AWSWhitepaper

Le migliori pratiche per etichettare le risorse AWS

Le migliori pratiche per etichettare le risorse AWS: AWSWhitepaper

Table of Contents

Best practice per etichettare le risorse AWS

Data di pubblicazione: 30 marzo 2023 () Revisioni del documento

Amazon Web Services (AWS) ti consente di assegnare metadati a molte delle tue AWS risorse sotto forma di tag. Ogni tag è una semplice etichetta che consiste di una chiave e un valore facoltativo che consiste di una chiave che consiste di una chiave o un valore facoltativo che consiste di una risorsa o i dati conservati su quella risorsa. Questo white paper si concentra sull'etichettatura di casi d'uso, strategie, tecniche e strumenti che possono aiutarti a classificare le risorse in base allo scopo, al team, all'ambiente o ad altri criteri pertinenti alla tua attività. L'implementazione di una strategia di etichettatura coerente può semplificare il filtraggio e la ricerca di risorse, il monitoraggio dei costi e dell'utilizzo e la gestione dell'ambiente. AWS

Questo paper si basa sulle pratiche e le linee guida fornite nel white paper Organization Your AWS Environment Using Multiple Accounts. Si consiglia di leggere quel white paper prima di questo. AWSconsiglia di stabilire le fondamenta del cloud in modo olistico. Per ulteriori informazioni, consulta Establishing your Cloud Foundation on AWS.

Sei Well-Architected?

Il AWSWell-Architected Framework ti aiuta a comprendere i pro e i contro delle decisioni che prendi quando crei sistemi nel cloud. I sei pilastri del Framework consentono di apprendere le migliori pratiche architettoniche per progettare e gestire sistemi affidabili, sicuri, efficienti, convenienti e sostenibili. Utilizzando AWS Well-Architected Tool, disponibile gratuitamente in AWS Management Console, puoi esaminare i tuoi carichi di lavoro rispetto a queste best practice rispondendo a una serie di domande per ogni pilastro.

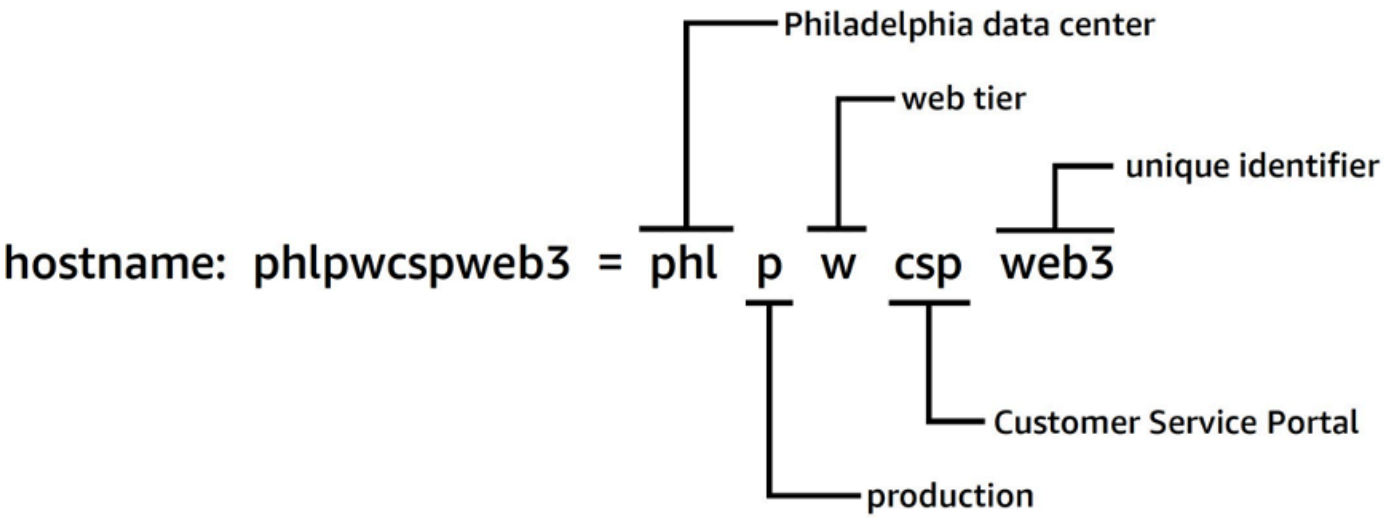
Per ulteriori indicazioni e best practice da parte degli esperti per la tua architettura cloud (implementazioni dell'architettura di riferimento, diagrammi e white paper), consulta l'Architecture Center. AWS

