AWSLivre blanc

Bonnes pratiques en matière de balisage des ressources AWS

Bonnes pratiques en matière de balisage des ressources AWS: AWSLivre blanc

Table of Contents

Bonnes pratiques pour le balisage des ressources AWS

Date de publication : 30 mars 2023 (Révisions du document)

Amazon Web Services (AWS) vous permet d'attribuer des métadonnées à de nombreuses AWS ressources sous forme de balises. Chaque balise est une étiquette simple composée d'une clé et d'une valeur facultative pour stocker des informations sur la ressource ou des données conservées sur cette ressource. Ce livre blanc met l'accent sur le balisage des cas d'utilisation, des stratégies, des techniques et des outils qui peuvent vous aider à classer les ressources par objectif, équipe, environnement ou selon d'autres critères pertinents pour votre entreprise. La mise en œuvre d'une stratégie de balisage cohérente peut faciliter le filtrage et la recherche de ressources, le suivi des coûts et de l'utilisation, ainsi que la gestion de votre AWS environnement.

Ce document s'appuie sur les pratiques et les conseils fournis dans le livre blanc Organizing Your AWS Environment Using Multiple Accounts. Il est recommandé de lire ce livre blanc avant celui-ci. AWSvous recommande d'établir les bases de votre cloud de manière holistique. Pour plus d'informations, reportez-vous à la section Etablissement de votre base cloud sur AWS.

Êtes-vous Well-Architected ?

Le AWSWell-Architected Framework vous aide à comprendre les avantages et les inconvénients des décisions que vous prenez lors de la création de systèmes dans le cloud. Les six piliers du cadre vous permettent d'apprendre les meilleures pratiques architecturales pour concevoir et exploiter des systèmes fiables, sécurisés, efficaces, rentables et durables. À l'aide du AWS Well-Architected Tool, disponible gratuitement dans le AWS Management Console, vous pouvez évaluer votre charge de travail par rapport à ces meilleures pratiques en répondant à une série de questions pour chaque pilier.

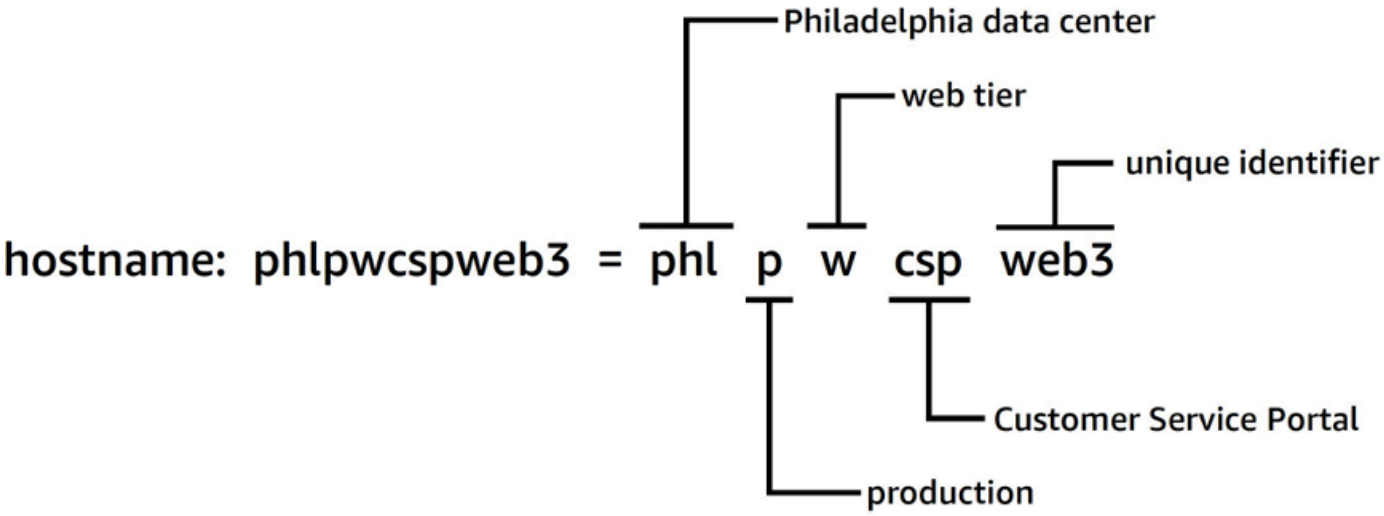
Pour obtenir des conseils d'experts supplémentaires et les meilleures pratiques relatives à votre architecture cloud (déploiements d'architecture de référence, diagrammes et livres blancs), consultez le Centre d'architecture. AWS

Introduction

AWSfacilite le déploiement de vos charges de travail en AWS créant des ressources, telles que des instances Amazon EC2, des volumes AmazonEBS, des groupes de sécurité et des fonctions. AWS Lambda Vous pouvez également faire évoluer et développer le parc de AWS ressources

qui héberge vos applications, stocke vos données et étend votre AWS infrastructure au fil du temps. Au fur et à mesure que votre AWS utilisation s'étendra à de nombreux types de ressources couvrant plusieurs applications, vous aurez besoin d'un mécanisme permettant de savoir quelles ressources sont affectées à telle ou telle application. Utilisez ce mécanisme pour soutenir vos activités opérationnelles, telles que le suivi des coûts, la gestion des incidents, l'application de correctifs, la sauvegarde et le contrôle d'accès.

Dans les environnements sur site, ces connaissances sont souvent capturées dans des systèmes de gestion des connaissances, des systèmes de gestion de documents et sur des pages wiki internes. Avec une base de données de gestion de configuration (CMDB), vous pouvez stocker et gérer les métadonnées détaillées pertinentes à l'aide de processus de contrôle des modifications standard. Cette approche assure la gouvernance, mais nécessite des efforts supplémentaires pour la développer et la maintenir. Vous pouvez adopter une approche structurée pour nommer les ressources, mais un nom de ressource ne peut contenir qu'une quantité limitée d'informations.



Approche structurée de la dénomination des ressources

Par exemple, les instances EC2 possèdent une balise prédéfinie appelée Name qui fournit des fonctionnalités similaires et vous permet de nommer les charges de travail au fur et à mesure de leur déplacement. AWS

En 2010, AWS a lancé des balises de ressources afin de fournir un mécanisme flexible et évolutif permettant d'associer des métadonnées à vos ressources. Ce livre blanc vous guide tout au long du processus de développement et de mise en œuvre d'une stratégie de balisage robuste dans votre environnement. AWS Ces conseils vous aideront à garantir la cohérence et la couverture du balisage afin de soutenir vos décisions et vos activités opérationnelles.

Qu'est-ce qu'une balise ?

Une balise est une paire clé-valeur appliquée à une ressource pour contenir les métadonnées relatives à cette ressource. Chaque balise est une étiquette composée d'une clé et d'une valeur facultative. À l'heure actuelle, tous les services et types de ressources ne prennent pas en charge les balises (voir Services qui prennent en charge l'API Resource Groups Tagging). D'autres services peuvent prendre en charge les balises via leurs propres API. Il convient de noter que les balises ne sont pas cryptées et ne doivent pas être utilisées pour stocker des données sensibles, telles que des données d'identification personnelle.

Les balises qu'un utilisateur crée et applique aux AWS ressources à l'AWS CLIaide de l'API ou du AWS Management Console sont appelées balises définies par l'utilisateur. Plusieurs AWS servicesAWS CloudFormation, tels qu'Elastic Beanstalk et Auto Scaling, attribuent automatiquement des balises aux ressources qu'ils créent et gèrent. Ces clés sont appelées balises AWSgénérées et sont généralement préfixées par`aws`. Ce préfixe ne peut pas être utilisé dans les clés de balise définies par l'utilisateur.

Il existe des exigences d'utilisation et des limites quant au nombre de balises définies par l'utilisateur qui peuvent être ajoutées à une AWS ressource. Pour plus d'informations, reportez-vous à la section Limites et exigences relatives à la dénomination des balises dans le guide de référence AWS général. AWSles balises générées ne sont pas prises en compte dans ces limites de balises définies par l'utilisateur.

Tableau 1 — Exemples de clés et de valeurs de balise définies par l'utilisateur

ID d'instance	Clé de tag	Tag Value (Valeur de balise)
`i-01234567abcdef89a`	`CostCenter`	`98765`
	`Stack`	`Test`
i-12345678abcdef90b	`CostCenter`	`98765`
	`Stack`	`Production`

Tableau 2 — Exemples de balises AWS générées

AWSClés de tag générées	Justification
`aws:ec2spot:fleet-request-id`	Identifie la demande d'instance Spot Amazon EC2 qui a lancé l'instance
`aws:cloudformation:stack-name`	Identifie la AWS CloudFormation pile qui a créé la ressource
`lambda-console:blueprint`	Identifie le plan utilisé comme modèle pour une fonction AWS Lambda
`elasticbeanstalk:environment-name`	Identifie l'application qui a créé la ressource
`aws:servicecatalog: provisionedProductArn`	Nom de ressource Amazon (ARN) du produit approvisionné
`aws:servicecatalog:productArn`	L'ARN du produit à partir duquel le produit approvisionné a été lancé

AWSles balises générées forment un espace de noms. Par exemple, dans un AWS CloudFormation modèle, vous définissez un ensemble de ressources à déployer ensemble dans un`stack`, où `stack-name` figure un nom descriptif que vous attribuez pour l'identifier. Si vous examinez une clé telle que*`aws:cloudformation:stack-name`*, vous pouvez voir que l'espace de noms utilisé pour définir le paramètre utilise trois éléments : aws l'organisation, cloudformation le service et stack-name le paramètre.

Les balises définies par l'utilisateur peuvent également utiliser des espaces de noms et il est recommandé d'utiliser un identifiant d'organisation comme préfixe. Cela vous permet de déterminer rapidement si une balise provient de votre schéma géré ou est définie par un service ou un outil que vous utilisez dans votre environnement.

Dans le AWS livre blanc Establishing Your Cloud Foundation on, nous recommandons un ensemble de balises à implémenter. Il est fort probable que différentes entreprises aient des modèles autorisés différents et des listes différentes pour une étiquette donnée. En regardant l'exemple du tableau 3 :

Tableau 3 — Même clé de balise, règles de validation des valeurs différentes

Organisation	Clé de tag	Validation des valeurs des balises	Exemple de valeur de balise
Entreprise A	`CostCenter`	`5432, 5422, 5499`	`5432`
Entreprise B	`CostCenter`	`ABC*`	`ABC123`

Si ces deux schémas appartiennent à des organisations distinctes, les conflits de balises ne posent aucun problème. Toutefois, si ces deux environnements fusionnent, les espaces de noms peuvent entrer en conflit et la validation devient plus complexe. Ce scénario peut sembler peu probable, mais des entreprises sont rachetées ou fusionnées, et il existe d'autres scénarios, tels que les clients travaillant avec un fournisseur de services gérés, un éditeur de jeux ou une entreprise de capital-risque, où les comptes de différentes organisations font partie d'une AWS organisation partagée. En utilisant le nom commercial comme préfixe pour définir un espace de noms unique, ces difficultés peuvent être évitées, comme le montre le tableau 4 :

Tableau 4 — Utilisation des espaces de noms dans les clés de balise

Organisation	Clé de tag	Validation des valeurs des balises	Exemple de valeur de balise
Entreprise A	`company-a :CostCenter`	`5432, 5422, 5499`	`5432`
Entreprise B	`company-b :CostCenter`	`ABC*`	`ABC123`

Dans les grandes organisations complexes où des entreprises sont régulièrement acquises et cédées, cette situation se produira plus fréquemment. Les processus et pratiques de la nouvelle acquisition étant harmonisés dans l'ensemble du groupe, la situation est résolue. Il est utile de disposer d'espaces de noms distincts, car l'utilisation des anciennes balises peut être signalée et les équipes concernées peuvent être contactées pour adopter le nouveau schéma. Un espace de noms peut également être utilisé pour indiquer une portée ou représenter un cas d'utilisation ou un domaine de responsabilité correspondant aux propriétaires de l'organisation.

