguros, eficientes, rentables y sostenibles. Mediante AWS Well-Architected Tool, disponible sin costo alguno en la AWS Management Console, puede comparar las cargas de trabajo con estas prácticas recomendadas respondiendo a una serie de preguntas para cada pilar.

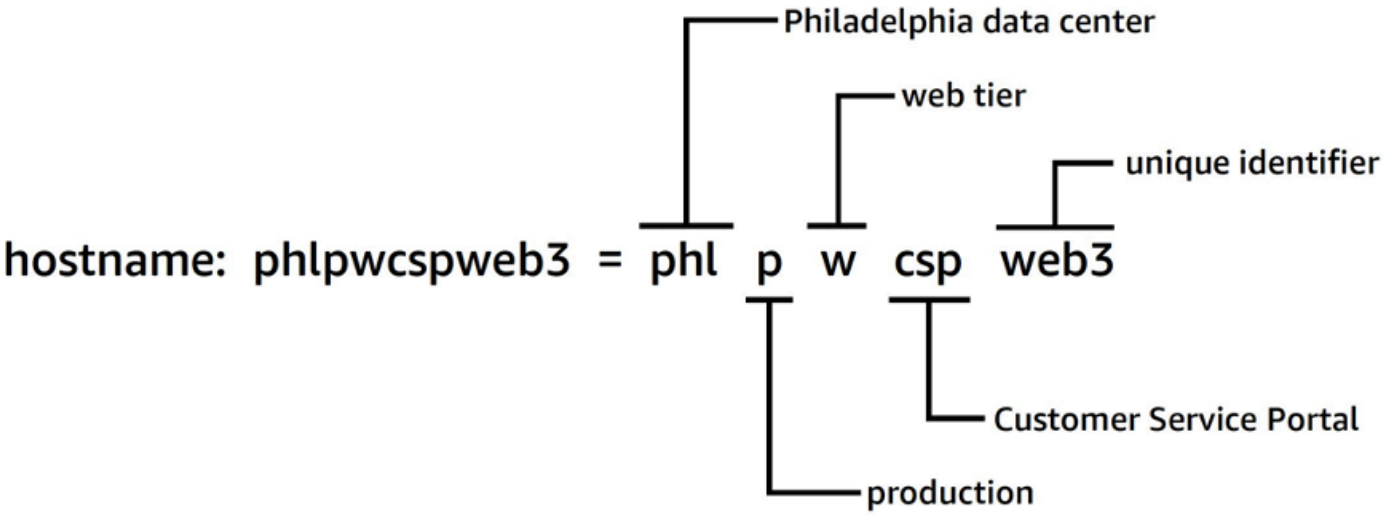
Para obtener más orientación experta y prácticas recomendadas para la arquitectura de la nube (implementaciones de arquitectura de referencia, diagramas y documentos técnicos), consulte el Centro de arquitectura de AWS.

Introducción

AWS facilita la implementación de las cargas de trabajo en AWS mediante la creación de recursos, como instancias de Amazon EC2, volúmenes de Amazon EBS, grupos de seguridad y funciones de

AWS Lambda. También puede escalar y hacer crecer la flota de recursos de AWS que alojan las aplicaciones, almacenan los datos y amplían la infraestructura de AWS a lo largo del tiempo. Como el uso de AWS se amplía a muchos tipos de recursos que abarcan varias aplicaciones, necesitará un mecanismo para realizar un seguimiento de los recursos que se asignan a cada aplicación. Utilice este mecanismo para respaldar las actividades operativas, como el monitoreo de costos, la gestión de incidentes, la aplicación de parches, las copias de seguridad y el control de acceso.

En los entornos en las instalaciones, este conocimiento suele plasmarse en los sistemas de gestión del conocimiento, los sistemas de gestión de documentos y en las páginas wiki internas. Con una base de datos de gestión de la configuración (CMDB), puede almacenar y administrar los metadatos detallados pertinentes mediante procesos de control de cambios estándar. Este enfoque proporciona control, pero su desarrollo y mantenimiento requieren un esfuerzo adicional. Puede adoptar un enfoque estructurado para la denominación de los recursos, pero el nombre de un recurso solo puede contener una cantidad limitada de información.



Enfoque estructurado para la denominación de los recursos

Por ejemplo, las instancias EC2 tienen una etiqueta predefinida llamada Nombre que proporciona una funcionalidad similar y permite asignar nombres a las cargas de trabajo a medida que se trasladan a AWS.

En 2010, AWS lanzó etiquetas de recursos para proporcionar un mecanismo flexible y escalable para adjuntar metadatos a los recursos. Este documento técnico lo guía a través del proceso de desarrollo e implementación de una estrategia de etiquetado sólida en todo el entorno de AWS. Esta guía lo ayudará a garantizar la coherencia y la cobertura del etiquetado que respalden las actividades operativas y de toma de decisiones

¿Qué son las etiquetas?

Una etiqueta es un par clave-valor que se aplica a un recurso para almacenar metadatos sobre ese recurso. Cada etiqueta es una marca que consta de una clave y un valor opcional. Actualmente, no todos los tipos de servicios y recursos admiten etiquetas (consulte Servicios que admiten la API de etiquetado de grupos de recursos). Es posible que otros servicios admitan etiquetas a través de sus propias API. Se debe tener en cuenta que las etiquetas no están cifradas y no se deben usar para almacenar datos confidenciales, como información de identificación personal (PII).

Las etiquetas que un usuario crea y aplica a los recursos de AWS con la AWS CLI, la API o la AWS Management Console se conocen como etiquetas definidas por el usuario. Varios servicios de AWS, como AWS CloudFormation, Elastic Beanstalk y escalado automático, asignan etiquetas automáticamente a los recursos que crean y administran. Estas claves se conocen como etiquetas generadas por AWS y, por lo general, tienen el prefijo `aws`. Este prefijo no se puede utilizar en las claves de etiquetas definidas por el usuario.

Existen requisitos de uso y límites en cuanto al número de etiquetas definidas por el usuario que se pueden agregar a un recurso de AWS. Para obtener más información, consulte Límites y requisitos para la denominación de etiquetas en la Guía de referencia general de AWS. Las etiquetas generadas por AWS no se tienen en cuenta para estos límites de etiquetas definidos por el usuario.

Tabla 1: Ejemplos de claves y valores de etiquetas definidos por el usuario

ID de instancia	Clave de etiqueta	Valor de etiqueta
`i-01234567abcdef89a`	`CostCenter`	`98765`
	`Stack`	`Test`
i-12345678abcdef90b	`CostCenter`	`98765`
	`Stack`	`Production`

Tabla 2: Ejemplos de etiquetas generadas por AWS

Claves de etiquetas generadas por AWS	Justificación
`aws:ec2spot:fleet-request-id`	Identifica la solicitud de instancia de spot de Amazon EC2 que lanzó la instancia
`aws:cloudformation:stack-name`	Identifica la pila de AWS CloudFormation que creó el recurso
`lambda-console:blueprint`	Identifica el esquema utilizado como plantilla para una función de AWS Lambda
`elasticbeanstalk:environment-name`	Identifica la aplicación que creó el recurso
`aws:servicecatalog: provisionedProductArn`	El nombre de recurso de Amazon (ARN) del producto aprovisionado
`aws:servicecatalog:productArn`	El ARN del producto desde el que se lanzó el producto aprovisionado

Las etiquetas generadas por AWS forman un espacio de nombres. Por ejemplo, en una plantilla de AWS CloudFormation, se define un conjunto de recursos que se van a implementar juntos en una `stack`, donde `stack-name` es un nombre descriptivo que se asigna para identificarlo. Si examina una clave como `aws:cloudformation:stack-name`, puede ver el espacio de nombres que se utiliza para determinar si el parámetro utiliza tres elementos: aws la organización, cloudformation el servicio y nombre de pila el parámetro.

Las etiquetas definidas por el usuario también pueden usar espacios de nombres y se recomienda usar un identificador organizativo como prefijo. Esto le ayuda a identificar rápidamente si una etiqueta es algo del esquema administrado o algo definido por un servicio o una herramienta que utilice en el entorno.

En el documento técnico Establecimiento de la base de nube en AWS, recomendamos un conjunto de etiquetas que se deberían implementar. Es muy probable que diferentes empresas tengan diferentes patrones permitidos y listas diferentes para una etiqueta determinada. Observación del ejemplo de la tabla 3:

Tabla 3: Misma clave de etiqueta, diferentes reglas de validación de valores

Organización	Clave de etiqueta	Validación de valores de etiquetas	Ejemplo de valor de etiqueta
Empresa A	`CostCenter`	`5432, 5422, 5499`	`5432`
Empresa A	`CostCenter`	`ABC*`	`ABC123`

Si estos dos esquemas están en organizaciones diferentes, no hay ningún problema con los conflictos de etiquetas. Sin embargo, si estos dos entornos se fusionan, los espacios de nombres pueden entrar en conflicto y la validación se vuelve más compleja. Este escenario puede parecer poco probable, pero las empresas se adquieren o se fusionan y hay otros escenarios, como los clientes que trabajan con un proveedor de servicios administrados, un publicador de juegos o una empresa de capital de riesgo, en los que las cuentas de diferentes organizaciones forman parte de una organización de AWS compartida. Al utilizar el nombre de la empresa como prefijo para definir un espacio de nombres único, se pueden evitar estos desafíos, como se muestra en la tabla 4:

Tabla 4: Uso de espacios de nombres en las claves de etiquetas

Organización	Clave de etiqueta	Validación de valores de etiquetas	Ejemplo de valor de etiqueta
Empresa A	`company-a :CostCenter`	`5432, 5422, 5499`	`5432`
Empresa B	`company-b :CostCenter`	`ABC*`	`ABC123`

En las organizaciones grandes y complejas en las que las empresas se adquieren y liquidan con regularidad, esta situación se producirá con más frecuencia. A medida que los procesos y prácticas de la nueva adquisición se armonicen en todo el grupo, la situación se resolverá. Disponer de espacios de nombres distintos ayuda, ya que se puede informar sobre el uso de las etiquetas antiguas y contactar con los equipos pertinentes para que adopten el nuevo esquema. Un espacio de nombres también se puede usar para indicar un ámbito o representar un caso de uso o un área de responsabilidad que esté alineada con los propietarios de la organización.