Introduzione

AWSsemplifica l'implementazione dei carichi di lavoro AWS creando risorse, come istanze Amazon EC2, volumi AmazonEBS, gruppi di sicurezza e funzioni. AWS Lambda Puoi anche scalare e ampliare il parco di AWS risorse che ospita le tue applicazioni, archivia i tuoi dati ed espande la tua infrastruttura nel tempo. AWS Man mano che AWS l'utilizzo aumenta fino a raggiungere diversi

tipi di risorse su più applicazioni, sarà necessario un meccanismo per tenere traccia delle risorse assegnate a ciascuna applicazione. Utilizzate questo meccanismo per supportare le vostre attività operative, come il monitoraggio dei costi, la gestione degli incidenti, l'applicazione di patch, il backup e il controllo degli accessi.

Negli ambienti locali, questa conoscenza viene spesso acquisita nei sistemi di gestione della conoscenza, nei sistemi di gestione dei documenti e nelle pagine wiki interne. Con un database di gestione della configurazione (CMDB), è possibile archiviare e gestire i metadati dettagliati pertinenti utilizzando processi standard di controllo delle modifiche. Questo approccio fornisce la governance, ma richiede uno sforzo aggiuntivo per lo sviluppo e la manutenzione. È possibile adottare un approccio strutturato alla denominazione delle risorse, ma un nome di risorsa può contenere solo una quantità limitata di informazioni.



Approccio strutturato alla denominazione delle risorse

Ad esempio, le istanze EC2 hanno un tag predefinito chiamato Name che offre funzionalità simili e consente di assegnare un nome ai carichi di lavoro man mano che vengono spostati. AWS

Nel 2010, AWS ha lanciato i tag di risorse per fornire un meccanismo flessibile e scalabile per allegare i metadati alle risorse. Questo white paper vi guida attraverso il processo di sviluppo e implementazione di una solida strategia di tagging in tutto il vostro ambiente. AWS Questa guida vi aiuterà a garantire la coerenza e la copertura dei tag a supporto delle vostre attività decisionali e operative

Cosa sono i tag?

Un tag è una coppia chiave-valore applicata a una risorsa per contenere i metadati relativi a quella risorsa. Ogni tag è un'etichetta composta da una chiave e un valore opzionale. Attualmente non tutti i servizi e i tipi di risorse supportano i tag (vedi Servizi che supportano l'API Resource Groups Tagging). Altri servizi possono supportare i tag tramite le proprie API. Si devono tenere presente che i tag non sono crittografati e non devono essere utilizzati per archiviare informazioni sensibili (PII).

I tag che un utente crea e applica alle AWS risorse utilizzando l'AWS CLIAPI o il AWS Management Console sono noti come tag definiti dall'utente. Diversi AWS serviziAWS CloudFormation, come Elastic Beanstalk e Auto Scaling, assegnano automaticamente tag alle risorse che creano e gestiscono. Queste chiavi sono note come tag AWSgenerati e in genere hanno come prefisso. `aws` Questo prefisso non può essere utilizzato nelle chiavi di tag definite dall'utente.

Esistono requisiti di utilizzo e limiti al numero di tag definiti dall'utente che possono essere aggiunti a una risorsa. AWS Per ulteriori informazioni, consulta Limiti e requisiti di denominazione dei tag nella guida di riferimento AWS generale. AWSi tag generati non vengono conteggiati ai fini di questi limiti di tag definiti dall'utente.