Tableau 5 — Exemple de champ d'application ou de cas d'utilisation (champ d'application) dans les clés de balise

Cas d'utilisation	Clé de tag	Justification	Valeurs autorisées
Classification des données	`example-inc:info-sec:data-classification`	Ensemble défini de classification des données pour la sécurité de l'information	`sensitive`, `company-confidential`, `customer-identifiable`
Opérations	`example-inc:dev-ops:environment`	Mettre en œuvre la planification des environnements de test et de développement	`development`, `staging`, `quality-assurance`, `production`
Reprise après sinistre	`example-inc:disaster-recovery:rpo`	Définir l'objectif du point de récupération (RPO) pour une ressource	6h, 24h
Répartition des coûts	`example-inc:cost-allocation:business-unit`	Les équipes financières ont besoin de rapports sur les coûts relatifs à l'utilisation et aux dépenses de chaque équipe	`corporate`, `recruitment`, `support`, `engineering`

Les balises sont simples et flexibles. La clé et la valeur de la balise sont toutes deux des chaînes de longueur variable qui peuvent prendre en charge un large jeu de caractères. Pour plus d'informations sur les longueurs et les jeux de caractères, consultez la section AWSRessources de balisage dans le manuel de référence AWS général. Les balises distinguent les majuscules `costCenter` et minuscules, c'est-à-dire que ce `costcenter` sont des clés de balise différentes. L'orthographe d'un mot peut varier d'un pays à l'autre, ce qui peut affecter vos clés. Par exemple, aux États-Unis, on peut définir une clé comme`costcenter`, mais au Royaume-Uni, elle `costcentre` peut être préférée. Ce sont des clés différentes du point de vue du balisage des ressources. Définissez

l'orthographe, les majuscules et la ponctuation dans le cadre de votre stratégie de balisage. Utilisez ces définitions comme référence pour toute personne qui crée ou gère des ressources. Ce sujet est abordé plus en détail dans la section suivanteElaboration de votre stratégie de marquage.

Elaboration de votre stratégie de marquage

Comme c'est le cas pour de nombreuses pratiques opérationnelles, la mise en œuvre d'une stratégie de balisage est un processus d'itération et d'amélioration. Commencez modestement avec votre priorité immédiate et développez le schéma de balisage selon vos besoins.

Itération de la stratégie de marquage et cycle d'amélioration

Tout au long de ce processus, l'appropriation est essentielle à la responsabilisation et au progrès. Les balises pouvant être utilisées à diverses fins, la stratégie globale de balisage peut être divisée en domaines de responsabilité au sein d'une organisation. Le balisage permet une approche programmatique des activités qui dépendent de la caractérisation des ressources. L'éventail des parties prenantes pouvant bénéficier du balisage dépendra de la taille de l'organisation et des pratiques opérationnelles. Les grandes entreprises peuvent tirer parti de la définition claire des responsabilités des équipes impliquées dans l'élaboration et la mise en œuvre d'une stratégie de marquage. Certaines parties prenantes peuvent être chargées d'identifier les besoins (définition des

cas d'utilisation) en matière de balisage ; d'autres peuvent être responsables de la maintenance, de la mise en œuvre et de l'amélioration de la stratégie de balisage.

En attribuant la propriété, vous êtes bien placé pour mettre en œuvre les différents aspects de la stratégie. Le cas échéant, cette propriété peut être formalisée sous forme de politique et documentée dans une matrice de responsabilité (par exemple, RACI : responsable, responsable, consulté et informé) ou dans un modèle de responsabilité partagée. Dans les petites entreprises, les équipes peuvent jouer plusieurs rôles dans une stratégie de balisage, de la définition des exigences à la mise en œuvre et à l'application.

Définition des besoins et des cas d'utilisation

Commencez à élaborer votre stratégie en dialoguant avec les parties prenantes qui ont un besoin sous-jacent fondamental de consommer des métadonnées. Ces équipes définissent les métadonnées avec lesquelles les ressources doivent être étiquetées pour soutenir leurs activités, telles que le reporting, l'automatisation et la classification des données. Ils décrivent la manière dont les ressources doivent être organisées et les politiques auxquelles elles doivent être associées. Voici des exemples de rôles et de fonctions que ces parties prenantes peuvent avoir dans les organisations :

- Les services financiers et les secteurs d'activité doivent comprendre la valeur de l'investissement en le mettant en relation avec les coûts afin de hiérarchiser les mesures à prendre pour remédier à l'inefficacité. Comprendre les coûts par rapport à la valeur générée permet d'identifier les secteurs d'activité ou les offres de produits qui échouent. Cela permet de prendre des décisions éclairées concernant le maintien du support, l'adoption d'une alternative (par exemple, l'utilisation d'une offre SaaS ou un service géré) ou le retrait d'une offre commerciale non rentable.
- La gouvernance et la conformité doivent comprendre la catégorisation des données (par exemple, publiques, sensibles ou confidentielles), savoir si une charge de travail spécifique est ou non couverte par un audit par rapport à une norme ou à une réglementation spécifique, et quel est l'importance du service (si le service ou l'application est essentiel pour l'entreprise) afin d'appliquer les contrôles et la supervision appropriés, tels que les autorisations, les politiques et la surveillance.
- Les opérations et le développement doivent comprendre le cycle de vie de la charge de travail, les étapes de mise en œuvre de leurs produits pris en charge et la gestion des étapes de lancement (par exemple, développement, test, répartition de la production) ainsi que les priorités de support associées et les exigences de gestion des parties prenantes. Les tâches telles que les sauvegardes, les correctifs, l'observabilité et la dépréciation doivent également être définies et comprises.

- La sécurité de l'information (InfoSec) et les opérations de sécurité (SecOps) décrivent les contrôles à appliquer et ceux qui sont recommandés. InfoSec définit normalement la mise en œuvre des contrôles et SecOps est généralement responsable de la gestion de ces contrôles.

En fonction de votre cas d'utilisation, de vos priorités, de la taille de votre organisation et de vos pratiques opérationnelles, vous devrez peut-être être représenté par différentes équipes au sein de l'organisation, telles que les finances (y compris les achats), la sécurité de l'information, l'activation du cloud et les opérations cloud. Vous devez également être représenté par les propriétaires des applications et des processus pour les fonctions telles que l'application de correctifs, la sauvegarde et la restauration, la surveillance, la planification des tâches et la reprise après sinistre. Ces représentants aident à définir, à mettre en œuvre et à mesurer l'efficacité de la stratégie de marquage. Ils devraient travailler à rebours à partir des parties prenantes et de leurs cas d'utilisation, et animer un atelier interfonctionnel. Au cours de l'atelier, ils ont l'occasion de partager leurs points de vue et leurs besoins, et de contribuer à l'élaboration d'une stratégie globale. Des exemples de participants et de leur implication dans divers cas d'utilisation sont décrits plus loin dans ce livre blanc.

Les parties prenantes définissent et valident également les clés pour les balises obligatoires, et peuvent recommander l'étendue des balises facultatives. Par exemple, les équipes financières peuvent avoir besoin de relier une ressource à un centre de coûts interne, à une unité commerciale ou aux deux. Ils peuvent donc exiger que certaines clés de balise, telles que `CostCenter` et`BusinessUnit`, soient rendues obligatoires. Les équipes de développement individuelles peuvent décider d'utiliser des balises supplémentaires à des fins d'automatisation`EnvironmentName`, telles que`OptIn`, ou`OptOut`.

Les principales parties prenantes doivent se mettre d'accord sur l'approche de la stratégie de marquage et documenter les réponses aux questions liées à la conformité et à la gouvernance, telles que :

- Quels cas d'utilisation doivent être traités ?
- Qui est responsable du balisage des ressources (mise en œuvre) ?
- Comment les balises sont-elles appliquées et quelles méthodes et quelles automatisations seront utilisées (proactives ou réactives) ?
- Comment mesure-t-on l'efficacité et les objectifs du balisage ?
- À quelle fréquence la stratégie de marquage doit-elle être revue ?
- Qui est à l'origine des améliorations ? Comment est-ce fait ?

Les fonctions commerciales, telles que Cloud Enablement, Cloud Business Office et Cloud Platform Engineering, peuvent alors jouer un rôle de facilitateur dans le processus d'élaboration de la stratégie de balisage, contribuer à son adoption et garantir la cohérence de son application en mesurant les progrès, en supprimant les obstacles et en réduisant les efforts dupliqués.

Définition et publication d'un schéma de balisage

Utilisez une approche cohérente pour baliser vos AWS ressources, à la fois pour les balises obligatoires et facultatives. Un schéma de balisage complet vous aide à atteindre cette cohérence. Les exemples suivants peuvent vous aider à démarrer :

- Acceptez les clés de tag obligatoires
- Définissez des valeurs acceptables et des conventions de dénomination des balises (majuscules ou minuscules, tirets ou traits de soulignement, hiérarchie, etc.)
- Confirmez que les valeurs ne constituent pas des informations personnelles (PII)
- Décidez qui peut définir et créer de nouvelles clés de balise
- Convenez de la manière d'ajouter de nouvelles valeurs de balises obligatoires et de la manière de gérer les balises facultatives

Consultez le tableau des catégories de balisage suivant, qui peut être utilisé comme référence pour ce que vous pouvez inclure dans votre schéma de balisage. Vous devez tout de même déterminer la convention que vous utiliserez pour la clé de balise et les valeurs autorisées pour chacune d'entre elles. Le schéma de balisage est le document dans lequel vous le définissez pour votre environnement.