Tabla 5: Ejemplo del ámbito o del ámbito de un caso de uso en las claves de etiquetas

Caso de uso	Clave de etiqueta	Justificación	Valores permitidos
Clasificación de datos	`example-inc:info-sec:data-classification`	Conjunto de clasificación de datos definido por la seguridad de la información	`sensitive`, `company-confidential`, `customer-identifiable`
Operaciones	`example-inc:dev-ops:environment`	Implementar la programación de los entornos de prueba y desarrollo	`development`, `staging`, `quality-assurance`, `production`
Recuperación de desastres	`example-inc:disaster-recovery:rpo`	Definir el objetivo de punto de recuperación (RPO) de un recurso	6h, 24h
Asignación de costos	`example-inc:cost-allocation:business-unit`	Los equipos de finanzas necesitan informes de costos sobre el uso y los gastos de cada equipo	`corporate`, `recruitment`, `support`, `engineering`

Las etiquetas son sencillas y flexibles. La clave y el valor de la etiqueta son cadenas de longitud variable y admiten un conjunto de caracteres amplio. Para obtener más información sobre longitudes y conjuntos de caracteres, consulte Etiquetado de los recursos de AWS en la Referencia general de AWS. Las etiquetas distinguen entre mayúsculas y minúsculas, lo que significa que `costCenter` y `costcenter` son claves de etiquetas diferentes. En distintos países, la ortografía de una palabra puede variar, lo que puede afectar a las claves. Por ejemplo, en Estados Unidos, se puede definir una clave como `costcenter`, pero en Reino Unido, es posible que se prefiera `costcentre`. Estas son claves diferentes desde la perspectiva del etiquetado de recursos. Defina la ortografía, las mayúsculas y minúsculas y la puntuación como parte de la estrategia de etiquetado. Utilice estas definiciones como referencia para cualquier persona que cree o administre recursos. Este tema se analiza con más detalle en la siguiente sección, Creación de la estrategia de etiquetado.

Creación de la estrategia de etiquetado

Como ocurre con muchas prácticas de operaciones, la implementación de una estrategia de etiquetado es un proceso de iteración y mejora. Comience poco a poco con su prioridad inmediata y amplíe el esquema de etiquetado a medida que lo necesite.

Ciclo de iteración y mejora de la estrategia de etiquetado

A lo largo de este proceso, la propiedad es clave para la responsabilidad y el progreso. Como las etiquetas se pueden utilizar para una variedad de propósitos, la estrategia general de etiquetado se puede dividir en áreas de responsabilidad dentro de una organización. El etiquetado permite un enfoque programático de las actividades que dependen de la caracterización de los recursos. La variedad de partes interesadas que pueden beneficiarse del etiquetado dependerá del tamaño de la organización y de las prácticas operativas. Las organizaciones más grandes pueden beneficiarse de una definición clara de las responsabilidades de los equipos que participan en la creación e implementación de una estrategia de etiquetado. Algunas partes interesadas pueden ser

responsables de identificar las necesidades (definir los casos de uso) del etiquetado; otras pueden ser responsables de mantener, implementar y mejorar la estrategia de etiquetado.

Al asignar la propiedad, se encuentra en una buena posición para implementar aspectos individuales de la estrategia. Cuando proceda, esta propiedad puede formalizarse como política y documentarse en una matriz de responsabilidad (por ejemplo, RACI: responsable, confiable, consultada e informada) o en un modelo de responsabilidad compartida. En las organizaciones más pequeñas, es posible que los equipos desempeñen múltiples funciones en una estrategia de etiquetado, desde la definición de los requisitos hasta la implementación y el cumplimiento.

Definición de las necesidades y los casos de uso

Comience a desarrollar la estrategia interactuando con las partes interesadas que tienen una necesidad subyacente fundamental de consumir metadatos. Estos equipos definen los metadatos con los que deben etiquetarse los recursos para respaldar las actividades, como la elaboración de informes, la automatización y la clasificación de datos. Describen cómo deben organizarse los recursos y a qué políticas se deben asignar. Algunos ejemplos de roles y funciones que estas partes interesadas pueden tener en las organizaciones:

- Finanzas y Línea de negocio deben comprender el valor de la inversión asignándolo a los costos para priorizar las acciones que deben tomarse al abordar la ineficiencia. La comprensión del costo frente al valor generado ayuda a identificar las líneas de negocio o las ofertas de productos erróneas. Esto lleva a tomar decisiones informadas sobre la continuidad del soporte, la adopción de una alternativa (por ejemplo, el uso de una oferta de SaaS o un servicio administrado) o la retirada de una oferta empresarial no rentable.
- La gobernanza y el cumplimiento deben comprender la categorización de los datos (por ejemplo, públicos o confidenciales), si una carga de trabajo específica está dentro o fuera del ámbito de auditoría según una norma o reglamento específicos y la importancia del servicio (si el servicio o la aplicación son fundamentales para la empresa) para aplicar los controles y la supervisión adecuados, como los permisos, las políticas y el monitoreo.
- Las operaciones y el desarrollo necesitan comprender el ciclo de vida de la carga de trabajo, las etapas de implementación de los productos compatibles y la gestión de las etapas de lanzamiento (por ejemplo, desarrollo, prueba o división de producción), así como las prioridades de soporte asociadas y los requisitos de gestión de las partes interesadas. También es necesario definir y comprender tareas como las copias de seguridad, la aplicación de parches, la observabilidad y la obsolescencia.

- Seguridad de la información (InfoSec) y Operaciones de seguridad (SecOps) describen qué controles se deben aplicar y cuáles se recomiendan. InfoSec normalmente define la implementación de los controles y SecOps generalmente es responsable de administrarlos.

En función del caso de uso, las prioridades, el tamaño de la organización y las prácticas operativas, es posible que necesite la representación de varios equipos de la organización, como los de finanzas (incluidas las adquisiciones), seguridad de la información, habilitación de la nube y operaciones en la nube. También necesita la representación de los propietarios de aplicaciones y procesos para funciones como la aplicación de parches, la copia de seguridad y la restauración, el monitoreo, la programación de tareas y la recuperación de desastres. Estos representantes ayudan a impulsar la definición, la implementación y la medición de la eficacia de la estrategia de etiquetado. Deberían trabajar retrospectivamente a partir de las partes interesadas y los casos de uso y llevar a cabo un taller interfuncional. En el taller, tienen la oportunidad de compartir sus perspectivas y necesidades y ayudar a impulsar una estrategia general. Más adelante en este documento técnico se describen ejemplos de los participantes y su participación en varios casos de uso.

Las partes interesadas también definen y validan las claves de las etiquetas obligatorias y pueden recomendar el alcance de las etiquetas opcionales. Por ejemplo, es posible que los equipos financieros necesiten relacionar un recurso con un centro de costos interno, una unidad empresarial o ambos. Por lo tanto, es posible que necesiten que determinadas claves de etiquetas, como `CostCenter` y `BusinessUnit`, sean obligatorias. Es posible que los equipos de desarrollo individuales decidan utilizar etiquetas adicionales con fines de automatización, como `EnvironmentName`, `OptIn` u `OptOut`.

Las principales partes interesadas deben ponerse de acuerdo sobre el enfoque de la estrategia de etiquetado y documentar las respuestas a las preguntas relacionadas con el cumplimiento y el gobierno, tales como:

- ¿Qué casos de uso se deben abordar?
- ¿Quién es responsable de etiquetar los recursos (implementación)?
- ¿Cómo se aplican las etiquetas y qué métodos y automatizaciones se utilizarán (proactivos o reactivos)?
- ¿Cómo se miden la eficacia y los objetivos del etiquetado?
- ¿Con qué frecuencia se debe revisar la estrategia de etiquetado?
- ¿Quién impulsa las mejoras? ¿Cómo se hace esto?

Las funciones empresariales, como la habilitación de la nube, la gestión empresarial de la nube y la ingeniería de plataformas de la nube, pueden entonces desempeñar un papel de facilitadoras para el proceso de creación de la estrategia de etiquetado, ayudar a impulsar su adopción y garantizar la coherencia de su aplicación al medir el progreso, eliminar los obstáculos y reducir la duplicación de esfuerzos.

Definición y publicación de un esquema de etiquetado

Emplee un enfoque coherente al etiquetar los recursos de AWS, tanto para etiquetas obligatorias como opcionales. Un esquema de etiquetado completo le ayuda a lograr esta coherencia. Los siguientes ejemplos le pueden ayudar a comenzar:

- Acordar las claves de etiquetas obligatorias
- Definir los valores aceptables y las convenciones de nomenclatura de las etiquetas (mayúsculas o minúsculas, guiones o guiones bajos, jerarquía, etc.)
- Confirmar valores no constituiría información de identificación personal (PII)
- Decidir quién puede definir y crear nuevas claves de etiquetas
- Acordar cómo agregar nuevos valores de etiquetas obligatorios y cómo administrar las etiquetas opcionales

Revise la tabla categorías de etiquetado siguiente, que se puede utilizar como referencia de lo que es posible que incluya en el esquema de etiquetado. Aún debe determinar la convención que utilizará para la clave de etiqueta y los valores permitidos para cada una de ellas. El esquema de etiquetado es el documento en el que se define esto para el entorno.

Tabla 6: Ejemplo de un esquema de etiquetado definitivo (parte 1)

Caso de uso	Clave de etiqueta	Justificación	Valores permitidos (mostrados o con el prefijo o sufijo del valor)	Usado para la asignación de costos	Tipos de recurso	Ámbito	Obligatorio
Asignación de costos	`example-inc:cost-allocation: ApplicationId`	Realizar un seguimiento del costo frente al valor generado por cada línea de negocio	`DataLakeX` , `RetailSiteX`	Y	Todos	Todos	Obligatorio
Asignación de costos	`example-inc:cost-allocation: BusinessUnitId`	Monitorear los costos por unidad de negocio	`Architecture` , `DevOps`, `Finance`	Y	Todos	Todos	Obligatorio
Asignación de costos	`example-inc:cost-allocation: CostCenter`	Monitorear los costos por centro de costos	`123-*`	Y	Todos	Todos	Obligatorio
Asignación de costos	`example-inc:cost-allocation :Owner`	Qué titular del presupuesto es responsable de esta carga de trabajo	`Marketing` , `RetailSupport`	Y	Todos	Todos	Obligatorio
Control de	`example-inc:access`	Identificar el subcompon	`DB_Layer`, `Web Layer` ,	N	Todos	Todos	Opcional

Tabla 6: Ejemplo de un esquema de etiquetado definitivo (parte 2)

Caso de uso	Clave de etiqueta	Justificación	Valores permitidos (mostrados o con el prefijo o sufijo del valor)	Usado para la asignación de costos	Tipos de recurso	Ámbito	Obligatorio
DevOps	`example-inc:operations: Owner`	Qué equipo o plantilla es responsable de la creación y el mantenimiento del recurso	`Squad01`	N	Todos	Todos	Obligatorio
Recuperación de desastres	`example-inc:disaster-recovery:rpo`	Definir el objetivo de punto de recuperación (RPO) de un recurso	`6h`, `24h`	N	S3, EBS	Prod.	Obligatorio
Clasificación de datos	`example-inc:data:classification`	Clasificar los datos para garantizar el cumplimiento y el gobierno	`Public`, `Private`, `Confidential` , `Restricted`	N	S3, EBS	Todos	Obligatorio
Conformidad de	`example-inc:compliance:framework`	Identifica el marco de cumplimiento al que está sujeta la carga de trabajo	`PCI-DSS`, `HIPAA`	N	Todos	Prod.	Obligatorio

Una vez definido el esquema de etiquetado, administre el esquema en un repositorio con control de versiones al que puedan acceder todas las partes interesadas pertinentes para facilitar su consulta y realizar un seguimiento de las actualizaciones. Este enfoque mejora la eficiencia y permite la agilidad.