Tabella 1 — Esempi di chiavi e valori di tag definiti dall'utente

ID istanza	Chiave tag	Valore Tag
`i-01234567abcdef89a`	`CostCenter`	`98765`
	`Stack`	`Test`
i-12345678abcdef90b	`CostCenter`	`98765`
	`Stack`	`Production`

Tabella 2 — Esempi di tag generati AWS

AWSChiavi di tag generate	Rationale
`aws:ec2spot:fleet-request-id`	Identifica la richiesta di istanza Spot di Amazon EC2 che ha avviato l'istanza

AWSChiavi di tag generate	Rationale
`aws:cloudformation:stack-name`	Identifica lo AWS CloudFormation stack che ha creato la risorsa
`lambda-console:blueprint`	Identifica il blueprint utilizzato come modello per una funzione AWS Lambda
`elasticbeanstalk:environment-name`	Identifica l'applicazione che ha creato la risorsa
`aws:servicecatalog: provisionedProductArn`	Il prodotto fornito Amazon Resource Name (ARN)
`aws:servicecatalog:productArn`	L'ARN del prodotto da cui è stato lanciato il prodotto fornito

AWSi tag generati formano un namespace. Ad esempio, in un AWS CloudFormation modello, si definisce un insieme di risorse da distribuire insieme in un`stack`, dove `stack-name` è un nome descrittivo che si assegna per identificarlo. Se si esamina una chiave come**`aws:cloudformation:stack-name`**, ad esempio, si può vedere lo spazio dei nomi utilizzato per l'ambito, il parametro utilizza tre elementi: aws l'organizzazione, cloudformation il servizio e stack-name il parametro.

I tag definiti dall'utente possono anche utilizzare namespace e si consiglia di utilizzare un identificatore organizzativo come prefisso. Ciò consente di identificare rapidamente se un tag proviene dallo schema gestito o è definito da un servizio o uno strumento che si utilizza nel proprio ambiente.

Nel AWS white paper Establishing Your Cloud Foundation on, consigliamo un set di tag da implementare. È molto probabile che diverse aziende abbiano modelli consentiti diversi ed elenchi diversi per un determinato tag. Guardando l'esempio nella Tabella 3:

Tabella 3 — Stessa chiave di tag, regole di convalida dei valori diverse

Organizzazione	Chiave tag	Convalida dei valori dei tag	Esempio di valore dei tag
Azienda A	`CostCenter`	`5432, 5422, 5499`	`5432`
Compagnia B	`CostCenter`	`ABC*`	`ABC123`

Se questi due schemi si trovano in organizzazioni separate, non vi è alcun problema di conflitto di tag. Tuttavia, se questi due ambienti dovessero fondersi, i namespace potrebbero entrare in conflitto e la convalida diventerebbe più complessa. Questo scenario potrebbe sembrare improbabile, ma le aziende vengono acquisite o unite e vi sono altri scenari, ad esempio clienti che collaborano con un fornitore di servizi gestiti, un editore di giochi o un'azienda di capitali di rischio, in cui account di diverse organizzazioni fanno parte di un'organizzazione condivisa. AWS Utilizzando il nome aziendale come prefisso per definire un namespace univoco, è possibile evitare queste problematiche, come illustrato nella Tabella 4:

Tabella 4 — Uso dei namespace nelle chiavi dei tag

Organizzazione	Chiave tag	Convalida dei valori dei tag	Esempio di valore dei tag
Azienda A	`company-a :CostCenter`	`5432, 5422, 5499`	`5432`
Compagnia B	`company-b :CostCenter`	`ABC*`	`ABC123`

Nelle organizzazioni grandi e complesse in cui le aziende vengono acquisite e cedute regolarmente, questa situazione si verificherà più frequentemente. Con l'armonizzazione dei processi e delle pratiche delle nuove acquisizioni in tutto il gruppo, la situazione si risolve. Avere namespace distinti aiuta perché è possibile segnalare l'uso dei tag più vecchi e contattare i team competenti per adottare il nuovo schema. Un namespace può essere utilizzato anche per indicare un ambito o rappresentare un caso d'uso o un'area di responsabilità che è allineata ai proprietari dell'organizzazione.