Tableau 6 — Exemple de schéma de balisage définitif (partie 1)

Cas d'utilisation	Clé de tag	Justification	Valeurs autorisées (listées ou préfixe/sufix de valeurs)	Utilisé pour la répartition des coûts	Types de ressources	Portée	Obligatoire
Allocation de coûts	`example-inc:cost-allocation: ApplicationId`	Suivez les coûts par rapport à la valeur générée par chaque secteur d'activité	`DataLakeX` , `RetailSiteX`	Y	Tous	Tous les comptes	Obligatoire
Allocation de coûts	`example-inc:cost-allocation: BusinessUnitId`	Surveillez les coûts par unité commerciale	`Architecture` , `DevOps`, `Finance`	Y	Tous	Tous les comptes	Obligatoire
Allocation de coûts	`example-inc:cost-allocation: CostCenter`	Surveillez les coûts par centre de coûts	`123-*`	Y	Tous	Tous les comptes	Obligatoire
Allocation de coûts	`example-inc:cost-allocation :Owner`	Quel responsable du budget est responsable de cette charge de travail ?	`Marketing` , `RetailSupport`	Y	Tous	Tous les comptes	Obligatoire
Contrôle d'accès	`example-inc:access`	SubComponent Identification/	`DB_Layer`, `Web Layer` ,	N	Tous	Tous les comptes	Facultatif

Tableau 6 — Exemple de schéma de balisage définitif (partie 2)

Cas d'utilisation	Clé de tag	Justification	Valeurs autorisées (listées ou préfixe/sufix de valeurs)	Utilisé pour la répartition des coûts	Types de ressources	Portée	Obligatoire
DevOps	`example-inc:operations: Owner`	Quelle équipe/escouade est responsable de la création et de la maintenance de la ressource	`Squad01`	N	Tous	Tous les comptes	Obligatoire
Reprise après sinistre	`example-inc:disaster-recovery:rpo`	Définir l'objectif de point de récupération (RPO) d'une ressource	`6h`, `24h`	N	S3, EBS	Prod	Obligatoire
Classification de données	`example-inc:data:classification`	Classifiez les données à des fins de conformité et de gouvernance	`Public`, `Private`, `Confidential` , `Restricted`	N	S3, EBS	Tous	Obligatoire
Conformité d'	`example-inc:compliance:framework`	Identifie le cadre de conformité auquel la charge de travail est soumise	`PCI-DSS`, `HIPAA`	N	Tous	Prod	Obligatoire

Une fois le schéma de balisage défini, gérez-le dans un référentiel contrôlé par version accessible à toutes les parties prenantes concernées pour une référence facile et des mises à jour traçables. Cette approche améliore l'eficacité et favorise l'agilité.

AWS Organizations— Politiques relatives aux tags

Les politiques vous AWS Organizations permettent d'appliquer d'autres types de gouvernance Comptes AWS à votre organisation. Une politique de balises est la façon dont vous pouvez exprimer votre schéma de balisage au format JSON afin que la plateforme puisse signaler et éventuellement appliquer le schéma dans votre AWS environnement. La politique de balises définit les valeurs acceptables pour une clé de balise pour des types de ressources spécifiques. Cette politique peut prendre la forme d'une liste de valeurs ou d'un préfixe suivi d'un caractère générique ()*. L'approche du préfixe simple est moins rigoureuse qu'une liste discrète de valeurs mais nécessite moins de maintenance.

Les exemples suivants montrent comment définir une politique de balisage pour valider les valeurs acceptables pour une clé donnée. À partir de la définition tabulaire conviviale du schéma, vous pouvez transcrire ces informations en une ou plusieurs politiques de balises. Des politiques distinctes peuvent être utilisées pour prendre en charge la délégation de propriété ou certaines politiques peuvent ne s'appliquer que dans des scénarios spécifiques.

ExampleInc- CostAllocation .json

Voici un exemple de politique de balises qui rend compte des balises de répartition des coûts :

```
{
  "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": {
```

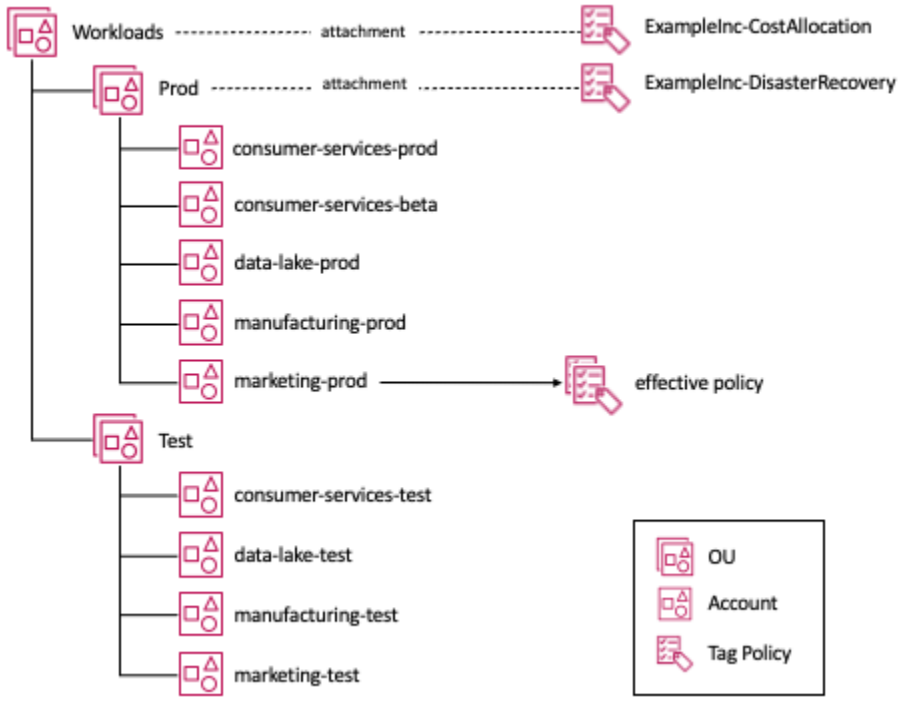
```
        "@@assign": "example-inc:cost-allocation:BusinessUnitId"
      },
      "tag_value": {
        "@@assign": [
          "Architecture",
          "DevOps",
          "FinanceDataLakeX"
        ]
      }
    },
    "example-inc:cost-allocation:CostCenter": {
      "tag_key": {
        "@@assign":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

ExampleInc- DisasterRecovery .json

Voici un exemple de politique de balises qui rend compte des balises Disaster Recovery :

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

Dans cet exemple, la politique de `ExampleInc-CostAllocation` balises est attachée à l'unité d'organisation `Workloads` et s'applique donc à tous les comptes de l'unité d'organisation `Prod` et de l'unité d'`Test`organisation enfant. De même, la politique en matière de `ExampleInc-DisasterRecovery` balises est attachée à l'unité d'`Prod`organisation et ne s'applique donc qu'aux comptes situés en dessous de cette unité d'organisation. Le livre blanc sur l'organisation de votre environnement à l'aide de plusieurs comptes explore plus en détail les structures d'UO recommandées.



Attachement de politiques de balises à une structure d'unité d'organisation

En regardant le `marketing-prod` compte dans le diagramme, les deux politiques de balises s'appliquent à ce compte. Nous avons donc le concept d'une politique efficace, qui est la convolution des politiques d'un type donné qui s'appliquent à un compte. Si vous gérez principalement vos ressources manuellement, vous pouvez consulter la politique effective en consultant la section Resource Groups & Tag Editor:Tag policies de la console. Si vous utilisez l'infrastructure sous forme de code (IaC) ou des scripts pour gérer vos ressources, vous pouvez utiliser l'appel d'`AWS::Organizations::DescribeEffectivePolicy`API.

Implémentation et application du balisage

Dans cette section, nous vous présenterons les outils disponibles pour les stratégies de gestion des ressources suivantes : manuel, infrastructure en tant que code (iAc) et intégration/livraison continues (CI/CD). La dimension clé de ces approches est un taux de déploiement de plus en plus fréquent.

Ressources gérées manuellement

Il s'agit généralement de charges de travail qui entrent dans les étapes de base ou de migration de l'adoption. Il s'agit souvent de charges de travail simples, largement statiques, créées à l'aide de procédures écrites traditionnelles ou migrées telles quelles à l'aide d'outils tels que ceux CloudEndure issus d'un environnement sur site. Les outils de migration, tels que Migration Hub et CloudEndure, peuvent appliquer des balises dans le cadre du processus de migration. Toutefois, si les balises n'ont pas été appliquées lors de la migration initiale ou si le schéma de balisage a changé depuis, l'éditeur de balises (une fonctionnalité duAWS Management Console) vous permet de rechercher des ressources à l'aide de divers critères de recherche et d'ajouter, de modifier ou de supprimer des balises en bloc. Les critères de recherche peuvent inclure des ressources avec ou sans la présence d'une balise ou d'une valeur particulière. L'API AWS Resource Tagging vous permet d'exécuter ces fonctions par programmation.

À mesure que ces charges de travail sont modernisées, des types de ressources tels que les groupes Auto Scaling sont introduits. Ces types de ressources permettent une plus grande élasticité et une meilleure résilience. Le groupe Auto Scaling gère les instances Amazon EC2 en votre nom, mais vous souhaiterez peut-être toujours que les instances EC2 soient étiquetées de manière cohérente avec les ressources créées manuellement. Un modèle de lancement Amazon EC2 permet de spécifier les balises que l'Auto Scaling doit appliquer aux instances qu'il crée.

Lorsque les ressources d'une charge de travail sont gérées manuellement, il peut être utile d'automatiser le balisage des ressources. Différentes solutions sont disponibles. Une approche consiste à utiliserAWS Config Rules, qui permet de vérifier `required_tags` puis de démarrer une fonction Lambda pour les appliquer. AWS Config Rulesest décrit plus en détail plus loin dans ce livre blanc.

Ressources gérées par l'infrastructure sous forme de code (IAc)

AWS CloudFormationfournit un langage commun pour le provisionnement de toutes les ressources d'infrastructure de votre AWS environnement. CloudFormation les modèles sont des fichiers JSON ou YAML qui créent AWS des ressources de manière automatisée. Lorsque vous créez des AWS

ressources à l'aide de CloudFormation modèles, vous pouvez utiliser la propriété CloudFormation Resource Tags pour appliquer des balises aux types de ressources pris en charge lors de leur création. La gestion des balises ainsi que des ressources avec IaC permet de garantir la cohérence.

Lorsque des ressources sont créées parAWS CloudFormation, le service applique automatiquement un ensemble de balises AWS définies aux ressources créées par le AWS CloudFormation modèle. Il s'agit des types suivants :

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

Vous pouvez facilement définir un groupe de ressources en fonction de la AWS CloudFormation pile. Ces balises AWS définies sont héritées par les ressources créées par la pile. Toutefois, pour les instances Amazon EC2 au sein d'un groupe Auto Scaling, `AWS::AutoScaling::AutoScalingGroup TagProperty`elles doivent être définies dans la définition du groupe Auto Scaling dans votre AWS CloudFormation modèle. Sinon, si vous utilisez un modèle de lancement EC2 avec le groupe Auto Scaling, vous pouvez définir les balises dans sa définition. Il est recommandé d'utiliser des modèles de lancement EC2 avec des groupes Auto Scaling ou avec un service de AWS conteneur. Ces services peuvent contribuer à garantir un balisage cohérent de vos instances Amazon EC2 et à prendre en charge l'Auto Scaling sur plusieurs types d'instances et options d'achat, ce qui peut améliorer la résilience et optimiser vos coûts de calcul.

AWS CloudFormationLes Hooks fournissent aux développeurs un moyen de maintenir les principaux aspects de leur application conformes aux normes de leur organisation. Les hooks peuvent être configurés pour fournir un avertissement ou empêcher le déploiement. Cette fonctionnalité est particulièrement adaptée pour vérifier les éléments de configuration clés de vos modèles, par exemple si un groupe Auto Scaling est configuré pour appliquer des balises définies par le client à toutes les instances Amazon EC2 qu'il lancera, ou pour garantir que tous les compartiments Amazon S3 sont créés avec les paramètres de chiffrement requis. Dans les deux cas, l'évaluation de cette conformité est repoussée au début du processus de déploiement avec des AWS CloudFormation hooks avant le déploiement.

AWS CloudFormationpermet de détecter lorsqu'une ressource (voir Ressources prenant en charge la détection des dérives) fournie à partir d'un modèle a été modifiée et que les ressources ne correspondent plus aux configurations de modèle attendues. C'est ce qu'on appelle la dérive. Si vous utilisez l'automatisation pour appliquer des balises aux ressources gérées via IaC, vous les modifiez,

ce qui introduit la dérive. Lors de l'utilisation d'IaC, il est actuellement recommandé de gérer toutes les exigences de balisage dans le cadre des modèles IaC, d'implémenter des AWS CloudFormation hooks et de publier des ensembles de règles AWS CloudFormation Guard pouvant être utilisés par l'automatisation.

ressources gérées par le pipeline CI/CD

À mesure que la maturité d'une charge de travail augmente, il est probable que des techniques telles que l'intégration et le déploiement continus (CI/CD) soient adoptées. Ces techniques contribuent à réduire les risques liés au déploiement en facilitant le déploiement plus fréquent de petites modifications grâce à une automatisation accrue des tests. Une stratégie d'observabilité qui détecte les comportements inattendus introduits par un déploiement peut automatiquement annuler le déploiement avec un impact minimal sur les utilisateurs. À mesure que l'on en arrive au stade du déploiement des dizaines de fois par jour, il n'est tout simplement plus pratique d'appliquer des balises rétroactivement. Tout doit être exprimé sous forme de code ou de configuration, contrôler les versions et, dans la mesure du possible, testé et évalué avant le déploiement en production. Dans le modèle combiné de développement et d'exploitation (DevOps), de nombreuses pratiques prennent en compte les considérations opérationnelles sous forme de code et les valident au début du cycle de vie du déploiement.

Idéalement, vous devez effectuer ces vérifications le plus tôt possible dans le processus (comme le montrent les AWS CloudFormation crochets), afin d'être sûr que votre AWS CloudFormation modèle respecte vos politiques avant qu'il ne quitte la machine du développeur.

AWS CloudFormationGuard 2.0 fournit les moyens de rédiger des règles de conformité préventives pour tout ce que vous pouvez définir. CloudFormation Le modèle est validé par rapport aux règles de l'environnement de développement. De toute évidence, cette fonctionnalité a de nombreuses applications, mais dans ce livre blanc, nous allons simplement examiner quelques exemples qui garantiraient qu'elle `AWS::AutoScaling::AutoScalingGroup TagProperty`est toujours utilisée.

Voici un exemple de règle de CloudFormation garde :