AWS Organizations: Políticas de etiquetas

Las políticas de AWS Organizations le permiten aplicar tipos adicionales de administración a las Cuentas de AWS de la organización. Una política de etiquetas es la forma en que puede expresar el esquema de etiquetado en formato JSON para que la plataforma pueda informar y, opcionalmente, aplicar el esquema en el entorno de AWS. La política de etiquetas define los valores que son aceptables para una clave de etiqueta en tipos de recursos específicos. Esta política puede tener la forma de una lista de valores o de un prefijo seguido de un carácter comodín (*). El enfoque de prefijo simple es menos riguroso que una lista discreta de valores, pero requiere menos mantenimiento.

Los siguientes ejemplos muestran cómo definir una política de etiquetado para validar los valores que son aceptables para una clave determinada. Partiendo de la definición tabular del esquema sencilla, puede transcribir esta información en una o más políticas de etiquetas. Se pueden usar políticas independientes para respaldar la propiedad delegada o es posible que algunas políticas solo se apliquen en escenarios específicos.

ExampleInc-CostAllocation.json

A continuación, se muestra un ejemplo de una política de etiquetas que informa sobre las etiquetas de asignación de costos:

```
{
  "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-*"
        ]
      }
    }
  }
}
```

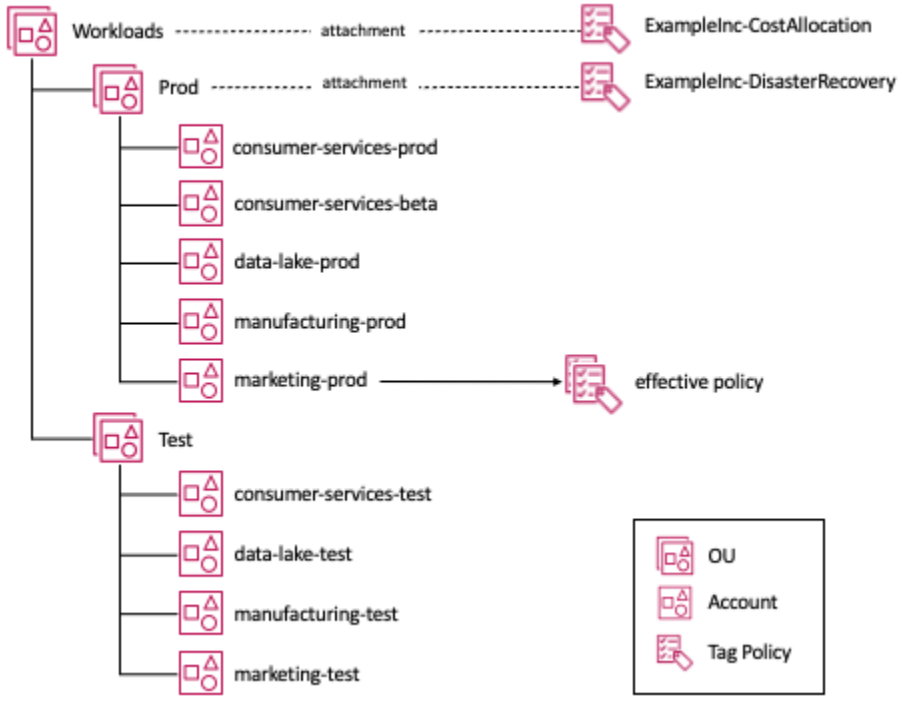
ExampleInc-DisasterRecovery.json

A continuación, se muestra un ejemplo de una política de etiquetas que informa sobre las etiquetas de recuperación de desastres:

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

```
        }
    }
}
```

En este ejemplo, la política de etiquetas `ExampleInc-CostAllocation` se adjunta a la unidad organizativa `Workloads` y, por lo tanto, se aplica a todas las cuentas de las unidades organizativas secundarias `Prod` y `Test`. Del mismo modo, la política de etiquetas `ExampleInc-DisasterRecovery` se adjunta a la unidad organizativa `Prod` y, por lo tanto, solo se aplica a las cuentas por debajo de esta unidad organizativa. El documento técnico Organización del entorno mediante varias cuentas analiza con más detalle las estructuras de las unidades organizativas recomendadas.



Asociación de las políticas de etiquetas a una estructura de unidad organizativa

Al examinar la cuenta de `marketing-prod` en el diagrama, ambas políticas de etiquetas se aplican a esta cuenta, por lo que tenemos el concepto de una política efectiva, que es la convolución de las políticas de un tipo determinado que se aplican a una cuenta. Si administra los recursos principalmente de forma manual, puede revisar la política vigente consultando Grupos de recursos y editor de etiquetas: políticas de etiquetas en la consola. Si utiliza la infraestructura como código (IaC) o secuencias de comandos para administrar los recursos, puede utilizar la llamada a la API `AWS::Organizations::DescribeEffectivePolicy`.

Implementación y aplicación del etiquetado

En esta sección, le presentaremos las herramientas disponibles para las siguientes estrategias de administración de recursos: manual, infraestructura como código (IaC) e integración continua o entrega continua (CI/CD). La dimensión clave de estos enfoques es una tasa de implementación cada vez más frecuente.

Recursos administrados manualmente

Por lo general, se trata de cargas de trabajo que se encuentran en las etapas básicas o de migración de la adopción. A menudo, se trata de cargas de trabajo simples, en gran parte estáticas, que se han creado mediante procedimientos escritos tradicionales o que se han migrado junto con herramientas como CloudEndure desde un entorno en las instalaciones. Las herramientas de migración, por ejemplo, Migration Hub y CloudEndure, pueden aplicar etiquetas como parte del proceso de migración. Sin embargo, si las etiquetas no se aplicaron durante la migración original o si el esquema de etiquetado ha cambiado desde entonces, el Editor de etiquetas (una característica de la AWS Management Console) le permite buscar recursos mediante diversos criterios de búsqueda y agregar, modificar o eliminar etiquetas de forma masiva. Los criterios de búsqueda pueden incluir recursos con o sin la presencia de una etiqueta o valor en particular. La API de etiquetado de recursos de AWS le permite realizar estas funciones mediante programación.

A medida que se modernizan estas cargas de trabajo, se ingresan tipos de recursos, como los grupos de escalado automático. Estos tipos de recursos permiten una mayor elasticidad y una mejor resiliencia. El grupo de escalado automático administra las instancias de Amazon EC2 en su nombre; sin embargo, es posible que desee etiquetar las instancias EC2 de forma coherente con los recursos creados manualmente. Una plantilla de lanzamiento de Amazon EC2 proporciona los medios para especificar las etiquetas que el escalado automático debe aplicar a las instancias que crea.

Cuando los recursos de una carga de trabajo se administran manualmente, puede resultar útil automatizar el etiquetado de los recursos. Hay varias soluciones disponibles. Un enfoque consiste en utilizar Reglas de AWS Config, que puede comprobar `required_tags` y, a continuación, iniciar una función de Lambda para aplicarlas. Reglas de AWS Config se describe con más detalle más adelante en este documento técnico.

Recursos administrados por la infraestructura como código (IaC)

AWS CloudFormation proporciona un lenguaje común para aprovisionar todos los recursos de infraestructura del entorno de AWS. Las plantillas de CloudFormation son archivos JSON o YAML que crean recursos de AWS de forma automatizada. Cuando crea recursos de AWS que utilizan

plantillas de CloudFormation, puede utilizar la propiedad Etiquetas de recursos de CloudFormation para aplicar etiquetas a los tipos de recursos compatibles al crearlos. Administrar las etiquetas y los recursos con IaC ayuda a garantizar la coherencia.

Cuando AWS CloudFormation crea los recursos, el servicio aplica automáticamente un conjunto de etiquetas definidas por AWS a los recursos creados por la plantilla de AWS CloudFormation. Estos son:

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

Puede definir fácilmente un grupo de recursos en función de la pila de AWS CloudFormation. Estas etiquetas definidas por AWS las heredan los recursos creados por la pila. Sin embargo, para las instancias de Amazon EC2 dentro de un grupo de escalado automático, `AWS::AutoScaling::AutoScalingGroup TagProperty` se debe establecer en la definición del grupo de escalado automático de la plantilla de AWS CloudFormation. Alternativamente, si utiliza una Plantilla de lanzamiento de EC2 con el grupo de escalado automático, puede definir las etiquetas en su definición. Se recomienda el uso de plantillas de lanzamiento de EC2 con grupos de escalado automático o con un servicio de contenedores de AWS. Estos servicios pueden ayudar a garantizar un etiquetado coherente de las instancias de Amazon EC2 y también son compatibles con el escalado automático entre varios tipos de instancias y opciones de compra, que pueden mejorar la resiliencia y optimizar los costos informáticos.

Los enlaces de AWS CloudFormation proporcionan a los desarrolladores un medio para mantener la coherencia de los aspectos clave de la aplicación con los estándares de la organización. Los enlaces se pueden configurar para proporcionar un aviso o impedir la implementación. Esta característica es la más adecuada para comprobar los elementos de configuración clave de las plantillas, por ejemplo, si un grupo de escalado automático está configurado para aplicar etiquetas definidas por el cliente a todas las instancias de Amazon EC2 que vaya a lanzar o para garantizar que todos los buckets de Amazon S3 se creen con la configuración de cifrado requerida. En ambos casos, la evaluación de este cumplimiento se está aplazando hasta una fase temprana del proceso de implementación con enlaces de AWS CloudFormation antes de la implementación.

AWS CloudFormation proporciona la capacidad de detectar cuándo un recurso (consulte Recursos que respaldan la detección de desviaciones) aprovisionado a partir de una plantilla se ha modificado y los recursos ya no coinciden con las configuraciones de plantilla esperadas. Esto se conoce como desviación. Si utiliza la automatización para aplicar etiquetas a los recursos administrados a través

de IaC, los está modificando e ingresando una desviación. Al utilizar IaC, actualmente se recomienda administrar cualquier requisito de etiquetado como parte de las plantillas de IaC, implementar los enlaces de AWS CloudFormation y publicar los conjuntos de reglas de AWS CloudFormation Guard que puede utilizar la automatización.