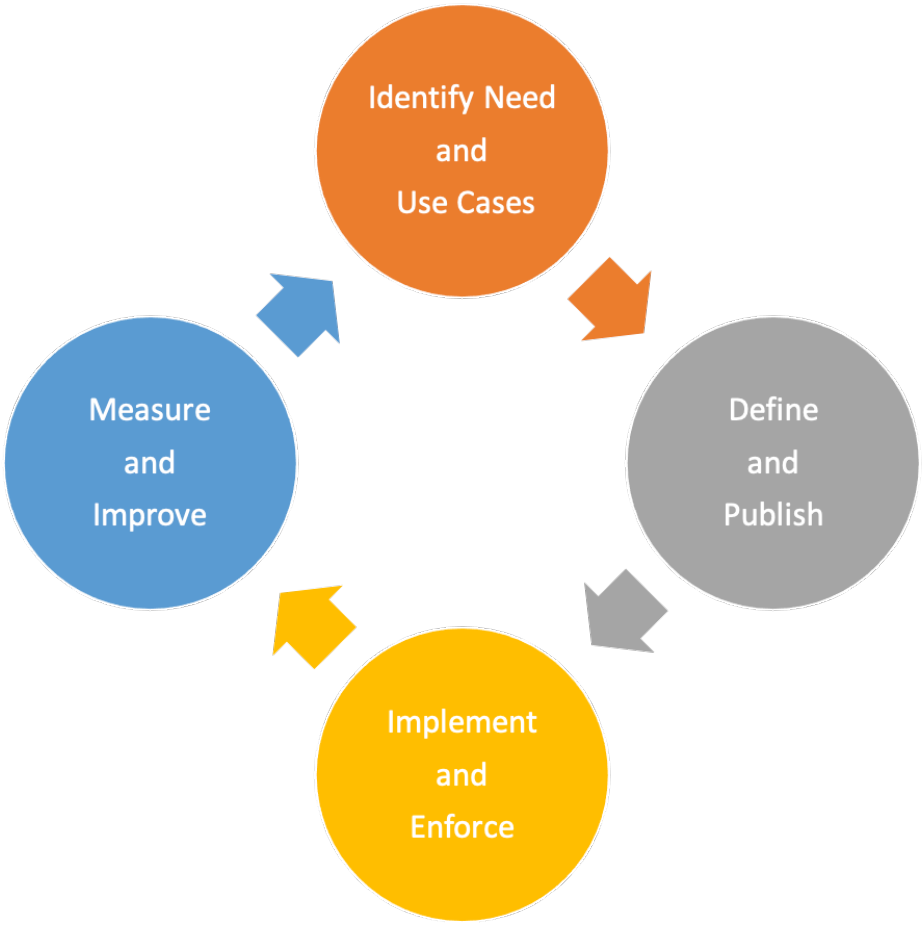
Tabella 5 — Esempio di ambito o ambito del caso d'uso all'interno delle chiavi dei tag

Caso d'uso	Chiave tag	Rationale	Valori consentiti
Classificazione dei dati	`example-inc:info-sec:data-classification`	Set di classificazione dei dati definito per la sicurezza delle informazioni	`sensitive`, `company-confidential`, `customer-identifiable`
Operazioni	`example-inc:dev-ops:environment`	Implementa la pianificazione degli ambienti di test e sviluppo	`development`, `staging`, `quality-assurance`, `production`
Disaster recovery	`example-inc:disaster-recovery:rpo`	Definire il Recovery Point Objective (RPO) per una risorsa	6h, 24h
Allocazione dei costi	`example-inc:cost-allocation:business-unit`	I team finanziari necessitano di report sui costi relativi all'utilizzo e alla spesa di ciascun team	`corporate`, `recruitment`, `support`, `engineering`