```
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'>>
    }
}
```

Dans l'exemple de code, nous filtrons le modèle pour toutes les ressources de ce typeAutoScalingGroup, puis nous appliquons deux règles :

- **`tags_asg_automation_EnvironmentId`**- Vérifie qu'une balise avec cette clé existe, qu'elle possède une valeur comprise dans la liste de valeurs autorisées et qu'elle `PropagateAtLaunch` est définie sur `true`
- **`tags_asg_costAllocation_CostCenter`**- Vérifie qu'une balise existe avec cette clé, qu'elle possède une valeur commençant par la valeur du préfixe définie et qu'elle `PropagateAtLaunch` est définie sur `true`

Exécution

Comme décrit précédemment, Resource Groups & Tag Editor permet d'identifier les domaines dans lesquels vos ressources ne répondent pas aux exigences de balisage définies dans les politiques de balises appliquées aux unités d'organisation de l'organisation. L'accès à l'outil de console Resource Groups & Tag Editor depuis le compte d'un membre de l'organisation vous indique les politiques qui s'appliquent à ce compte et les ressources du compte qui ne répondent pas aux exigences de la politique de balises. En cas d'accès depuis le compte de gestion (et si l'accès aux politiques de balises est activé dans les services sousAWS Organizations), il est possible de vérifier la conformité aux politiques de balises pour tous les comptes associés de l'organisation.

Dans la politique de balises elle-même, vous pouvez activer l'application pour des types de ressources spécifiques. Dans l'exemple de politique suivant, nous avons ajouté l'application de

telle sorte que toutes les ressources, `ec2:instance` quels que `ec2:volume` soient leur type, doivent être conformes à la politique. Il existe certaines limites connues, telles que la nécessité d'une balise sur une ressource pour qu'elle soit évaluée par la politique de balises. Voir Ressources qui soutiennent l'application de politiques de balises pour obtenir une liste.

ExampleInc-Coût-allocation.json

Voici un exemple de politique de balises qui signale et/ou applique les balises de répartition des coûts :