Recursos administrados por canalización de CI/CD

A medida que aumenta la madurez de una carga de trabajo, es probable que se adopten técnicas como la integración y la implementación continuas (CI/CD). Estas técnicas ayudan a reducir el riesgo de implementación al facilitar la implementación de pequeños cambios con mayor frecuencia y, al mismo tiempo, aumentar la automatización de las pruebas. Una estrategia de observabilidad que detecta un comportamiento inesperado ingresado por una implementación puede revertirla automáticamente con un impacto mínimo en los usuarios. Al llegar a la fase de implementación decenas de veces al día, aplicar etiquetas retroactivamente ya no es práctico. Todo se debe expresar como código o configuración, controlar las versiones y, siempre que sea posible, probarse y evaluarse antes de implementarlo en producción. En el modelo de desarrollo y operaciones (DevOps) combinado, muchas de las prácticas abordan las consideraciones operativas en forma de código y las validan al principio del ciclo de vida de la implementación.

Lo ideal sería realizar estas comprobaciones lo antes posible en el proceso (como se muestra con los enlaces de AWS CloudFormation), para que pueda estar seguro de que la plantilla de AWS CloudFormation cumple con las políticas antes de que salga de la máquina para desarrolladores.

AWS CloudFormation Guard 2.0 proporciona los medios para redactar reglas de cumplimiento preventivo para todo lo que pueda definir con CloudFormation. La plantilla se valida según las reglas del entorno de desarrollo. Evidentemente, esta característica tiene una amplia gama de aplicaciones, pero en este documento técnico solo veremos algunos ejemplos que garantizarían que `AWS::AutoScaling::AutoScalingGroup TagProperty` se utilice siempre.

A continuación, se muestra un ejemplo de una regla de CloudFormation Guard:

```
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'>>
    }
}
```

En el ejemplo de código, filtramos la plantilla para todos los recursos que son del tipo `AutoScalingGroup` y, a continuación, tenemos dos reglas:

- **`tags_asg_automation_EnvironmentId`**: comprueba que existe una etiqueta con esta clave, que tiene un valor dentro de la lista de valores permitidos y que `PropagateAtLaunch` se establece en `true`
- **`tags_asg_costAllocation_CostCenter`**: comprueba que existe una etiqueta con esta clave, que tiene un valor que comienza con el valor de prefijo definido y que `PropagateAtLaunch` se establece en `true`

Cumplimiento

Como se ha descrito anteriormente, el editor de grupos de recursos y etiquetas proporciona los medios para identificar los casos en los que los recursos no cumplen con los requisitos de etiquetado definidos en las políticas de etiquetado que se aplican a las unidades organizativas de la organización. Al acceder a la herramienta de la consola editor de grupos de recursos y etiquetas desde la cuenta de un miembro de la organización, se muestran las políticas que se aplican a esa cuenta y el recurso de la cuenta que no cumple los requisitos de la política de etiquetas. Si se accede desde la cuenta de administración (y si Políticas de etiquetas tiene el Acceso habilitado en los servicios de AWS Organizations), entonces es posible ver el cumplimiento de la política de etiquetas para todas las cuentas vinculadas de la organización.

Dentro de la propia Política de etiquetas, puede habilitar la aplicación para tipos de recursos específicos. En el siguiente ejemplo de política, hemos agregado la aplicación de manera que todos

los tipos de recursos `ec2:instance` y `ec2:volume` deben cumplir con la política. Existen algunas limitaciones conocidas, como que debe haber una etiqueta en un recurso para que la política de etiquetas la evalúe. Consulte Recursos que respaldan la aplicación con políticas de etiquetas para obtener una lista.

ExampleInc-Cost-Allocation.json

A continuación, se muestra un ejemplo de una política de etiquetas que informa o aplica las etiquetas de asignación de costos:

```
{
  "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 Config es un servicio que le permite evaluar y auditar las configuraciones de los recursos de AWS (consulte Tipos de recursos compatibles con AWS Config). En el caso del etiquetado, podemos usarlo para identificar los recursos que carecen de etiquetas con claves específicas, con la regla `required_tags` (consulte Tipos de recursos compatibles con required_tags). En el ejemplo anterior, podríamos comprobar la existencia de la clave en todas las instancias de Amazon EC2. En los casos en los que la clave no exista, la instancia se registrará como no compatible. Esta plantilla de AWS CloudFormation describe una regla de AWS Config para comprobar la presencia de las claves obligatorias descritas en la tabla, en los buckets de Amazon S3, las instancias de Amazon EC2 y los volúmenes de Amazon EBS.

```
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
```

Para los entornos en los que los recursos se administran manualmente, una regla de AWS Config se puede mejorar para agregar automáticamente la clave de etiqueta que falta a los recursos mediante una corrección automática a través de una función de AWS Lambda. Aunque esto funciona bien para las cargas de trabajo estáticas, es cada vez menos eficaz a medida que se empiezan a administrar los recursos mediante IaC y canalizaciones de implementación.

AWS Organizations: las políticas de control de servicio (SCP) son un tipo de política de organización que puede utilizar para administrar permisos en la organización. Las políticas de control de servicios (SCP) ofrecen un control central sobre los máximos permisos disponibles para todas las cuentas de la organización o unidad organizativa (OU). Las SCP solo afectan a los usuarios y roles administrados por cuentas que forman parte de la organización. Aunque no afectan directamente a los recursos, restringen los permisos de los usuarios y los roles, lo que incluye los permisos para etiquetar las acciones. Con respecto al etiquetado, las SCP pueden proporcionar detalles adicionales a la hora de aplicar el etiquetado, además de lo que pueden ofrecer las políticas de etiquetado.

En el siguiente ejemplo, la política denegará solicitudes `ec2:RunInstances` donde la etiqueta `example-inc:cost-allocation:CostCenter` no está presente.

A continuación, se muestra una SCP de denegación:

```
{
  "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"
        }
      }
    }
  ]
}
```

Por diseño, no es posible recuperar la política de control de servicios efectiva que se aplica a una cuenta enlazada. Cuando se impone el etiquetado con las SCP, la documentación debe estar disponible para que los desarrolladores puedan garantizar que los recursos cumplen con las políticas que se han aplicado a las cuentas. Proporcionar acceso de solo lectura a los eventos de CloudTrail de la cuenta puede ayudar a los desarrolladores a realizar tareas de depuración cuando los recursos no cumplen con los requisitos.

Medir la eficacia del etiquetado e impulsar mejoras

Una vez implementada una estrategia de etiquetado, es importante medir su eficacia en función de los casos de uso objetivo. La medida de la eficacia variará según el caso de uso. Por ejemplo:

- Atribución de costos: puede medir la cobertura de etiquetado de los recursos en función del gasto con herramientas como AWS Cost Explorer o informe de costo y uso de AWS. Por ejemplo, podría realizar un seguimiento del porcentaje de recursos etiquetados o no etiquetados que generan cargos, en particular el monitoreo de claves de etiquetas específicas.
- Automatización: es posible que desee auditar si se ha logrado el resultado deseado. Por ejemplo, si las instancias de Amazon EC2 que no están en producción se suspenden fuera del horario laboral o auditar las horas de inicio y finalización de las instancias.

Editor de grupos de recursos y etiquetas dentro de la cuenta de administración, ofrece funciones adicionales para analizar el cumplimiento de la política de etiquetas en todas las cuentas enlazadas de la organización.

En función de los resultados de la medición de la eficacia del etiquetado, identifique si es necesaria alguna mejora o modificación en alguno de los pasos, como la definición de los casos de uso, la implementación o el cumplimiento del esquema de etiquetado. Realice los cambios necesarios y

repita el ciclo hasta lograr la eficacia deseada. En el ejemplo de la atribución de costos, puede ver el porcentaje de mejora.

Dado que son los desarrolladores y los operadores los que tienen que etiquetar los recursos propiamente dichos, es fundamental que se hagan cargo de ellos. Esta no es la única responsabilidad adicional que suelen asumir los equipos a lo largo de su trayectoria de adopción de AWS. También es importante aumentar la responsabilidad por la seguridad y el costo de desarrollar la aplicación y su funcionamiento. Las organizaciones suelen utilizar los objetivos y metas como medio para motivar la adopción de nuevas prácticas, por lo que esto también se puede aplicar en este caso.

Etiquetado de casos de uso

Temas

- Etiquetas para la asignación de costos y la administración financiera
- Etiquetas para operaciones y ayuda
- Etiquetas para la seguridad de los datos, la administración de riesgos y el control de acceso

Etiquetas para la asignación de costos y la administración financiera

Uno de los primeros casos de uso del etiquetado que suelen abordar las organizaciones es la visibilidad y la administración de los costos y el uso. Por lo general, esto se debe a varios motivos:

- Normalmente, es un escenario bien entendido y los requisitos son bien conocidos. Por ejemplo, los equipos financieros desean ver el costo total de las cargas de trabajo y la infraestructura que abarcan varios servicios, características, cuentas o equipos. Una forma de lograr esta visibilidad de los costos es mediante un etiquetado coherente de los recursos.
- Las etiquetas y sus valores están claramente definidos. Por lo general, los mecanismos de asignación de costos ya existen en los sistemas financieros de una organización, por ejemplo, el seguimiento por centro de costos, unidad de negocio, equipo o función de la organización.
- Retorno de la inversión rápido y demostrable. Es posible realizar un seguimiento de las tendencias de optimización de costos a lo largo del tiempo si los recursos se etiquetan de forma coherente, por ejemplo, si los recursos tienen el tamaño correcto, se escalan automáticamente o se programan.

Entender cómo se incurre en los costos en AWS le permite tomar decisiones financieras informadas. Saber dónde se han generado costos a nivel de recursos, carga de trabajo, equipo u organización mejora la comprensión del valor ofrecido en el nivel correspondiente en comparación con los resultados empresariales logrados.

Es posible que los equipos de ingeniería no tengan experiencia en la administración financiera de los recursos. Adjuntar a una persona con una destreza especializada en administración financiera de AWS que pueda entrenar a los equipos de ingeniería y desarrollo sobre los conceptos básicos de la administración financiera de AWS y la creación de una relación entre las finanzas y la ingeniería para

fomentar la cultura de FinOps ayudará a lograr resultados mensurables para la empresa y alentarán a los equipos a construir teniendo en cuenta los costos. El establecimiento de prácticas financieras recomendadas se analiza en profundidad en Pilar de optimización de costos del Marco de Buena Arquitectura, pero abordaremos algunos de los principios fundamentales en este documento técnico.

Etiquetas de asignación de costos

La asignación de costos se refiere a la asignación o distribución de los costos generados a los usuarios o beneficiarios de esos costos siguiendo un proceso definido. En el contexto de este documento técnico, dividimos la asignación de costos en dos tipos: análisis y reintegro.

Las herramientas y los mecanismos de análisis ayudan a aumentar el conocimiento de los costos. El reintegro contribuye a la recuperación de los costos e impulsa el conocimiento de los costos. El análisis trata de la presentación, el cálculo y los informes de los cargos que ha generado una entidad específica, como una unidad de negocio, una aplicación, un usuario o un centro de costos. Por ejemplo: “El equipo de ingeniería de infraestructuras fue responsable de una inversión de X $ de AWS el mes pasado”. El reintegro se refiere al cargo real de los costos generados a esas entidades a través de los procesos contables internos de una organización, como los sistemas financieros o los comprobantes diarios. Por ejemplo: “Se dedujeron X $ del presupuesto de AWS para el equipo de ingeniería de infraestructuras”. En ambos casos, el etiquetado de los recursos adecuadamente puede ayudar a asignar el costo a una entidad, con la única diferencia de si se espera que alguien realice un pago o no.

Es posible que el gobierno financiero de la organización requiera una contabilidad transparente de los costos generados a nivel de aplicación, unidad de negocio, centro de costos y equipo. Realizar la atribución de costos con el apoyo de las Etiquetas de asignación de costos le proporciona los datos necesarios para atribuir con precisión los costos generados por una entidad a partir de los recursos debidamente etiquetados.

- Responsabilidad: asegúrese de que el costo se asigne a quienes son responsables del uso de los recursos. Un único punto de servicio o grupo puede ser responsable de la revisión y la elaboración de informes sobre los gastos.
- Transparencia financiera: muestre una visión clara de las asignaciones en efectivo a TI mediante la creación de paneles eficaces y un análisis de costos significativo para el liderazgo.
- Inversiones informadas de TI: realice un seguimiento del ROI en función del proyecto, la aplicación o la línea de negocio y permita a los equipos tomar mejores decisiones empresariales, por ejemplo, destinando más fondos a las aplicaciones que generan ingresos.

En resumen, las etiquetas de asignación de costos pueden ayudarle a saber:

- ¿Quién es el propietario del gasto y quién es responsable de optimizarlo?
- ¿En qué carga de trabajo, aplicación o producto se está gastando? ¿Qué entorno o etapa?
- ¿Qué áreas de gasto están creciendo más rápido?
- ¿Cuánto gasto se puede deducir de un presupuesto de AWS basado en tendencias del pasado?
- ¿Cuál fue el impacto de los esfuerzos de optimización de costos en determinadas cargas de trabajo, aplicaciones o productos?

La activación de las etiquetas de recursos para la asignación de costos ayuda a definir prácticas de medición dentro de la organización que se pueden utilizar para proporcionar visibilidad de uso de AWS que aumenta la transparencia en la rendición de cuentas por el gasto. También se centra en crear un nivel adecuado de detalle con respecto a la visibilidad de los costos y el uso, y en influir en los comportamientos de consumo de la nube mediante la elaboración de informes de asignación de costos y el seguimiento de los KPI.

Elaboración de una estrategia de asignación de costos

Definición e implementación de un modelo de asignación de costos

Cree una estructura de cuenta y de costos para los recursos que se van a implementar en AWS. Establezca la relación entre los costos de gasto de AWS, cómo se generaron esos costos y quién o qué generó esos costos. Las estructuras de costos comunes se basan en AWS Organizations, Cuentas de AWS, entornos y entidades dentro de las organizaciones, como una línea de negocio o una carga de trabajo. Las estructuras de costos se pueden basar en múltiples atributos para permitir el examen de los costos de diferentes maneras o con diferentes niveles de granularidad, por ejemplo, acumulando los costos de las cargas de trabajo individuales en la línea de negocio a la que prestan servicio.

Al elegir una estructura de costos que se alinea con los resultados deseados, evalúe los mecanismos de asignación de costos en la facilidad de implementación frente a la precisión deseada. Es posible que esto incluya consideraciones relacionadas con la responsabilidad, la disponibilidad de herramientas y los cambios culturales. Tres modelos populares de asignación de costos de los que los clientes de AWS suelen partir:

- Basado en cuentas: este modelo es el que requiere el menor esfuerzo y proporciona una alta precisión en cuanto a análisis y reintegros, y es adecuado para organizaciones que tienen una

estructura contable definida (y es coherente con las recomendaciones del documento técnico Organización del entorno de AWS con varias cuentas). Esto proporciona una visibilidad clara de los costos por cuenta. Para la visibilidad y la asignación de los costos, puede utilizar AWS Cost Explorer, informes de costos y uso, así como presupuestos de AWS para el monitoreo y el seguimiento de los costos. Estas herramientas ofrecen opciones de filtrado y agrupación por Cuentas de AWS. Desde el punto de vista de la asignación de costos, este modelo no tiene por qué basarse en un etiquetado preciso de los recursos individuales.

- Basado en unidades de negocio o equipos: el costo se puede asignar a los equipos, unidades de negocio u organizaciones de una empresa. Este modelo requiere un esfuerzo moderado, proporciona una alta precisión en cuanto a análisis y reintegros y es adecuado para organizaciones que tienen una estructura contable definida (por lo general, con AWS Organizations), con separación entre varios equipos, aplicaciones y tipos de carga de trabajo. Esto proporciona una visibilidad clara de los costos entre los equipos y las aplicaciones y, como beneficio adicional, reduce el riesgo de que se produzcan AWS Service Quotas dentro de una sola Cuenta de AWS. Por ejemplo, cada equipo puede tener cinco cuentas (`prod`, `staging`, `test`, `dev`, `sandbox`) y no habrá dos equipos y aplicaciones que compartan la misma cuenta. Con esa estructura Categorías de costos de AWS a continuación, proporcionará la funcionalidad de agrupar cuentas u otras etiquetas (“metaetiquetado”) en categorías, de las que se podrá hacer un seguimiento con las herramientas mencionadas en el ejemplo anterior. Es importante tener en cuenta que AWS Organizations permite etiquetar cuentas y unidades organizativas (OU); sin embargo, estas etiquetas no se aplicarán a los informes de asignación de costos y facturación (es decir, no puede agrupar ni filtrar los costos en AWS Cost Explorer por unidad organizativa). AWS Las categorías de costos se deben usar para este propósito.