I tag sono semplici e flessibili. Sia la chiave che il valore del tag sono stringhe a lunghezza variabile e possono supportare un ampio set di caratteri. Per ulteriori informazioni sulle lunghezze e sui set di caratteri, consultate Etichettatura AWS delle risorse nella Guida generale. AWS I tag fanno distinzione tra maiuscole `costCenter` e minuscole, il che significa che `costcenter` sono chiavi di tag diverse. In diversi Paesi, l'ortografia di una parola potrebbe essere diversa, il che potrebbe influire sui tasti utilizzati. Ad esempio, negli Stati Uniti, si potrebbe definire una chiave come`costcenter`, ma nel Regno Unito `costcentre` potrebbe essere preferita. Si tratta di chiavi diverse dal punto di vista della codifica delle risorse. Definisci l'ortografia, le maiuscole e le minuscole e la punteggiatura come parte della tua strategia di tagging. Usa queste definizioni come riferimento per chiunque crei o gestisca risorse. Questo argomento viene discusso più dettagliatamente nella sezione successiva,Sviluppa la strategia di tagging.

Sviluppa la strategia di tagging

Come per molte pratiche operative, l'implementazione di una strategia di tagging è un processo di iterazione e miglioramento. Inizia in piccolo con la priorità immediata e amplia lo schema di tagging in base alle tue esigenze.



Iterazione e ciclo di miglioramento della strategia di etichettatura

Durante tutto questo processo, la proprietà è fondamentale per la responsabilità e il progresso. Poiché i tag possono essere utilizzati per una varietà di scopi, la strategia generale di etichettatura può essere suddivisa in aree di responsabilità all'interno di un'organizzazione. L'etichettatura consente un approccio programmatico alle attività che dipendono dalla caratterizzazione delle risorse. La gamma di parti interessate che possono trarre vantaggio dall'etichettatura dipenderà dalle dimensioni dell'organizzazione e dalle pratiche operative. Le organizzazioni più grandi possono trarre vantaggio dalla definizione chiara delle responsabilità dei team coinvolti nella creazione e nell'implementazione di una strategia di etichettatura. Alcune parti interessate possono essere responsabili dell'identificazione delle esigenze (definizione dei casi d'uso) in materia di etichettatura;

altre possono essere responsabili del mantenimento, dell'implementazione e del miglioramento della strategia di etichettatura.

Assegnando la proprietà, siete in una buona posizione per implementare singoli aspetti della strategia. Se del caso, questa titolarità può essere formalizzata come politica e documentata in una matrice di responsabilità (ad esempio, RACI: Responsible, Accountable, Consulted and Informed) o in un modello di responsabilità condivisa. Nelle organizzazioni più piccole, i team possono svolgere più ruoli in una strategia di etichettatura, dalla definizione dei requisiti all'implementazione e all'applicazione.

Definizione delle esigenze e dei casi d'uso

Inizia a sviluppare la tua strategia interagendo con le parti interessate che hanno l'esigenza fondamentale di utilizzare i metadati. Questi team definiscono i metadati con cui le risorse devono essere etichettate per supportare le loro attività, come la reportistica, l'automazione e la classificazione dei dati. Descrivono come le risorse devono essere organizzate e a quali politiche devono essere mappate. Esempi di ruoli e funzioni che queste parti interessate possono avere nelle organizzazioni includono:

- Finance e Line of Business devono comprendere il valore degli investimenti associandolo ai costi per dare priorità alle azioni da intraprendere per far fronte alle disparità. Comprendere il rapporto tra costo e valore generato aiuta a identificare le linee di business o le offerte di prodotti che non hanno avuto successo. Ciò porta a decisioni informate sulla continuazione del supporto, sull'adozione di un'alternativa (ad esempio, l'utilizzo di un'offerta SaaS o di un servizio gestito) o sul ritiro di un'offerta aziendale non redditizia.
- La governance e la conformità devono comprendere la categorizzazione dei dati (ad esempio, pubblici, sensibili o riservati), se un carico di lavoro specifico rientra o non rientra nell'ambito di controllo rispetto a uno standard o regolamento specifici e la criticità del servizio (indipendentemente dal fatto che il servizio o l'applicazione siano critici per l'azienda) per applicare controlli e supervisione appropriati, come autorizzazioni, politiche e monitoraggio.
- Le operazioni e lo sviluppo devono comprendere il ciclo di vita del carico di lavoro, le fasi di implementazione dei prodotti supportati e la gestione delle fasi di rilascio (ad esempio, sviluppo, test, divisione della produzione) e le relative priorità di supporto e i requisiti di gestione degli stakeholder. È inoltre necessario definire e comprendere compiti quali backup, applicazione di patch, osservabilità e deprecazione.

- Information Security (InfoSec) e Security Operations (SecOps) delineano quali controlli devono essere applicati e quali sono consigliati. InfoSec definisce normalmente l'implementazione dei controlli ed SecOps è generalmente responsabile della gestione di tali controlli.

A seconda del caso d'uso, delle priorità, delle dimensioni dell'organizzazione e delle pratiche operative, potresti aver bisogno della rappresentanza di vari team all'interno dell'organizzazione, come Finance (incluso Procurement), Information Security, Cloud Enablement e Cloud Operations. È inoltre necessaria la rappresentanza dei proprietari delle applicazioni e dei processi per funzioni quali l'applicazione di patch, il backup e il ripristino, il monitoraggio, la pianificazione dei lavori e il disaster recovery. Questi rappresentanti aiutano a definire, implementare e misurare l'efficacia della strategia di tagging. Dovrebbero basarsi sulla conoscenza delle parti interessate e dei relativi casi d'uso e condurre un seminario interfunzionale. Nel seminario, hanno la possibilità di condividere le loro prospettive e le loro esigenze e contribuire a definire una strategia globale. Esempi di partecipanti e del loro coinvolgimento in vari casi d'uso sono descritti più avanti in questo white paper.

Le parti interessate definiscono e convalidano inoltre le chiavi per i tag obbligatori e possono consigliare l'ambito per i tag opzionali. Ad esempio, i team finanziari potrebbero dover collegare una risorsa a un centro di costo interno, a un'unità aziendale o a entrambi. Pertanto, potrebbero richiedere che determinate chiavi di tag, come `CostCenter` e`BusinessUnit`, siano rese obbligatorie. I singoli team di sviluppo potrebbero decidere di utilizzare tag aggiuntivi per scopi di automazione, ad esempio `EnvironmentNameOptIn`, o`OptOut`.

Le principali parti interessate devono concordare l'approccio strategico di etichettatura e documentare le risposte alle domande relative alla conformità e alla governance, come ad esempio:

- Quali casi d'uso devono essere affrontati?
- Chi è responsabile dell'etichettatura delle risorse (implementazione)?
- Come vengono applicati i tag e quali metodi e automazione verranno utilizzati (proattivi o reattivi)?
- Come vengono misurati l'efficacia e gli obiettivi dei tag?
- Con che frequenza deve essere rivista la strategia di tagging?
- Chi promuove i miglioramenti? Come si fa?

Le funzioni aziendali, come Cloud Enablement, Cloud Business Office e Cloud Platform Engineering, possono quindi svolgere un ruolo di facilitatori nel processo di costruzione della strategia di tagging, contribuire a favorirne l'adozione e garantire la coerenza della sua applicazione misurando i progressi, rimuovendo gli ostacoli e riducendo gli sforzi duplicati.