```
{
  "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 Configest un service qui vous permet d'évaluer et d'évaluer les configurations de vos AWS ressources (voir les types de ressources pris en charge par AWS Config). Dans le cas du balisage, nous pouvons l'utiliser pour identifier les ressources dépourvues de balises avec des clés spécifiques, en utilisant la `required_tags` règle (voir Types de ressources pris en charge par required_tags). À partir de l'exemple précédent, nous pouvons tester l'existence de la clé sur toutes les instances Amazon EC2. Dans les cas où la clé n'existe pas, l'instance sera enregistrée comme non conforme. Ce AWS CloudFormation modèle décrit une AWS Config règle permettant de tester la présence des clés obligatoires décrites dans le tableau, sur les compartiments Amazon S3, les instances Amazon EC2 et les volumes 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
```

Pour les environnements où les ressources sont gérées manuellement, une AWS Config règle peut être améliorée pour ajouter automatiquement la clé de balise manquante aux ressources à l'aide d'une correction automatique via une AWS Lambda fonction. Bien que cela fonctionne bien pour les charges de travail statiques, cela devient progressivement moins efficace lorsque vous commencez à gérer vos ressources via iAC et des pipelines de déploiement.

AWS Organizations— Les politiques de contrôle de service (SCP) sont un type de politique d'organisation que vous permet de gérer les autorisations au sein de votre organisation. Les SCP permettent de contrôler de manière centralisée tous les comptes de votre organisation ou de votre unité organisationnelle (UO). Les SCP affectent uniquement les utilisateurs et les rôles gérés par les comptes qui font partie de l'organisation. Bien qu'ils n'affectent pas directement les ressources, ils limitent les autorisations des utilisateurs et des rôles, y compris les autorisations pour les actions de balisage. En ce qui concerne le marquage, les SCP peuvent fournir une granularité supplémentaire pour l'application des balises, en plus de ce que les politiques en matière de balises peuvent fournir.

Dans l'exemple suivant, la politique refusera les `ec2:RunInstances` demandes où le `example-inc:cost-allocation:CostCenter` tag n'est pas présent.

Ce qui suit est un SCP refusé :

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

Il n'est pas possible de retrouver la politique de contrôle des services effective qui s'applique à un compte lié dès sa conception. Lorsque vous appliquez le balisage avec des SCP, la documentation doit être mise à la disposition des développeurs afin qu'ils puissent s'assurer que leurs ressources respectent les politiques appliquées à leurs comptes. Fournir un accès en lecture seule aux CloudTrail événements de leur compte peut aider les développeurs à déboguer lorsque leurs ressources ne sont pas conformes.

Mesurer l'efficacité du marquage et apporter des améliorations

Une fois que vous avez mis en œuvre une stratégie de balisage, il est important de mesurer son efficacité par rapport aux cas d'utilisation cibles. La mesure de l'efficacité varie selon les cas d'utilisation. Par exemple :

- Attribution des coûts : vous pouvez mesurer la couverture des ressources par balisage en fonction des dépenses à l'aide d'outils tels que le AWS Cost Explorerrapport sur les AWS coûts et l'utilisation. Par exemple, vous pouvez suivre le pourcentage de ressources étiquetées ou non étiquetées qui génèrent des frais, en particulier en surveillant des clés de balise spécifiques.
- Automatisation - Vous souhaiterez peut-être vérifier si le résultat souhaité a été atteint. Par exemple, si les instances Amazon EC2 hors production sont suspendues en dehors des heures de bureau, audit des heures de démarrage et de fin des instances.

Resource Groups & Tag Editor intégré au compte de gestion fournit des fonctionnalités supplémentaires permettant d'analyser le respect des politiques de balises pour tous les comptes associés de votre organisation.

Sur la base des résultats de la mesure de l'efficacité de votre balisage, déterminez si des améliorations ou des modifications sont nécessaires dans l'une des étapes telles que la définition des

cas d'utilisation, la mise en œuvre ou l'application du schéma de balisage. Apportez les modifications nécessaires et répétez le cycle jusqu'à ce que l'efficacité souhaitée soit atteinte. Dans l'exemple d'attribution des coûts, vous pouvez examiner le pourcentage d'amélioration.

Étant donné que ce sont les développeurs et les opérateurs qui doivent effectuer le balisage proprement dit des ressources, il est essentiel qu'ils en prennent possession. Ce n'est pas la seule responsabilité supplémentaire que les équipes assument généralement dans leur parcours d'AWSadoption. Une responsabilité accrue en matière de sécurité et de coût liés au développement et à l'exploitation de leurs applications est également importante. Organisations utilisent souvent des objectifs et des cibles pour motiver l'adoption de nouvelles pratiques. Cela peut donc également s'appliquer ici.

Cas d'utilisation du balisage

Rubriques

Tags pour la répartition des coûts et la gestion financière

L'un des premiers cas d'utilisation du balisage auxquels les entreprises sont souvent confrontées est la visibilité et la gestion des coûts et de l'utilisation. Il y a généralement plusieurs raisons à cela :

- Il s'agit généralement d'un scénario bien compris et les exigences sont bien connues. Par exemple, les équipes financières souhaitent connaître le coût total des charges de travail et de l'infrastructure couvrant plusieurs services, fonctionnalités, comptes ou équipes. L'un des moyens d'obtenir cette visibilité des coûts consiste à étiqueter les ressources de manière cohérente.
- Les balises et leurs valeurs sont clairement définies. En général, des mécanismes de répartition des coûts existent déjà dans les systèmes financiers d'une organisation, par exemple le suivi par centre de coûts, unité commerciale, équipe ou fonction organisationnelle.
- Retour sur investissement rapide et démontrable. Il est possible de suivre les tendances d'optimisation des coûts au fil du temps lorsque les ressources sont étiquetées de manière cohérente, par exemple pour les ressources correctement dimensionnées, mises à l'échelle automatique ou planifiées.

Comprendre comment vous engagez les coûts vous AWS permet de prendre des décisions financières éclairées. Savoir où vous avez engagé des coûts au niveau des ressources, de la charge de travail, de l'équipe ou de l'organisation vous permet de mieux comprendre la valeur apportée au niveau applicable par rapport aux résultats commerciaux obtenus.

Les équipes d'ingénierie n'ont peut-être pas d'expérience en matière de gestion financière de leurs ressources. Le recrutement d'une personne spécialisée en gestion AWS financière capable de former les équipes d'ingénierie et de développement aux bases de la gestion AWS financière et de créer une relation entre les finances et l'ingénierie afin de promouvoir la culture de la finance FinOps aidera à obtenir des résultats mesurables pour l'entreprise et encouragera les équipes à construire en tenant

compte des coûts. L'établissement de bonnes pratiques financières est traité en profondeur par le pilier d'optimisation des coûts du Well-Architected Framework, mais nous aborderons quelques-uns des principes fondamentaux dans ce livre blanc.

Balises d'allocation des coûts

La répartition des coûts fait référence à l'attribution ou à la distribution des coûts encourus aux utilisateurs ou aux bénéficiaires de ces coûts selon un processus défini. Dans le contexte de ce livre blanc, nous divisons la répartition des coûts en deux types : showback et chargeback.

Les outils et mécanismes de présentation contribuent à accroître la prise en compte des coûts. La rétrofacturation contribue au recouvrement des coûts et favorise la prise de conscience des coûts. Le showback concerne la présentation, le calcul et le reporting des frais engagés par une entité spécifique, telle qu'une unité commerciale, une application, un utilisateur ou un centre de coûts. Par exemple : « l'équipe d'ingénierie de l'infrastructure était responsable de X dollars de AWS dépenses le mois dernier ». La rétrofacturation consiste à imputer les coûts engagés à ces entités par le biais des processus comptables internes d'une organisation, tels que les systèmes financiers ou les bons de journal. Par exemple : « X dollars ont été déduits du AWS budget de l'équipe d'ingénierie de l'infrastructure ». Dans les deux cas, le balisage approprié des ressources peut aider à attribuer le coût à une entité, la seule différence étant de savoir si quelqu'un est censé effectuer un paiement ou non.

La gouvernance financière de votre organisation peut nécessiter une comptabilité transparente des coûts engagés au niveau de l'application, de l'unité commerciale, du centre de coûts et de l'équipe. L'attribution des coûts à l'aide de balises de répartition des coûts vous fournit les données nécessaires pour attribuer avec précision les coûts engagés par une entité à partir de ressources étiquetées de manière appropriée.

- Responsabilité — Veiller à ce que les coûts soient alloués aux personnes responsables de l'utilisation des ressources. Un point de service ou un groupe unique peut être responsable de l'examen des dépenses et des rapports.
- Transparence financière — Affichez une vision claire des allocations de trésorerie destinées à l'informatique en créant des tableaux de bord efficaces et une analyse des coûts significative pour les dirigeants.
- Investissements informatiques éclairés : suivez le retour sur investissement en fonction du projet, de l'application ou du secteur d'activité, et permettez aux équipes de prendre de meilleures décisions commerciales, par exemple en allouant davantage de fonds aux applications génératrices de revenus.

En résumé, les balises de répartition des coûts peuvent vous aider à savoir :

- Qui est responsable des dépenses et qui est chargé de les optimiser ?
- Quelle charge de travail, quelle application ou quel produit est à l'origine de ces dépenses ? Quel environnement ou quelle scène ?
- Quels sont les domaines de dépenses qui augmentent le plus rapidement ?
- Quel montant de dépenses peut être déduit d'un AWS budget en fonction des tendances passées ?
- Quel a été l'impact des efforts d'optimisation des coûts sur des charges de travail, des applications ou des produits particuliers ?

L'activation des balises de ressources pour la répartition des coûts aide à définir des pratiques de mesure au sein de l'organisation qui peuvent être utilisées pour fournir une visibilité de l'AWSutilisation et accroître la transparence en matière de responsabilisation en matière de dépenses. Il vise également à créer un niveau de granularité approprié en ce qui concerne la visibilité des coûts et de l'utilisation et à influencer les comportements de consommation dans le cloud grâce à des rapports sur la répartition des coûts et au suivi des KPI.

Élaboration d'une stratégie de répartition des coûts

Définition et mise en œuvre d'un modèle de répartition des coûts

Créez un compte et une structure de coûts pour les ressources déployées dansAWS. Établissez la relation entre les coûts liés aux AWS dépenses, la manière dont ces coûts ont été engagés et qui ou quoi les a engagés. Les structures de coûts communes sont basées sur AWS Organizations les Comptes AWS environnements et les entités au sein de vos organisations, telles qu'un secteur d'activité ou une charge de travail. Les structures de coûts peuvent être basées sur plusieurs attributs afin de permettre l'examen des coûts de différentes manières ou à différents niveaux de granularité, par exemple en cumulant les coûts des différentes charges de travail au secteur d'activité qu'elles desservent.

Lorsque vous choisissez une structure de coûts qui correspond aux résultats souhaités, évaluez les mécanismes de répartition des coûts en fonction de la facilité de mise en œuvre par rapport à la précision souhaitée. Cela peut inclure des considérations relatives à la responsabilité, à la disponibilité des outils et aux changements culturels. Les trois modèles de répartition des coûts les plus courants sur lesquels AWS les clients partent généralement sont les suivants :

- Basé sur les comptes : ce modèle nécessite le moins d'efforts et fournit une grande précision pour les showbacks et les rétrofacturations. Il convient aux organisations ayant une structure de compte définie (et est conforme aux recommandations du livre blanc Organizing Your AWS Environment Using Multiple Accounts). Cela permet une visibilité claire des coûts par compte. Pour la visibilité et la répartition des coûts, vous pouvez utiliser AWS Cost Explorerles rapports sur les coûts et l'utilisation, ainsi que AWSles budgets pour le suivi et le suivi des coûts. Ces outils fournissent des options de filtrage et de regroupement parComptes AWS. Du point de vue de la répartition des coûts, ce modèle ne doit pas nécessairement reposer sur un étiquetage précis des ressources individuelles.
- Par unité commerciale ou par équipe : coût imputable aux équipes, aux unités commerciales ou aux organisations au sein d'une entreprise. Ce modèle nécessite un effort modéré, fournit une grande précision pour les showbacks et les rétrofacturations, et convient aux organisations qui ont une structure de compte définie (généralement en utilisantAWS Organizations), avec une séparation entre les différentes équipes, applications et types de charge de travail. Cela permet une visibilité claire des coûts entre les équipes et les applications et, en tant qu'avantage supplémentaire, réduit le risque d'atteindre les quotas de AWS service en une seule foisCompte AWS. Par exemple, chaque équipe peut avoir cinq comptes (`prod`,`staging`,`test`,`dev`,`sandbox`), et aucune équipe ou application ne partagera le même compte. Avec une telle structure, AWSCost Categories fournira alors la fonctionnalité permettant de regrouper les comptes ou d'autres balises (« méta-tagging ») en catégories, qui peuvent être suivies dans les outils mentionnés dans l'exemple précédent. Il est important de noter que le AWS Organizations balisage des comptes et des unités organisationnelles (UO) est autorisé, mais ces balises ne seront pas applicables à la répartition des coûts et aux rapports de facturation (c'est-à-dire que vous ne pouvez pas regrouper ou filtrer vos coûts AWS Cost Explorer par unité d'organisation). AWS Cost Categories doit être utilisée à cette fin.