- Basado en etiquetas: este modelo requiere más esfuerzo en comparación con los dos anteriores y proporcionará una alta precisión en los análisis y reintegros, según los requisitos y el objetivo final. Aunque le recomendamos encarecidamente que adopte las prácticas descritas en el documento técnico Organización del entorno de AWS con varias cuentas, siendo realistas, los clientes suelen encontrarse con estructuras de cuentas mixtas y complejas que requieren tiempo para migrar. En este escenario, la clave es implementar una estrategia de etiquetado rigurosa y eficaz, seguida de activar las etiquetas relevantes para la asignación de costos en la consola de administración de facturación y costos (en AWS Organizations, las etiquetas se pueden activar para la asignación de costos solo desde la cuenta de administración del pagador). Una vez activadas las etiquetas para la asignación de costos, se pueden utilizar las herramientas de visibilidad y asignación de costos que se mencionaron en los métodos anteriores para los análisis y los reintegros. Tenga en cuenta que las etiquetas de asignación de costos no son retrospectivas y solo aparecerán en las

herramientas de informes de facturación y seguimiento de costos una vez que se hayan activado para la asignación de costos.

En resumen, si necesita realizar un seguimiento de los costos por unidad de negocio, puede utilizar Categorías de costos de AWS para agrupar las cuentas enlazadas dentro de la organización de AWS en consecuencia y consultar esta agrupación en los informes de facturación. Al crear cuentas independientes para los entornos de producción y que no sean de producción, también puede filtrar los costos relacionados con los entornos en herramientas como AWS Cost Explorer o realizar un seguimiento de esos costos mediante AWS Budgets. Por último, si el caso de uso requiere un seguimiento de los costos más detallado, por ejemplo, mediante cargas de trabajo o aplicaciones individuales, puede etiquetar los recursos de esas cuentas en consecuencia, activar esas claves de etiquetas para la asignación de costos en la cuenta de administración y, a continuación, filtrar ese costo por claves de etiquetas en las herramientas de informes de facturación.

Establecimiento de los procesos de informes y monitoreo de costos

Comience por identificar los tipos de costos que son importantes para las partes interesadas internas (por ejemplo, el gasto diario, el costo por cuenta, el costo por X, los costos amortizados). De este modo, podrá mitigar los riesgos presupuestarios asociados a los gastos inesperados o anómalos más rápido que esperar a la factura de AWS finalizada. Las etiquetas proporcionan la atribución que permite estos escenarios de informes. La información obtenida a partir de los informes puede servir de base para las acciones a fin de mitigar el impacto de los gastos anómalos e inesperados en los presupuestos financieros. Cuando se produce un aumento inesperado de los costos, es importante evaluar si se ha producido un aumento imprevisto en el valor entregado para poder determinar si es necesario tomar medidas y qué medidas son necesarias.

Al desarrollar una estrategia de etiquetado para respaldar la asignación de costos, tenga en cuenta los siguientes elementos:

- AWS Organizations: la asignación de costos en varias cuentas se puede realizar por cuenta, grupo de cuentas o grupo de etiquetas creadas para los recursos de esas cuentas. Las etiquetas creadas para los recursos que residen en cuentas individuales en AWS Organizations solo se pueden usar para la asignación de costos desde la cuenta de administración.
- Cuenta de AWS: la asignación de costos dentro de una Cuenta de AWS se puede realizar mediante dimensiones adicionales, como servicios o regiones. Es posible etiquetar aún más los recursos de una cuenta y trabajar con los grupos de dichas etiquetas de recursos.

- Etiquetas de asignación de costos: las etiquetas creadas por el usuario y las etiquetas generadas por AWS se pueden activar para la asignación de costos, si es necesario. La habilitación de las etiquetas para la asignación de costos en la consola de facturación (de la cuenta de administración en AWS Organizations) ayuda con los análisis y los reintegros.
- Categorías de costos: las categorías de costos de AWS permiten agrupar cuentas y agrupar etiquetas ("metaetiquetado") dentro de una organización de AWS, que además brinda la capacidad de analizar los costos relacionados con estas categorías a través de herramientas como AWS Cost Explorer, presupuestos de AWS e informes de costo y uso de AWS.

Realización de análisis y reintegros para las unidades de negocio, los equipos u organizaciones de la empresa

Atribuya los costos mediante el proceso de asignación de costos respaldado por la estructura de costos y las etiquetas de asignación de costos. Las etiquetas se pueden utilizar para proporcionar análisis a los equipos que no son directamente responsables de pagar los costos, pero que son responsables de haberlos generado. Este enfoque permite conocer la contribución al gasto y la forma en que se incurre en esos costos. Realice el reintegro a los equipos directamente responsables de los costos para recuperar el gasto de los recursos que han consumido y darles a conocer esos costos y la forma en que se han producido.

Medición y circulación de los KPI de eficacia o valor

Acuerde un conjunto de métricas de costo unitario o KPI para medir el impacto de las inversiones de administración financiera en la nube. Este ejercicio crea un lenguaje común entre las partes interesadas en la tecnología y la empresa, y cuenta una historia basada en la eficacia, en lugar de una historia centrada solo en el gasto agregado absoluto. Para obtener información adicional, consulte este blog que habla de cómo las métricas unitarias pueden ayudar a crear una alineación entre las funciones empresariales.

Asignación de gastos no asignables

En función de las prácticas contables de la organización, es posible que los diferentes tipos de cargos requieran un tratamiento diferente. Identifique las categorías de recursos o costos que no se pueden etiquetar. En función de los servicios utilizados y de los que se planifique utilizar, acuerde los mecanismos sobre cómo tratar y medir ese gasto no asignable. Por ejemplo, consulte la lista de recursos admitidos por el Editor de etiquetas y AWS Resource Groups en la Guía del usuario de etiquetas y AWS Resource Groups.

Un ejemplo habitual de categoría de costos que no se puede etiquetar son las tarifas de los descuentos por compromiso, como las instancias reservadas (RI) y los Savings Plans (SP). Aunque las tarifas de suscripción y las tarifas de SP y RI no utilizados no se pueden etiquetar antes de que aparezcan en las herramientas de informes de facturación, puede realizar un seguimiento de cómo se aplican los descuentos de RI y SP a las cuentas, los recursos y las etiquetas en AWS Organizations después de los hechos. Por ejemplo, en AWS Cost Explorer es posible analizar el costo amortizado, agrupar ese gasto por las claves de etiquetas correspondientes y aplicar filtros adecuados al caso de uso. En informe de uso y costo (CUR) de AWS, puede filtrar las líneas que correspondan al uso cubierto por los descuentos de RI y SP (encontrará más información en la sección de casos de uso de la Documentación de CUR) y seleccionar las columnas que solo sean relevantes para usted. Cada clave de etiqueta activada para la asignación de costos se presentará en una columna independiente al final del informe CUR, de forma similar a como se presenta en otros informes de facturación tradicionales, como el informe mensual de asignación de costos. Para obtener más información, consulte los Laboratorios de Buena Arquitectura de AWS para ver ejemplos de cómo obtener información sobre costos y uso a partir de los datos del CUR.

Informes

Además de las herramientas de AWS disponibles para ayudarle con los análisis y reintegros, hay una variedad de otras soluciones creadas por AWS y de terceros que pueden ayudar a monitorear el costo de los recursos etiquetados y medir la eficacia de la estrategia de etiquetado. En función de los requisitos y el objetivo final de la organización, se puede invertir tiempo y recursos en la creación de soluciones personalizadas o adquirir las herramientas proporcionadas por uno de los Socios con competencias en herramientas de administración de Nube de AWS. Si decide crear su propia herramienta de asignación de costos de fuente única de verdad con parámetros controlados relevantes para el negocio, el informe de uso y costo de AWS (CUR) proporciona los datos más detallados sobre costos y uso y permite crear paneles de optimización personalizados, que permiten filtrar y agrupar por cuentas, servicios, categorías de costos, etiquetas de asignación de costos y muchas otras dimensiones. Entre las soluciones basadas en CUR desarrolladas por AWS que se pueden utilizar como una de estas herramientas, compruebe Paneles de inteligencia en la nube en el sitio web de Laboratorios de Buena Arquitectura de AWS.

Etiquetas para operaciones y ayuda

Un entorno de AWS tendrá varias cuentas, recursos y cargas de trabajo con diferentes requisitos operativos. Las etiquetas se pueden usar para proporcionar contexto y orientación para ayudar a los equipos de operaciones a mejorar la administración de los servicios. Las etiquetas también

se pueden utilizar para proporcionar transparencia en la gobernanza operativa de los recursos administrados.

Algunos de los principales factores que impulsan una definición coherente de las etiquetas operativas son:

- Filtrar los recursos durante las actividades de infraestructura automatizadas. Por ejemplo, al implementar, actualizar o eliminar recursos. Otro es el escalado de los recursos para optimizar los costos y reducir el uso fuera del horario laboral. Consulte la solución del programador de instancias de AWS para un ejemplo práctico.
- Identificar recursos aislados u obsoletos. Los recursos que hayan sobrepasado su vida útil definida o que se hayan señalado por mecanismos internos para su aislamiento deberían estar debidamente etiquetados para ayudar al personal de apoyo en su investigación. Los recursos obsoletos se deben etiquetar antes de aislarlos, archivarlos y eliminarlos.
- Requisitos de soporte para un grupo de recursos. Los recursos suelen tener requisitos de soporte diferentes; por ejemplo, estos requisitos se podrían negociar entre equipos o establecerse como parte de la importancia crítica de una aplicación. Puede encontrar más información sobre los modelos operativos en el Pilar de excelencia operativa.
- Mejore el proceso de administración de incidentes. Al etiquetar los recursos con etiquetas que ofrezcan una mayor transparencia en el proceso de administración de incidentes, los equipos de soporte e ingenieros, así como los equipos de administración de incidentes graves (MIM), pueden administrar los eventos de forma más eficaz.
- Copias de seguridad. Las etiquetas también se pueden usar para identificar la frecuencia con la que se deben hacer copias de seguridad de los recursos y dónde deben ir las copias de seguridad o dónde restaurarlas. Guía prescriptiva sobre los enfoques de copia de seguridad y recuperación en AWS.
- Aplicación de parches. Aplicar parches a las instancias mutables que se ejecutan en AWS es crucial para la estrategia general de aplicación de parches y para aplicar parches a las vulnerabilidades de día cero. Puede encontrar información más detallada sobre la estrategia más amplia de aplicación de parches en la orientación prescriptiva. En este blog se analiza la aplicación de parches a las vulnerabilidades de día cero.
- Observabilidad operativa. Tener una estrategia de KPI operativa traducida en etiquetas de recursos ayudará a los equipos de operaciones a realizar un mejor seguimiento del cumplimiento de los objetivos para mejorar los requisitos empresariales. El desarrollo de una estrategia de KPI es un tema independiente, pero suele centrarse en una empresa que opera de forma estable o en dónde medir el impacto y los resultados del cambio. El Panel de KPI (Laboratorios de

Buena Arquitectura de AWS) y el taller de KPI de operaciones (un servicio proactivo de AWS Enterprise Support) abordan la medición del rendimiento en un estado estable. El artículo del blog de estrategia empresarial de AWS Medir el éxito de la transformación, analiza la medición de los KPI para un programa de transformación, como la modernización de TI o la migración de en las instalaciones a AWS.

Actividades de infraestructura automatizadas

Las etiquetas se pueden utilizar en una amplia gama de actividades de automatización al administrar la infraestructura. El uso de AWS Systems Manager, por ejemplo, le permitirá administrar las automatizaciones y los manuales de procedimientos en los recursos especificados por el par clave-valor definido que cree. En el caso de los nodos administrados, puede definir un conjunto de etiquetas para rastrear o dirigir los nodos por sistema operativo y entorno. A continuación, puede ejecutar un script de actualización para todos los nodos de un grupo o revisar el estado de esos nodos. Los recursos de Systems Manager también se pueden etiquetar para refinar y rastrear aún más las actividades automatizadas.