Definizione e pubblicazione di uno schema di tagging

Utilizza un approccio coerente per etichettare AWS le tue risorse, sia per i tag obbligatori che per quelli facoltativi. Uno schema di etichettatura completo ti aiuta a raggiungere questa coerenza. I seguenti esempi possono aiutare a iniziare:

- Concordate i tag key obbligatori
- Definisci valori accettabili e convenzioni di denominazione dei tag (lettere maiuscole o minuscole, trattini o sottolineature, gerarchia e così via)
- I valori di conferma non costituirebbero informazioni di identificazione personale (PII)
- Decidi chi può definire e creare nuove chiavi di tag
- Concorda su come aggiungere nuovi valori di tag obbligatori e su come gestire i tag opzionali

Consulta la seguente tabella delle categorie di tag, che può essere utilizzata come base di riferimento per ciò che potresti includere nel tuo schema di etichettatura. È comunque necessario determinare la convenzione da utilizzare per la chiave del tag e quali valori sono consentiti per ciascuna di esse. Lo schema di tagging è il documento in cui lo definisci per il tuo ambiente.

Tabella 6 — Esempio di schema di etichettatura definitivo (parte 1)

Caso d'uso	Chiave tag	Rationale	Valori consentiti (elencati o prefisso/ sottofisso del valore)	Utilizzato per l'allocazione dei costi	Tipi di risorsa	Ambito	Obbligatorio
Allocazione dei costi	`example-inc:cost-allocation: ApplicationId`	Tieni traccia del costo rispetto al valore generato da ciascuna linea di business	`DataLakeX` , `RetailSiteX`	Y	Tutti	Tutti	Obbligatorio
Allocazione dei costi	`example-inc:cost-allocation: BusinessUnitId`	Monitora i costi per unità aziendale	`Architecture` , `DevOps`, `Finance`	Y	Tutti	Tutti	Obbligatorio
Allocazione dei costi	`example-inc:cost-allocation: CostCenter`	Monitora i costi per centro di costo	`123-*`	Y	Tutti	Tutti	Obbligatorio
Allocazione dei costi	`example-inc:cost-allocation :Owner`	Quale titolare del budget è responsabile di questo carico di lavoro	`Marketing` , `RetailSupport`	Y	Tutti	Tutti	Obbligatorio
Controllo degli	`example-inc:access`	Identifica SubCompon	`DB_Layer`, `Web Layer` ,	N	Tutti	Tutti	Facoltativo

Tabella 6 — Esempio di schema di tagging definitivo (parte 2)

Caso d'uso	Chiave tag	Rationale	Valori consentiti (elencati o prefisso/ sottofisso del valore)	Utilizzato per l'allocazione dei costi	Tipi di risorsa	Ambito	Obbligatorio
DevOps	`example-inc:operations: Owner`	Quale squadra/ squadra è responsabile della creazione e del mantenimento della risorsa	`Squad01`	N	Tutti	Tutti	Obbligatorio
Disaster recovery	`example-inc:disaster-recovery:rpo`	Definire il Recovery Point Objective (RPO) per una risorsa	`6h`, `24h`	N	S3, EBS	Prod	Obbligatorio
Classificazione dei dati	`example-inc:data: classification`	Classificazione dei dati per la conformità e la governance	`Public`, `Private`, `Confidential` , `Restricted`	N	S3, EBS	Tutti	Obbligatorio
Conformità	`example-inc:compliance: framework`	Identifica il framework di conformità a cui è soggetto il carico di lavoro	`PCI-DSS`, `HIPAA`	N	Tutti	Prod	Obbligatorio

Dopo aver definito lo schema di tagging, gestisci lo schema in un repository a controllo di versione accessibile a tutte le parti interessate per facilitare la consultazione e garantire aggiornamenti tracciabili. Questo approccio migliora l'efficienza e consente l'agilità.

AWS Organizations— Politiche relative ai tag

Le politiche AWS Organizations consentono di applicare ulteriori tipi di governance Account AWS all'interno dell'organizzazione. Una politica di tag consente di esprimere lo schema di tagging in formato JSON in modo che la piattaforma possa segnalare e, facoltativamente, applicare lo schema all'interno del proprio ambiente. AWS La politica dei tag definisce i valori accettabili per una chiave di tag su tipi di risorse specifici. Questa politica può assumere la forma di un elenco di valori o di un prefisso seguito da un carattere jolly ()*. L'approccio con prefisso semplice è meno rigoroso di un elenco discreto di valori, ma richiede meno manutenzione.