- Basé sur des balises : ce modèle demande plus d'efforts que les deux précédents et fournira une grande précision pour les présentations et les rétrofacturations en fonction des exigences et de l'objectif final. Nous vous recommandons vivement d'adopter les pratiques décrites dans le livre blanc Organiser votre AWS environnement à l'aide de comptes multiples, mais en réalité, les clients se retrouvent souvent avec des structures de comptes mixtes et complexes dont la migration prend du temps. La mise en œuvre d'une stratégie de balisage rigoureuse et efficace est essentielle dans ce scénario, suivie de l'activation des balises pertinentes pour la répartition des coûts dans la console Billing and Cost Management (dans ce casAWS Organizations, les balises ne peuvent être activées pour la répartition des coûts qu'à partir du compte Management Payer). Une fois les balises activées pour la répartition des coûts, les outils de visibilité et de répartition des coûts mentionnés dans les méthodes précédentes peuvent être utilisés pour les showbacks et

les rétrofacturations. Notez que les balises de répartition des coûts ne sont pas rétrospectives et n'apparaîtront dans les outils de reporting de facturation et de suivi des coûts qu'une fois qu'elles auront été activées pour la répartition des coûts.

En résumé, si vous devez suivre les coûts par unité commerciale, vous pouvez utiliser AWSCost Categories pour regrouper les comptes liés au sein de AWS l'organisation en conséquence et afficher ce regroupement dans les rapports de facturation. Lorsque vous créez des comptes distincts pour les environnements de production et non liés à la production, vous pouvez également filtrer les coûts liés aux environnements dans des outils tels que AWS Cost Explorer, ou suivre ces coûts à l'aide de AWSBudgets. Enfin, si votre cas d'utilisation nécessite un suivi des coûts plus précis, par exemple par charge de travail ou application individuelle, vous pouvez étiqueter les ressources de ces comptes en conséquence, activer ces clés de balise pour la répartition des coûts sur le compte de gestion, puis filtrer ce coût par clés de balise dans les outils de reporting de facturation.

Mise en place de processus de reporting des coûts et de suivi

Commencez par identifier les types de coûts importants pour les parties prenantes internes (par exemple, les dépenses quotidiennes, le coût par compte, le coût par X, les coûts amortis). Ce faisant, vous pouvez atténuer les risques budgétaires associés à des dépenses inattendues ou anormales plus rapidement que d'attendre la AWS facture finalisée. Les balises fournissent l'attribution qui permet ces scénarios de reporting. Les informations tirées des rapports peuvent éclairer vos actions afin d'atténuer l'impact des dépenses anormales et imprévues sur les budgets financiers. En cas d'augmentation inattendue des coûts, il est important d'évaluer s'il y a eu une augmentation inattendue de la valeur livrée afin de déterminer si et quelles mesures sont nécessaires.

Lorsque vous élaborez une stratégie de balisage pour soutenir la répartition des coûts, gardez à l'esprit les éléments suivants :

- AWS Organizations- La répartition des coûts au sein de plusieurs comptes peut être effectuée par compte, par groupe de comptes ou par groupe de balises créé pour les ressources de ces comptes. Les balises créées pour les ressources résidant dans des comptes individuels ne AWS Organizations peuvent être utilisées pour la répartition des coûts qu'à partir du compte de gestion.
- AWSCompte - La répartition des coûts au sein d'un compte Compte AWS peut être effectuée par des dimensions supplémentaires telles que les services ou les régions. Il est possible de baliser davantage les ressources d'un compte et de travailler avec les groupes de ces balises de ressources.

- Balises de répartition des coûts - Les balises créées par l'utilisateur et les balises AWS générées peuvent être activées pour la répartition des coûts, si nécessaire. L'activation de balises pour la répartition des coûts dans la console de facturation (du compte de gestion intégréAWS Organizations) facilite les showbacks et les rétrofacturations.
- Cost Categories - Les catégories de AWS coûts permettent de regrouper des comptes et des balises de regroupement (« méta-tagging ») au sein d'une AWS organisation, ce qui permet également d'analyser les coûts liés à ces catégories à l'aide d'outils tels que AWS Cost Explorer les AWS budgets et le rapport sur les AWS coûts et l'utilisation.

Réalisation d'une rétrofacturation et d'une rétrofacturation pour les unités commerciales, les équipes ou les organisations de l'entreprise

Attribuez les coûts à l'aide de votre processus de répartition des coûts, soutenu par votre structure de coûts et vos balises de répartition des coûts. Les tags peuvent être utilisés pour donner un aperçu aux équipes qui ne sont pas directement responsables du paiement des coûts, mais qui sont responsables de ces coûts. Cette approche permet de prendre conscience de leur contribution aux dépenses et de la manière dont ces coûts sont engagés. Procédez à la rétrofacturation aux équipes directement responsables des coûts afin de récupérer les dépenses liées aux ressources qu'elles ont consommées et de les informer de ces coûts et de la manière dont ils ont été engagés.

Mesurer et diffuser l'eficacité ou les KPI de valeur

Convenez d'un ensemble de mesures de coût unitaire ou d'indicateurs de performance clés pour mesurer l'impact de vos investissements en gestion financière dans le cloud. Cet exercice crée un langage commun entre les acteurs technologiques et commerciaux, et raconte une histoire basée sur l'eficience, plutôt qu'une histoire centrée uniquement sur les dépenses globales absolues. Pour plus d'informations, consultez ce blog qui explique comment les indicateurs unitaires peuvent aider à harmoniser les fonctions commerciales.

Allocation de dépenses non allouables

Selon les pratiques comptables de l'organisation, les différents types de frais peuvent nécessiter un traitement différent. Identifiez les ressources ou les catégories de coûts qui ne peuvent pas être étiquetées. En fonction des services utilisés et de ceux qu'il est prévu d'utiliser, convenez des mécanismes permettant de traiter et de mesurer ces dépenses non allouables. Par exemple, consultez la liste des ressources prises en charge par AWS Resource Groupset Tag Editor dans le guide de l'utilisateur de AWS Resource Groups and Tags.

Certains frais liés à des remises basées sur des engagements, tels que Reserved Instances (RI) et Savings Plans (SP), constituent un exemple courant de catégorie de coûts qui ne peut pas être étiquetée. Bien que les frais d'abonnement et les frais SP et RI non utilisés ne puissent pas être étiquetés avant d'apparaître dans les outils de reporting de facturation, vous pouvez suivre la manière dont les remises RI et SP s'appliquent aux comptes, aux ressources et à leurs tags AWS Organizations après coup. Par exemple, AWS Cost Explorer il est possible d'examiner le coût amorti, de regrouper les dépenses en fonction des clés de balise pertinentes et d'appliquer des filtres adaptés à votre cas d'utilisation. Dans le rapport sur les AWS coûts et l'utilisation (CUR), vous pouvez filtrer les lignes correspondant à l'utilisation couverte par les remises RI et SP (pour en savoir plus, consultez la section sur les cas d'utilisation de la documentation CUR) et sélectionner les colonnes qui ne concernent que vous. Chaque clé de balise activée pour la répartition des coûts sera présentée dans sa propre colonne distincte à la fin du rapport CUR, de la même manière qu'elle est présentée dans d'autres rapports de facturation existants, tels que le rapport mensuel de répartition des coûts. Pour des références supplémentaires, consultez les AWSWell-Architected Labs pour obtenir des exemples d'informations sur les coûts et l'utilisation à partir des données CUR.

Génération de rapports

Outre les AWS outils disponibles pour faciliter les showbacks et les rétrofacturations, il existe toute une gamme d'autres solutions AWS créées ou tierces qui peuvent aider à surveiller le coût des ressources étiquetées et à mesurer l'efficacité de la stratégie de balisage. En fonction des exigences et de l'objectif final de l'organisation, on peut soit investir du temps et des ressources dans la création de solutions personnalisées, soit acheter des outils fournis par l'un des partenaires de compétence en outils de AWS Cloud gestion. Si vous décidez de créer votre propre outil de répartition des coûts basé sur une source unique de vérité avec des paramètres contrôlés adaptés à l'entreprise, le rapport sur les AWS coûts et l'utilisation (CUR) fournit les données les plus détaillées sur les coûts et l'utilisation et permet de créer des tableaux de bord d'optimisation personnalisés, permettant le filtrage et le regroupement par comptes, services, catégories de coûts, balises de répartition des coûts et de nombreuses autres dimensions. Parmi les solutions basées sur le Cur développées par AWS Cur qui peuvent être utilisées comme l'un de ces outils, consultez les tableaux de bord Cloud Intelligence sur le site Web de Well-Architected LabsAWS.

Tags pour les opérations et le support

Un AWS environnement comportera plusieurs comptes, ressources et charges de travail avec des exigences opérationnelles différentes. Les balises peuvent être utilisées pour fournir du contexte et des conseils aux équipes opérationnelles d'assistance afin d'améliorer la gestion de vos services.

Les balises peuvent également être utilisées pour assurer la transparence de la gouvernance opérationnelle des ressources gérées.

Certains des principaux facteurs à l'origine d'une définition cohérente des balises opérationnelles sont les suivants :

- Pour filtrer les ressources lors des activités d'infrastructure automatisées. Par exemple, lors du déploiement, de la mise à jour ou de la suppression de ressources. Une autre solution est la mise à l'échelle des ressources pour optimiser les coûts et réduire l'utilisation en dehors des heures de bureau. Voir la solution AWSInstance Scheduler pour un exemple pratique.
- Identification des ressources isolées ou déconseillées. Les ressources qui ont dépassé leur durée de vie définie ou qui ont été signalées comme devant être isolées par des mécanismes internes doivent être étiquetées de manière appropriée afin d'aider le personnel de soutien dans son enquête. Les ressources obsolètes doivent être étiquetées avant leur isolation, leur archivage et leur suppression.
- Support requis pour un groupe de ressources. Les ressources ont souvent des exigences de support différentes. Par exemple, ces exigences peuvent être négociées entre les équipes ou définies dans le cadre de la criticité d'une application. Des conseils supplémentaires sur les modèles opérationnels sont disponibles dans le pilier de l'excellence opérationnelle.
- Améliorez le processus de gestion des incidents. En balisant les ressources avec des balises qui offrent une plus grande transparence dans le processus de gestion des incidents, les équipes d'assistance et les ingénieurs ainsi que les équipes de gestion des incidents majeurs (MIM) peuvent gérer les événements plus efficacement.
- Sauvegardes. Les balises peuvent également être utilisées pour identifier la fréquence à laquelle vos ressources doivent être sauvegardées, ainsi que l'emplacement des copies de sauvegarde ou l'endroit où les restaurer. Conseils prescriptifs pour les approches de sauvegarde et de restauration sur. AWS
- Corriger. L'application de correctifs aux instances mutables en cours d'exécution AWS est essentielle à la fois dans le cadre de votre stratégie globale de correction et dans le cadre de la correction des vulnérabilités de type « jour zéro ». Des conseils plus détaillés sur la stratégie globale d'application des correctifs peuvent être trouvés dans les directives prescriptives. La correction des vulnérabilités de type « zero-day » est abordée dans ce blog.
- Observabilité opérationnelle. La traduction d'une stratégie de KPI opérationnels en balises de ressources aidera les équipes opérationnelles à mieux déterminer si les objectifs sont atteints afin d'améliorer les exigences commerciales. L'élaboration d'une stratégie d'indicateurs clés de performance est un sujet distinct, mais elle a tendance à se concentrer sur une entreprise qui

fonctionne de manière stable ou sur laquelle mesurer l'impact et les résultats du changement. Les KPI Dashboards (AWSWell-Architected labs) et l'Operations KPI Workshop (un service proactif de Support aux AWS entreprises) permettent tous deux de mesurer les performances de manière stable. L'article de blog sur la stratégie d'AWSentreprise Measuring the Success of Your Transformation explore la mesure des KPI pour un programme de transformation, tel que la modernisation informatique ou la migration d'une solution sur site vers. AWS

Activités d'infrastructure automatisées

Les balises peuvent être utilisées dans un large éventail d'activités d'automatisation lors de la gestion de l'infrastructure. L'utilisation de AWSSystems Manager, par exemple, vous permettra de gérer les automatisations et les runbooks sur les ressources spécifiées par la paire clé-valeur définie que vous créez. Pour les nœuds gérés, vous pouvez définir un ensemble de balises pour suivre ou cibler les nœuds par système d'exploitation et environnement. Vous pouvez ensuite exécuter un script de mise à jour pour tous les nœuds d'un groupe ou vérifier l'état de ces nœuds. Les ressources de Systems Manager peuvent également être étiquetées pour affiner et suivre vos activités automatisées.

L'automatisation du cycle de vie de démarrage et d'arrêt des ressources de l'environnement peut permettre une réduction significative des coûts pour toute organisation. Le planificateur d'instance activé AWS est un exemple de solution capable de démarrer et d'arrêter des instances Amazon EC2 et Amazon RDS lorsqu'elles ne sont pas nécessaires. Par exemple, les environnements de développement utilisant des instances Amazon EC2 ou Amazon RDS qui ne doivent pas nécessairement être exécutées le week-end n'exploitent pas le potentiel d'économie que peut apporter la fermeture de ces instances. En analysant les besoins des équipes et de leurs environnements, et en étiquetant correctement ces ressources pour automatiser leur gestion, vous pouvez utiliser votre budget de manière efficace.

Exemple de balise de planification utilisée par le planificateur d'instance sur une instance Amazon EC2 :

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