La automatización del ciclo de vida de inicio y finalización de los recursos del entorno puede proporcionar una reducción de costos significativa para cualquier organización. El programador de instancias en AWS es un ejemplo de solución que puede iniciar y detener instancias de Amazon EC2 y Amazon RDS cuando no son necesarias. Por ejemplo, los entornos de desarrolladores que utilizan instancias de Amazon EC2 o Amazon RDS que no tienen que funcionar los fines de semana no aprovechan el potencial de ahorro de costos que puede ofrecer el apagado de esas instancias. Al analizar las necesidades de los equipos y los entornos y etiquetar adecuadamente estos recursos para automatizar su administración, podrá utilizar el presupuesto de forma eficaz.

Un ejemplo de etiqueta de programación utilizada por el programador de instancias en una instancia de Amazon EC2:

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

Ciclo de vida de la carga de trabajo

Revise la precisión de los datos operativos de soporte. Asegúrese de que se realicen revisiones periódicas de las etiquetas asociadas al ciclo de vida de la carga de trabajo y de que las partes interesadas correspondientes participen en estas revisiones.

Tabla 7: Revise las etiquetas operativas como parte del ciclo de vida de la carga de trabajo

Caso de uso	Clave de etiqueta	Justificación	Valores de ejemplo
Propietario de la cuenta	`example-inc:account-owner:owner`	El propietario de la cuenta y los recursos que contiene.	`ops-center` , `dev-ops`, `app-team`
Revisión de propietario de cuenta	`example-inc:account-owner:review`	Compruebe si los detalles de propiedad de la cuenta están actualizados y son correctos.	<revisar la fecha en el formato correcto definido en la biblioteca de etiquetado>
Propietario de los datos	`example-inc:data-owner:owner`	El propietario de los datos de las cuentas en las que residen los datos.	`bi-team`, `logistics` , `security`
Revisión del propietario de los datos	`example-inc:data-owner:review`	Revise si los detalles de propiedad de los datos están actualizados y son correctos.	<revisar la fecha en el formato correcto definido en la biblioteca de etiquetado>

Asignación de etiquetas a las cuentas suspendidas antes de migrar a la unidad organizativa suspendida

Antes de suspender una cuenta y pasar a la unidad organizativa suspendida, tal y como se detalla en el documento técnico de Organización del entorno de AWS con varias cuentas, se deben agregar etiquetas a la cuenta para facilitar el seguimiento interno y la auditoría del ciclo de vida de una cuenta. Por ejemplo, una URL relativa o una referencia de ticket en un sistema de emisión de tickets ITSM de una organización, que muestre el registro de auditoría de una solicitud suspendida.

Tabla 8: Agregar etiquetas operativas cuando el ciclo de vida de la carga de trabajo ingrese en una nueva etapa

Caso de uso	Clave de etiqueta	Justificación	Valores de ejemplo
Propietario de la cuenta	`example-inc:account-owner:owner`	El propietario de la cuenta y los recursos que contiene.	`ops-center` , `dev-ops`, `app-team`
Propietario de los datos	`example-inc:data-owner:owner`	El propietario de los datos de las cuentas en las que residen los datos.	`bi-team`, `logistics` , `security`
Fecha de suspensión	`example-inc:suspension:date`	La fecha en que se suspendió la cuenta	<la fecha suspendida en el formato correcto definido en la biblioteca de etiquetado>
Aprobación para suspensión	`example-inc:suspension:approval`	El enlace a la aprobación de la suspensión de la cuenta	`workload/deprecation`

Administración de incidentes

Las etiquetas pueden desempeñar un papel fundamental en todas las fases de la administración de incidentes, desde el registro, la priorización, la investigación, la comunicación y la resolución de los incidentes hasta su cierre.

Las etiquetas pueden detallar dónde se debe registrar un incidente, el equipo o los equipos a los que se debe informar del incidente y la prioridad de escalamiento definida. Es importante recordar que las etiquetas no están cifradas, así que tenga en cuenta la información que almacena en ellas. Además, en las organizaciones, los equipos y las estructuras jerárquicas, las responsabilidades cambian, así que considere la posibilidad de almacenar un enlace a un portal seguro donde esta información se pueda administrar de forma más eficaz. No es necesario que estas etiquetas sean exclusivas. Por ejemplo, el ID de la aplicación se podría usar para buscar las rutas de escalamiento en un portal de

administración de servicios de TI. Asegúrese de que en las definiciones operativas quede claro que esta etiqueta se utiliza para varios fines.

Las etiquetas de requisitos operativos también se pueden detallar para ayudar a los mánager de incidentes y al personal de operaciones a refinar aún más los objetivos en respuesta a un incidente o evento.

Se pueden incluir enlaces relativos (a la URL de la base del sistema de conocimiento) para manuales de procedimientos y cuadernos de trabajo como etiquetas para ayudar a los equipos que respondieron a identificar el proceso, el procedimiento y la documentación correspondientes.

Tabla 9: Utilice etiquetas operativas para informar sobre la administración de incidentes

Caso de uso	Clave de etiqueta	Justificación	Valores de ejemplo
Administración de incidentes	`example-inc:incident-management:escalationlog`	El sistema que utiliza el equipo de apoyo para registrar los incidentes	`jira`, `servicenow` , `zendesk`
Administración de incidentes	`example-inc:incident-management:escalationpath`	Ruta de escalada	`ops-center` , `dev-ops`, `app-team`
Asignación de costos y administración de incidentes	`example-inc:cost-allocation:CostCenter`	Monitorear los costos por centro de costos. Este es un ejemplo de una etiqueta de doble uso en la que el centro de costos se utiliza como código de aplicación para el registro de incidentes	`123-*`
Programar copias de seguridad	`example-inc:backup:schedule`	Programación de copia de seguridad del recurso	`Daily`

Caso de uso	Clave de etiqueta	Justificación	Valores de ejemplo
Manual/Administración de incidentes	`example-inc:incident-management:playbook`	Manual documentado	`webapp/incident/playbook`

Aplicación de parches

Las organizaciones pueden automatizar la estrategia de aplicación de parches para entornos informáticos mutables y mantener las instancias mutables en línea con la línea de base de revisiones definida para ese entorno de aplicaciones mediante el administrador de parches de AWS Systems Manager y AWS Lambda. Se puede administrar una estrategia de etiquetado para instancias mutables en estos entornos asignando dichas instancias a Grupos de parches y Periodos de mantenimiento. Consulte los siguientes ejemplos para ver una división Dev → Test → Prod. La guía prescriptiva de AWS está disponible para la administración de parches de instancias mutables.

Tabla 10: Las etiquetas operativas pueden ser específicas del entorno

Desarrollo	Staging	Producción
{ "Tags": [{ "Key": "Maintenance Window", "ResourceId": "i-012345678ab9ab111", "ResourceType": "instance", "Value": "cron(30 23 ? * TUE#1 *)" }, { "Key": "Name", "ResourceId": "i-012345678ab9ab222",	{ "Tags": [{ "Key": "Maintenance Window", "ResourceId": "i-012345678ab9ab444", "ResourceType": "instance", "Value": "cron(30 23 ? * TUE#2 *)" }, { "Key": "Name", "ResourceId": "i-012345678ab9ab555",	{ "Tags": [{ "Key": "Maintenance Window", "ResourceId": "i-012345678ab9ab777", "ResourceType": "instance", "Value": "cron(30 23 ? * TUE#3 *)" }, { "Key": "Name", "ResourceId": "i-012345678ab9ab888",

Desarrollo	Staging	Producción
<pre>"ResourceType": "instance", "Value": "WEBAPP" }, { "Key": "Patch Group", "ResourceId": "i-012345678ab9ab333", "ResourceType": "instance", "Value": "WEBAPP-DEV-AL2" }] }</pre>	<pre>"ResourceType": "instance", "Value": "WEBAPP" }, { "Key": "Patch Group", "ResourceId": "i-012345678ab9ab666", "ResourceType": "instance", "Value": "WEBAPP-TEST-AL2" }] }</pre>	<pre>"ResourceType": "instance", "Value": "WEBAPP" }, { "Key": "Patch Group", "ResourceId": "i-012345678ab9ab999", "ResourceType": "instance", "Value": "WEBAPP-PROD-AL2" }] }</pre>

Las vulnerabilidades de día cero también se pueden administrar definiendo etiquetas para complementar la estrategia de aplicación de parches. Consulte Evite las vulnerabilidades de día cero con la aplicación de parches de seguridad el mismo día mediante AWS Systems Manager para obtener una orientación detallada.

Observabilidad operativa

La observabilidad es necesaria para obtener información útil sobre el rendimiento de los entornos y ayudarle a detectar e investigar los problemas. También tiene un propósito secundario que le permite definir y medir los indicadores clave de rendimiento (KPI) y los objetivos de nivel de servicio (SLO), como el tiempo de actividad. Para la mayoría de las organizaciones, los KPI de operaciones importantes son el tiempo medio de detección (MTTD) y el tiempo medio de recuperación (MTTR) de un incidente.

En toda la observabilidad, el contexto es importante, ya que se recopilan los datos y, a continuación, se recopilan las etiquetas asociadas. Independientemente del servicio, la aplicación o el nivel de aplicación en el que se centre, puede filtrar y analizar ese conjunto de datos específico. Las etiquetas se pueden usar para automatizar la incorporación a Alarmas de CloudWatch, de modo que se pueda avisar a los equipos adecuados cuando se superen determinados umbrales de métricas. Por ejemplo, una clave de etiqueta `example-inc:ops:alarm-tag` y el valor podrían indicar

la creación de la alarma de CloudWatch. Una solución que lo demuestra se describe en Utilice etiquetas para crear y mantener las alarmas de Amazon CloudWatch para las instancias de Amazon EC2.

Configurar demasiadas alarmas puede provocar fácilmente una tormenta de alertas, ya que un gran número de alarmas o notificaciones abruman rápidamente a los operadores y reducen su eficacia general, mientras los operadores clasifican y priorizan manualmente las alarmas individuales. Se puede proporcionar un contexto adicional para las alarmas en forma de etiquetas, lo que significa que las reglas se pueden definir en Amazon EventBridge para garantizar que se centre en el problema inicial y no en las dependencias posteriores.

A menudo se pasa por alto el rol de las operaciones junto con DevOps, pero para muchas organizaciones, los equipos de operaciones centrales siguen siendo la primera respuesta fundamental fuera del horario laboral habitual. (Se pueden encontrar más detalles sobre este modelo en el Documento técnico sobre excelencia operativa). A diferencia del equipo de DevOps, que es el responsable de la carga de trabajo, no suelen tener el mismo nivel de conocimiento, por lo que el contexto que proporcionan las etiquetas en los paneles y las alertas puede llevarlos al manual de procedimientos correcto para cada problema o iniciar un manual de procedimientos automatizado (consulte la publicación del blog Automatizar las alarmas de Amazon CloudWatch con AWS Systems Manager).

Etiquetas para la seguridad de los datos, la administración de riesgos y el control de acceso

Las organizaciones tienen diferentes necesidades y obligaciones que cumplir en relación con el manejo adecuado del almacenamiento y el procesamiento de los datos. La clasificación de los datos es una precursora importante para varios casos de uso, como el control de acceso, la retención de datos, el análisis de datos y el cumplimiento.

Seguridad de datos y administración de riesgos

En un entorno de AWS, es probable que tenga cuentas con diferentes requisitos de cumplimiento y seguridad. Por ejemplo, es posible que tenga un entorno aislado para desarrolladores y una cuenta que aloje el entorno de producción para una carga de trabajo altamente regulada, como el procesamiento de pagos. Al aislarlos en diferentes cuentas, puede aplicar distintos controles de seguridad, restringir el acceso a los datos confidenciales y reducir el alcance de la auditoría en el caso de cargas de trabajo reguladas.