```
}
```

Cycle de vie des charges

Vérifiez l'exactitude des données opérationnelles à l'appui. Assurez-vous que les balises associées au cycle de vie de votre charge de travail font l'objet de révisions périodiques et que les parties prenantes concernées participent à ces révisions.

Tableau 7 — Révision des balises opérationnelles dans le cadre du cycle de vie de la charge de travail

Cas d'utilisation	Clé de tag	Justification	Exemple de valeurs
Titulaire du compte	`example-inc:account-owner:owner`	Le propriétaire du compte et les ressources qu'il contient.	`ops-center` , `dev-ops`, `app-team`
Avis du titulaire du compte	`example-inc:account-owner:review`	Vérification de la mise à jour et de l'exactitude des informations relatives à la propriété du compte.	<review date in the correct format defined in your tagging library>
Propriétaire des données	`example-inc:data-owner:owner`	Le propriétaire des données résidant sur les comptes.	`bi-team`, `logistics` , `security`
Examen par le propriétaire des données	`example-inc:data-owner:review`	Vérification de la mise à jour et de l'exactitude des informations relatives à la propriété des données.	<review date in the correct format defined in your tagging library>

Affectation de balises aux comptes suspendus avant de migrer vers l'unité d'organisation suspendue

Avant de suspendre un compte et de passer à l'unité d'organisation suspendue, comme indiqué dans le livre blanc Organiser votre AWS environnement à l'aide de plusieurs comptes, des balises doivent être ajoutées au compte afin de faciliter le suivi et l'audit internes du cycle de vie d'un compte. Par exemple, une URL relative ou une référence de ticket sur le système de billetterie ITSM d'une organisation, qui indique la piste d'audit d'une application suspendue.

Tableau 8 - Ajouter des balises opérationnelles lorsque le cycle de vie de la charge de travail entre dans une nouvelle phase

Cas d'utilisation	Clé de tag	Justification	Exemple de valeurs
Titulaire du compte	`example-inc:account-owner:owner`	Le propriétaire du compte et les ressources qu'il contient.	`ops-center` , `dev-ops`, `app-team`
Propriétaire des données	`example-inc:data-owner:owner`	Le propriétaire des données résidant sur les comptes.	`bi-team`, `logistics` , `security`
Date de suspension	`example-inc:suspension:date`	Date à laquelle le compte a été suspendu	<suspended date in the correct format defined in your tagging library>
Approbation de la suspension	`example-inc:suspension:approval`	Le lien vers l'approbation de la suspension du compte	`workload/deprecation`

Gestion des incidents

Les tags peuvent jouer un rôle essentiel dans toutes les phases de la gestion des incidents, qu'il s'agisse de l'enregistrement des incidents, de la priorisation, de l'investigation, de la communication, de la résolution ou de la clôture.

Les balises peuvent indiquer où un incident doit être enregistré, l'équipe ou les équipes qui doivent être informées de l'incident et la priorité d'escalade définie. Il est important de se rappeler que les balises ne sont pas cryptées. Pensez donc aux informations que vous y stockez. De plus, dans les organisations, les équipes et les chaînes hiérarchiques, les responsabilités changent. Pensez donc à stocker un lien vers un portail sécurisé où ces informations peuvent être gérées plus efficacement. Il n'est pas nécessaire que ces balises soient exclusives. Par exemple, l'ID d'application peut être utilisé pour rechercher les chemins d'escalade dans un portail de gestion des services informatiques. Assurez-vous qu'il est clairement indiqué dans vos définitions opérationnelles que cette balise est utilisée à des fins multiples.

Les balises relatives aux exigences opérationnelles peuvent également être détaillées, afin d'aider les responsables des incidents et le personnel des opérations à affiner leurs objectifs en réponse à un incident ou à un événement.

Les liens relatifs (vers l'URL de la base de connaissances) pour les runbooks et les playbooks peuvent être inclus sous forme de balises pour aider les équipes répondantes à identifier le processus, la procédure et la documentation correspondants.

Tableau 9 - Utiliser des balises opérationnelles pour informer la gestion des incidents

Cas d'utilisation	Clé de tag	Justification	Exemple de valeurs
Gestion des incidents	`example-inc:incident-management:escalationlog`	Le système utilisé par l'équipe d'assistance pour enregistrer les incidents	`jira`, `servicenow` , `zendesk`
Gestion des incidents	`example-inc:incident-management:escalationpath`	La voie de l'escalade	`ops-center` , `dev-ops`, `app-team`
Répartition des coûts et gestion des incidents	`example-inc:cost-allocation:CostCenter`	Surveillez les coûts par centre de coûts. Il s'agit d'un exemple de balise à double usage dans laquelle le centre de coûts est utilisé comme code	`123-*`

Cas d'utilisation	Clé de tag	Justification	Exemple de valeurs
		d'application pour la journalisation des incidents.	
Calendrier de sauvegarde	`example-inc:backup:schedule`	Backup planning de la ressource	`Daily`
Playbook/Gestion des incidents	`example-inc:incident-management:playbook`	Playbook documenté	`webapp/incident/playbook`

Corriger

Organisations peuvent automatiser leur stratégie d'application de correctifs pour les environnements informatiques mutables et maintenir les instances mutables conformes à la ligne de base de correctifs définie pour cet environnement d'application en utilisant AWS Systems Manager Patch Manager et. AWS Lambda Une stratégie de balisage pour les instances mutables au sein de ces environnements peut être gérée en affectant ces instances à des groupes de correctifs et à des fenêtres de maintenance. Consultez les exemples suivants pour un split Dev → Test → Prod. AWSdes instructions prescriptives sont disponibles pour la gestion des correctifs des instances mutables.

Tableau 10 - Les balises opérationnelles peuvent être spécifiques à l'environnement

Développement	Intermédiaire	Production
{ "Tags": [{ "Key": "Maintenance Window", "ResourceId": "i-012345678ab9ab111", "ResourceType": "instance",	{ "Tags": [{ "Key": "Maintenance Window", "ResourceId": "i-012345678ab9ab444", "ResourceType": "instance",	{ "Tags": [{ "Key": "Maintenance Window", "ResourceId": "i-012345678ab9ab777", "ResourceType": "instance",

Développement	Intermédiaire	Production

<pre>"Value": "cron(30 23 ? * TUE#1 *)"
},
{
"Key": "Name",
"ResourceId": "i-012345678ab9ab222",
"ResourceType": "instance",
"Value": "WEBAPP"
},
{
"Key": "Patch Group",
"ResourceId": "i-012345678ab9ab333",
"ResourceType": "instance",
"Value": "WEBAPP-DEV-AL2"
}
]
}</pre>
	<pre>"Value": "cron(30 23 ? * TUE#2 *)"
	},
	{
	"Key": "Name",
	"ResourceId": "i-012345678ab9ab555",
	"ResourceType": "instance",
	"Value": "WEBAPP"
	},
	{
	"Key": "Patch Group",
	"ResourceId": "i-012345678ab9ab666",
	"ResourceType": "instance",
	"Value": "WEBAPP-TEST-AL2"
	}
	]
	}</pre>
		<pre>"Value": "cron(30 23 ? * TUE#3 *)"
		},
		{
		"Key": "Name",
		"ResourceId": "i-012345678ab9ab888",
		"ResourceType": "instance",
		"Value": "WEBAPP"
		},
		{
		"Key": "Patch Group",
		"ResourceId": "i-012345678ab9ab999",
		"ResourceType": "instance",
		"Value": "WEBAPP-PROD-AL2"
		}
		]
		}</pre>

Les vulnérabilités de type « jour zéro » peuvent également être gérées en définissant des balises pour compléter votre stratégie d'application de correctifs. Reportez-vous à la section Éviter les vulnérabilités de type « jour zéro » grâce à l'application de correctifs de sécurité le jour même à l'aide de AWS Systems Manager pour obtenir des instructions détaillées.

Observabilité opérationnelle

L'observabilité est nécessaire pour obtenir des informations exploitables sur les performances de vos environnements et vous aider à détecter et à étudier les problèmes. Il a également un objectif secondaire qui vous permet de définir et de mesurer des indicateurs de performance clés (KPI) et des objectifs de niveau de service (SLO) tels que le temps de disponibilité. Pour la plupart des entreprises, les KPI opérationnels importants sont le temps moyen de détection (MTTD) et le temps moyen de reprise (MTTR) après un incident.

Tout au long de l'observabilité, le contexte est important, car les données sont collectées, puis les balises associées sont collectées. Quel que soit le service, l'application ou le niveau d'application sur lequel vous vous concentrez, vous pouvez filtrer et analyser pour ce jeu de données spécifique. Les tags peuvent être utilisés pour automatiser l'intégration aux CloudWatch alarmes afin que les bonnes équipes puissent être alertées lorsque certains seuils métriques sont dépassés. Par exemple, une clé de balise `example-inc:ops:alarm-tag` et la valeur qu'elle contient peuvent indiquer la création de l' CloudWatch alarme. Une solution illustrant cela est décrite dans Utiliser des balises pour créer et gérer des CloudWatch alarmes Amazon pour les instances Amazon EC2.

La configuration d'un trop grand nombre d'alarmes peut facilement créer une tempête d'alertes, lorsqu'un grand nombre d'alarmes ou de notifications submergent rapidement les opérateurs et réduisent leur efficacité globale alors que les opérateurs trient et hiérarchisent manuellement les alarmes individuelles. Un contexte supplémentaire pour les alarmes peut être fourni sous forme de balises, ce qui signifie que des règles peuvent être définies au sein d'Amazon EventBridge pour garantir que l'accent est mis sur le problème en amont plutôt que sur les dépendances en aval.

Le rôle des opérations parallèles DevOps est souvent négligé, mais pour de nombreuses organisations, les équipes opérationnelles centrales continuent d'apporter une première réponse essentielle en dehors des heures normales de bureau. (Vous trouverez plus de détails sur ce modèle dans le livre blanc sur l'excellence opérationnelle.) Contrairement à l' DevOps équipe responsable de la charge de travail, elle n'a généralement pas les mêmes connaissances approfondies. Le contexte fourni par les balises dans les tableaux de bord et les alertes peut donc les diriger vers le runbook adapté au problème, ou lancer un runbook automatique (voir le billet de blog Automating Amazon CloudWatch Alarms with). AWS Systems Manager

Balises pour la sécurité des données, la gestion des risques et le contrôle d'accès

Organisations ont des besoins et des obligations variés à satisfaire en ce qui concerne la gestion appropriée du stockage et du traitement des données. La classification des données est un précurseur important pour plusieurs cas d'utilisation, tels que le contrôle d'accès, la conservation des données, l'analyse des données et la conformité.

Sécurité des données et gestion des risques

Au sein d'un AWS environnement, vous aurez probablement des comptes soumis à des exigences de conformité et de sécurité différentes. Par exemple, vous pouvez disposer d'un sandbox pour

développeurs et d'un compte hébergeant l'environnement de production pour une charge de travail hautement réglementée, telle que le traitement des paiements. En les isolant dans différents comptes, vous pouvez appliquer des contrôles de sécurité distincts, restreindre l'accès aux données sensibles et réduire la portée de l'audit pour les charges de travail réglementées.

L'adoption d'une norme unique pour toutes les charges de travail peut être source de défis. Bien que de nombreux contrôles s'appliquent de la même manière dans un environnement, certains sont excessifs ou non pertinents pour les comptes qui n'ont pas besoin de respecter des cadres réglementaires spécifiques et pour les comptes dans lesquels aucune donnée personnelle identifiable ne sera jamais présente (par exemple, un bac à sable pour développeurs ou des comptes de développement de charge de travail). Cela conduit généralement à des résultats de sécurité faussement positifs qui doivent être triés et corrigés sans aucune action, ce qui réduit les efforts nécessaires aux résultats qui devraient faire l'objet d'une enquête.

Tableau 11 — Exemples de balises de sécurité des données et de gestion des risques

Cas d'utilisation	Clé de tag	Justification	Exemple de valeurs
Gestion des incidents	`example-inc:incident-management:escalationlog`	Le système utilisé par l'équipe d'assistance pour enregistrer les incidents	`jira`, `servicenow` , `zendesk`
Gestion des incidents	`example-inc:incident-management:escalationpath`	La voie de l'escalade	`ops-center` , `dev-ops`, `app-team`
Classification des données	`example-inc:data:classification`	Classifiez les données à des fins de conformité et de gouvernance	`Public`, `Private`, `Confidential` , `Restricted`
Conformité d'	`example-inc:compliance:framework`	Identifie le cadre de conformité auquel la charge de travail est soumise	`PCI-DSS`, `HIPAA`

La gestion manuelle des différents contrôles dans un AWS environnement est à la fois chronophage et source d'erreurs. L'étape suivante consiste à automatiser le déploiement des contrôles de sécurité appropriés et à configurer l'inspection des ressources en fonction de la classification de ce compte. En appliquant des balises aux comptes et aux ressources qu'ils contiennent, le déploiement des contrôles peut être automatisé et configuré en fonction de la charge de travail.

Exemple :

Une charge de travail inclut un compartiment Amazon S3 dont la balise `example-inc:data:classification` contient la valeur`Private`. L'automatisation des outils de sécurité déploie une AWS Config règle `s3-bucket-public-read-prohibited` qui vérifie les paramètres de blocage de l'accès public du compartiment Amazon S3, la politique du compartiment et la liste de contrôle d'accès au compartiment (ACL), confirmant que la configuration du compartiment est adaptée à la classification des données. Pour garantir que le contenu du compartiment est conforme à la classification, Amazon Macie peut être configuré pour vérifier la présence d'informations personnelles identifiables (PII). Le blog Utiliser Amazon Macie pour valider la classification des données des compartiments S3 explore ce modèle de manière plus approfondie.

Certains environnements réglementaires, tels que les assurances et les soins de santé, peuvent être soumis à des politiques obligatoires de conservation des données. La conservation des données à l'aide de balises, associée aux politiques de cycle de vie d'Amazon S3, peut être un moyen simple et efficace de définir les transitions d'objets vers un autre niveau de stockage. Les règles du cycle de vie d'Amazon S3 peuvent également être utilisées pour faire expirer des objets afin de les supprimer après l'expiration de la période de conservation obligatoire. Reportez-vous à Simplifiez le cycle de vie de vos données en utilisant des balises d'objet avec Amazon S3 Lifecycle pour un guide détaillé de ce processus.

En outre, lors du tri ou de la prise en compte d'une constatation de sécurité, les balises peuvent fournir à l'enquêteur un contexte important qui aide à qualifier le risque et à impliquer les équipes appropriées pour enquêter ou atténuer le résultat.

Tags pour la gestion des identités et le contrôle d'accès

Lors de la gestion du contrôle d'accès dans un AWS environnement doté de balisesAWS IAM Identity Center, les balises peuvent activer plusieurs modèles de mise à l'échelle. Plusieurs modèles de délégation peuvent être appliqués, certains sont basés sur le balisage. Nous les aborderons individuellement et fournirons des liens pour en savoir plus sur chacun d'entre eux.

ABAC pour les ressources individuelles

Les utilisateurs et les rôles IAM de l'IAM Identity Center prennent en charge le contrôle d'accès basé sur les attributs (ABAC), qui vous permet de définir l'accès aux opérations et aux ressources en fonction des balises. ABAC permet de réduire le besoin de mettre à jour les politiques d'autorisation et vous aide à baser l'accès sur les attributs des employés figurant dans le répertoire de votre entreprise. Si vous utilisez déjà une stratégie multi-comptes, l'ABAC peut être utilisé en complément du contrôle d'accès basé sur les rôles (RBAC) pour fournir à plusieurs équipes opérant sur le même compte un accès granulaire à différentes ressources. Par exemple, les utilisateurs du centre d'identité IAM ou les rôles IAM peuvent inclure des conditions visant à limiter l'accès à des instances Amazon EC2 spécifiques qui, autrement, devraient être explicitement répertoriées dans chaque politique pour y accéder.

Étant donné qu'un modèle d'autorisation ABAC repose sur des balises pour accéder aux opérations et aux ressources, il est important de prévoir des garde-fous pour empêcher tout accès involontaire. Les SCP peuvent être utilisés pour protéger les tags au sein de votre organisation en autorisant uniquement la modification des tags sous certaines conditions. Les blogs Sécurisation des balises de ressources utilisées pour l'autorisation en utilisant une politique de contrôle des services dans AWS Organizations et des limites d'autorisations pour les entités IAM fournissent des informations sur la façon de l'implémenter.

Lorsque des instances Amazon EC2 à longue durée de vie sont utilisées pour prendre en charge des pratiques opérationnelles plus traditionnelles, cette approche peut être utilisée. Le blog Configure IAM Identity Center ABAC pour les instances Amazon EC2 et le gestionnaire de session Systems Manager abordent plus en détail cette forme de contrôle d'accès basé sur les attributs. Comme indiqué précédemment, tous les types de ressources ne prennent pas en charge le balisage, et parmi ceux qui le sont, tous ne prennent pas en charge l'application de politiques de balises. Il est donc conseillé d'évaluer cela avant de commencer à implémenter cette stratégie sur unCompte AWS.

Pour en savoir plus sur les services compatibles avec ABAC, consultez AWSServices compatibles avec IAM.

Conclusion

AWSles ressources peuvent être étiquetées à diverses fins, qu'il s'agisse de mettre en œuvre une stratégie de répartition des coûts, de soutenir l'automatisation ou d'autoriser l'accès aux AWS ressources. La mise en œuvre d'une stratégie de marquage peut s'avérer difficile pour certaines organisations, en raison du nombre de groupes de parties prenantes impliqués et de considérations telles que l'approvisionnement en données et la gouvernance des balises.

Dans ce livre blanc, nous avons présenté des recommandations concernant la conception et la mise en œuvre d'une stratégie de marquage dans une organisation basée sur les pratiques opérationnelles, les cas d'utilisation définis, les parties prenantes impliquées dans le processus, ainsi que les outils et services fournis par. AWS Lorsqu'il s'agit d'une stratégie de balisage, il s'agit d'un processus d'itération et d'amélioration, dans le cadre duquel vous commencez modestement par rapport à votre priorité immédiate, identifiez les cas d'utilisation pertinents au sein de votre organisation, puis implémentez et développez le schéma de balisage selon vos besoins, tout en mesurant et en améliorant continuellement l'efficacité. Nous avons indiqué qu'un ensemble bien défini de balises au sein de votre organisation vous permettra de relier l'AWSutilisation et la consommation aux équipes responsables des ressources et de l'objectif commercial pour lesquels elles existent, afin de les aligner sur la stratégie et la valeur de l'organisation.

Collaborateurs

Les contributeurs à ce document incluent :

- Chris Pates, responsable technique senior des comptes, Amazon Web Services
- Vijay Shekhar Rao, responsable du support aux entreprises, Amazon Web Services
- Nataliya Godunok, responsable technique senior des comptes, Amazon Web Services
- Yogish Kutkunje Pai, architecte de solutions senior, Amazon Internet Services Private Limited
- Jamie Ibbs, responsable technique senior des comptes, Amazon Web Services

Suggestions de lecture

Pour plus d'informations, reportez-vous à

- AWSre:Invent 2020 : Travailler à rebours : l'approche d'Amazon en matière d'innovation
- AWSConseils prescriptifs : application automatique de correctifs pour les instances mutables dans le cloud hybride à l'aide de Systems Manager AWS
- AWSCentre d'architecture

AWSWell-Architected

- AWSFramework Well-Architected
- Pilier de l'excellence opérationnelle - AWS Well-Architected Framework
- Plan de reprise après sinistre (DR) - Pilier de fiabilité AWS Well-Architected
- Pilier d'optimisation des coûts - AWS Well-Architected Framework
- AWSWell-Architected Labs : AWS activer les balises de répartition des coûts générées
- AWSWell-Architected Labs : Politiques relatives aux balises
- AWSWell-Architected Labs AWS : bibliothèque de requêtes CUR

AWSblogues

- AWS HealthAware — Personnalisez les AWS Health alertes pour les AWS comptes professionnels et personnels
- Comment baliser automatiquement les ressources Amazon EC2 en réponse à des événements d'API
- AWSBalise de répartition des coûts générée ou définie par l'utilisateur
- Marquage des coûts et établissement de rapports avec AWS Organizations
- Appliquer des correctifs à vos instances Windows EC2 à l'aide AWS Systems Manager du Gestionnaire de correctifs
- Évitez les vulnérabilités de type « jour zéro » en appliquant des correctifs de sécurité le jour même à l'aide de AWS Systems Manager

Documentation AWS

- Utilisation des balises de répartition des coûts, gestion des coûts AWS Billing and Cost Management et gestion des coûts
- Que sont les Rapports d'utilisation et de AWS coûts
- Référence API AWS Resource Groups
- Comment puis-je utiliser les balises de politique IAM pour restreindre la manière dont une instance EC2 ou un volume EBS peut être créé ?
- Modèles de mise à jour mutables ou immuables

Autre

- Bryar, C. et Carr, B. (2021). Travailler à rebours : informations, histoires et secrets provenant d'Amazon. Londres Macmillan.
- AWS CloudFormationGarde (GitHub)

Révisions du document

Pour recevoir les notifications des mises à jour de ce livre blanc, abonnez-vous au flux RSS.

Modification	Description	Date
Mise à jour mineure	Mises à jour de la gestion des identités	30 mars 2023
Révision mineure	Référence mise à jour dans ABAC pour les ressources individuelles.	24 février 2023
Révision mineure	Guide mis à jour pour s'aligner sur les bonnes pratiques IAM. Pour de plus amples informations, veuillez consulter Bonnes pratiques de sécurité dans IAM.	6 février 2023
Révision majeure	Ajout d'une référence plus spécifique pour les types de ressources pris en charge par AWS Config la règle`required_tags` .	18 janvier 2023
Révision majeure	Mis à jour pour inclure les dernières pratiques et capacités de service, en particulier dans le domaine de l'identité.	29 septembre 2022
Mise à jour mineure	Formatage de tableau fixe dans la version PDF.	25 avril 2022
Révision majeure	Structure du document mise à jour et sections étendues sur la stratégie de balisage	22 avril 2022

	et les cas d'utilisation. Ajout de directives plus prescript ives basées sur les derniers outils, techniques et ressource s disponibles.	
Publication initiale	Livre blanc publié pour la première fois.	1 décembre 2018

> **Note**
>
> Pour vous abonner aux mises à jour RSS, un plug-in RSS doit être activé pour le navigateur que vous utilisez.

Avis

Les clients sont tenu de réaliser leur propre évaluation indépendante des informations contenues dans ce document. Ce document : (a) est fourni à titre informatif uniquement, (b) représente les offres de AWS produits et les pratiques actuelles, qui sont susceptibles d'être modifiées sans préavis, et (c) ne crée aucun engagement ni aucune assurance de la part de AWS ses filiales, fournisseurs ou concédants de licence. AWSles produits ou services sont fournis « tels quels » sans garanties, déclarations ou conditions d'aucune sorte, qu'elles soient explicites ou implicites. Les responsabilités et obligations AWS de ses clients sont régies par AWS des accords, et ce document ne fait partie d'aucun accord conclu entre AWS et ses clients et ne les modifie pas.

Glossaire AWS

Pour connaître la terminologie la plus récente d'AWS, consultez le Glossaire AWS dans la Référence Glossaire AWS.

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.