La adopción de un estándar único para todas las cargas de trabajo puede generar desafíos. Aunque muchos controles se aplican por igual en todos los entornos, algunos son excesivos o irrelevantes para las cuentas que no necesitan cumplir marcos normativos específicos y para las cuentas en las que nunca habrá datos de identificación personal (por ejemplo, un entorno aislado para desarrolladores o cuentas de desarrollo de cargas de trabajo). Por lo general, esto lleva a resultados de seguridad con falsos positivos que se deben clasificar y cerrar sin tomar ninguna medida, lo que resta esfuerzo a los resultados que se deberían investigar.

Tabla 11: Ejemplos de etiquetas de seguridad de datos y administración de riesgos

Caso de uso	Clave de etiqueta	Justificación	Valores de ejemplo
Administración de incidentes	`example-inc:incident-management:escalationlog`	El sistema que utiliza el equipo de apoyo para registrar los incidentes	`jira`, `servicenow`, `zendesk`
Administración de incidentes	`example-inc:incident-management:escalationpath`	Ruta de escalada	`ops-center`, `dev-ops`, `app-team`
Clasificación de datos	`example-inc:data:classification`	Clasificar los datos para garantizar el cumplimiento y el gobierno	`Public`, `Private`, `Confidential`, `Restricted`
Conformidad de	`example-inc:compliance:framework`	Identifica el marco de cumplimiento al que está sujeta la carga de trabajo	`PCI-DSS`, `HIPAA`

Administrar manualmente los diferentes controles en un entorno de AWS consume tiempo y es propenso a errores. El siguiente paso es automatizar la implementación de los controles de seguridad adecuados y configurar la inspección de los recursos en función de la clasificación de esa cuenta. Al aplicar etiquetas a las cuentas y a los recursos que contienen, la implementación de los controles se puede automatizar y configurar de forma adecuada para la carga de trabajo.

Ejemplo:

Una carga de trabajo incluye un bucket de Amazon S3 con la etiqueta `example-inc:data:classification` con el valor `Private`. La automatización de las herramientas de seguridad implementa la regla de AWS Config `s3-bucket-public-read-prohibited`, que comprueba la configuración del acceso público de bloques del bucket de Amazon S3, la política del bucket y la lista de control de acceso (ACL) del bucket para confirmar que la configuración del bucket es adecuada para la clasificación de datos. Para garantizar que el contenido del bucket sea coherente con la clasificación, Amazon Macie se puede configurar para comprobar la información de identificación personal (PII). El blog Uso de Amazon Macie para validar la clasificación de datos del bucket de S3 explora este patrón con mayor profundidad.

Es posible que determinados entornos regulatorios, como los seguros y la atención médica, estén sujetos a políticas obligatorias de retención de datos. La retención de datos mediante etiquetas, combinada con las políticas de ciclo de vida de Amazon S3, puede ser una forma eficaz y sencilla de determinar las transiciones de objetos a un nivel de almacenamiento diferente. Las reglas del ciclo de vida de Amazon S3 también se pueden utilizar para hacer caducar los objetos para la eliminación de datos una vez transcurrido el periodo de retención obligatorio. Consulte Simplificar el ciclo de vida de los datos mediante el uso de etiquetas de objetos con Amazon S3 Lifecycle para obtener una guía detallada de este proceso.

Además, al clasificar o abordar el resultado de seguridad, las etiquetas pueden proporcionar al investigador un contexto importante que ayuda a calificar el riesgo y ayudan a contratar a los equipos adecuados para investigar o mitigar el resultado.

Etiquetas para administración de identidades y control de acceso

Al administrar el control de acceso a través de un entorno de AWS con AWS IAM Identity Center, las etiquetas pueden habilitar varios patrones de escalado. Se pueden aplicar varios patrones de delegación, algunos se basan en el etiquetado. Los abordaremos de forma individual y proporcionaremos enlaces a lecturas adicionales sobre cada uno de ellos.

ABAC para recursos individuales

Los usuarios del Centro de identidades de IAM y los roles de IAM admiten el control de acceso basado en atributos (ABAC), que permite definir el acceso a las operaciones y los recursos en función de las etiquetas. ABAC ayuda a reducir la necesidad de actualizar las políticas de permisos y a basar el acceso a los atributos de los empleados del directorio corporativo. Si ya utiliza una estrategia de varias múltiples, puede utilizar ABAC además del control de acceso basado en roles

(RBAC) para proporcionar a varios equipos que operan en la misma cuenta un acceso detallado a diferentes recursos. Por ejemplo, los usuarios del Centro de identidades de IAM o los roles de IAM pueden incluir condiciones para limitar el acceso a instancias específicas de Amazon EC2 que, de lo contrario, se tendrían que mostrar de forma explícita en cada política para poder acceder a ellas.

Dado que un modelo de autorización de ABAC depende de las etiquetas para acceder a las operaciones y los recursos, es importante proporcionar barreras de protección para evitar el acceso no deseado. Las SCP se pueden usar para proteger las etiquetas en toda la organización, ya que solo permiten que las etiquetas se modifiquen bajo determinadas condiciones. Los blogs Protección de las etiquetas de recursos utilizadas para la autorización mediante una política de control de servicios en AWS Organizations y Límites de permisos para las entidades de IAM proporcionan información sobre cómo implementar esto.

Cuando se utilizan instancias de Amazon EC2 de larga duración para respaldar prácticas operativas más tradicionales, se puede utilizar este enfoque, el blog Configurar ABAC de Centro de identidades de IAM para las instancias de Amazon EC2 y el administrador de sesiones de Systems Manager analiza con más detalle esta forma de control de acceso basada en atributos. Como se mencionó anteriormente, no todos los tipos de recursos admiten el etiquetado y, de los que lo hacen, no todos admiten la aplicación mediante políticas de etiquetado, por lo que es una buena idea evaluar esto antes de empezar a implementar esta estrategia en una Cuenta de AWS.

Para obtener más información sobre los servicios compatibles con ABAC, consulte servicios de AWS que funcionan con IAM.

Conclusión

Los recursos de AWS se pueden etiquetar para una variedad de propósitos, desde implementar una estrategia de asignación de costos hasta respaldar la automatización o autorizar el acceso a los recursos de AWS. La implementación de una estrategia de etiquetado puede resultar difícil para algunas organizaciones, debido a la cantidad de grupos de partes interesadas que participan y a consideraciones como la obtención de datos y el control del etiquetado.

En este documento técnico, presentamos recomendaciones para diseñar e implementar una estrategia de etiquetado en una organización basada en las prácticas operativas, los casos de uso definidos, las partes interesadas que participan en el proceso y las herramientas y servicios proporcionados por AWS. Cuando se trata de una estrategia de etiquetado, es un proceso de iteración y mejora en el que se empieza poco a poco a partir de la prioridad inmediata, se identifican los casos de uso relevantes en toda la organización y, a continuación, se implementa y amplía el esquema de etiquetado según sea necesario, al tiempo que se mide y mejora continuamente la eficacia. Hemos señalado que un conjunto bien definido de etiquetas dentro de la organización le permitirá relacionar uso y consumo de AWS para los equipos responsables de los recursos y el propósito empresarial para los que existen, a fin de alinearlos con la estrategia y el valor de la organización.

Colaboradores

Los colaboradores de este documento son:

- Chris Pates, administrador técnico de cuentas especialista sénior, Amazon Web Services
- Vijay Shekhar Rao, jefe de soporte empresarial de Amazon Web Services
- Nataliya Godunok, administradora técnica de cuentas especialista sénior, Amazon Web Services
- Yogish Kutkunje Pai, arquitecto sénior de soluciones, Amazon Internet Services Private Limited
- Jamie Ibbs, administrador técnico de cuentas especialista sénior, Amazon Web Services

Documentación adicional

Para obtener más información, consulte

- AWS re:Invent 2020: Working Backwards: Enfoque de Amazon hacia la innovación
- Guía prescriptiva de AWS: aplicación automática de parches para instancias mutables en la nube híbrida mediante AWS Systems Manager
- Centro de arquitectura de AWS

Buena Arquitectura de AWS

- Marco de Buena Arquitectura de AWS
- Pilar de excelencia operativa: Marco de Buena Arquitectura de AWS
- Plan de recuperación de desastres (DR): pilar de fiabilidad de Buena Arquitectura de AWS
- Pilar de optimización de costos: Marco de Buena Arquitectura de AWS
- Laboratorios de Buena Arquitectura de AWS: habilite etiquetas de asignación de costos generadas por AWS
- Laboratorios de Buena Arquitectura de AWS: políticas de etiquetas
- Laboratorios de Buena Arquitectura de AWS: biblioteca de consultas AWS CUR

Blogs de AWS

- AWS Health Aware: personalice alertas de AWS Health para cuentas de AWS de la organización y personales
- Cómo etiquetar automáticamente los recursos de Amazon EC2 en respuesta a eventos de la API
- Etiqueta de asignación de costos generada por AWS frente a definida por el usuario
- Etiquetado e informes de costos con AWS Organizations
- Cómo aplicar parches a las instancias EC2 de Windows mediante AWS Systems Manager Patch Manager
- Evitar las vulnerabilidades de día cero con la aplicación de parches de seguridad el mismo día mediante AWS Systems Manager

Documentación de AWS

- Uso de etiquetas de asignación de costos: AWS Billing and Cost Management y administración de costos
- Qué son los informes de costo y uso de AWS
- Referencia de la API de AWS Resource Groups
- ¿Cómo puedo usar las etiquetas de política de IAM para restringir la forma en que se puede crear una instancia EC2 o un volumen de EBS?
- Modelos de actualización mutables frente a modelos inmutables

Otros

- Bryar, C. y Carr, B. (2021). Working Backwards: ideas, historias y secretos desde dentro de Amazon. London Macmillan.
- AWS CloudFormation Guard (GitHub)

Revisiones del documento

Para recibir notificaciones sobre las actualizaciones de este documento técnico, suscríbase a la fuente RSS.

Cambio	Descripción	Fecha
Actualización menor	Actualizaciones de la administración de identidades	30 de marzo de 2023
Revisión menor	Referencia actualizada en ABAC para los recursos individuales.	24 de febrero de 2023
Revisión menor	Guía actualizada para implementar las prácticas recomendadas de IAM. Para obtener más información, consulte Prácticas recomendadas de seguridad en IAM.	6 de febrero de 2023
Revisión importante	Se ha agregado una referencia más específica para los tipos de recursos compatibles con AWS Config regla `required_tags` .	18 de enero de 2023
Revisión importante	Se ha actualizado para incluir las prácticas y capacidades de servicio más recientes, especialmente en el área de identidad.	29 de septiembre de 2022
Actualización menor	Formato de tabla fijo en versión PDF.	25 de abril de 2022
Revisión importante	Se ha actualizado la estructura del documento y se han	22 de abril de 2022

	ampliado las secciones de estrategia de etiquetado y casos de uso. Se ha agregado una guía más prescriptiva basada en las herramientas, técnicas y recursos disponibl es más recientes.	
Publicación inicial	Documento técnico publicado por primera vez.	1 de diciembre de 2018

> **Note**
>
> Para suscribirse a las actualizaciones de RSS, debe tener un complemento de RSS habilitado para el navegador que esté utilizando.

Avisos

Es responsabilidad de los clientes realizar su propia evaluación independiente de la información que contiene este documento. El presente documento: (a) tiene solo fines informativos, (b) representa las ofertas y prácticas actuales de los productos de AWS, que están sujetas a cambios sin previo aviso, y (c) no supone ningún compromiso ni garantía por parte de AWS y sus filiales, proveedores o licenciantes. Los productos o servicios de AWS se proporcionan “tal cual”, sin garantías, afirmaciones ni condiciones de ningún tipo, ya sean expresas o implícitas. Las responsabilidades y obligaciones de AWS con respecto a sus clientes se controlan mediante los acuerdos de AWS y este documento no forma parte ni modifica ningún acuerdo entre AWS y sus clientes.

© 2022 Amazon Web Services, Inc. o sus filiales. Todos los derechos reservados.

Glosario de AWS

Para ver la terminología más reciente de AWS, consulte el Glosario de AWS en la Referencia de Glosario de AWS.