Gli esempi seguenti mostrano come definire una politica di etichettatura per convalidare i valori accettabili per una determinata chiave. Partendo dalla definizione tabulare intuitiva dello schema, è possibile trascrivere queste informazioni in una o più politiche di tag. È possibile utilizzare politiche separate per supportare la proprietà delegata oppure alcune politiche potrebbero essere applicate solo in scenari specifici.

ExampleInc- .json CostAllocation

Di seguito è riportato un esempio di politica dei tag che riporta i tag di allocazione dei costi:

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

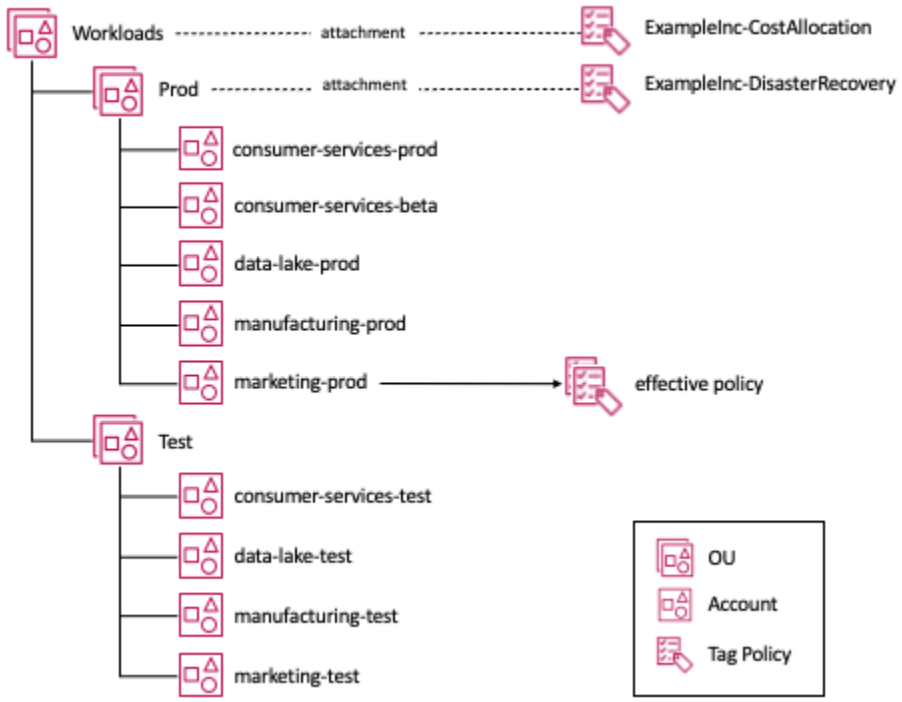
ExampleInc- .json DisasterRecovery

Di seguito è riportato un esempio di politica dei tag che riporta i tag di Disaster Recovery:

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

In questo esempio, la politica dei `ExampleInc-CostAllocation` tag è allegata all'`Workloads`unità organizzativa e pertanto si applica a tutti gli account sia dell'`Prod`unità

organizzativa che di quella `Test` secondaria. Analogamente, la politica sui `ExampleInc-DisasterRecovery` tag è allegata all'`Prod`unità organizzativa e pertanto si applica solo agli account al di sotto di questa unità organizzativa. Il white paper Organizing Your Environment Using Multiple Accounts analizza le strutture organizzative consigliate in modo più dettagliato.



Allegamento delle politiche relative ai tag a una struttura di unità organizzative

Osservando l'`marketing-prod`account nel diagramma, entrambe le politiche relative ai tag si applicano a questo account, quindi abbiamo il concetto di politica efficace, che è la convoluzione delle politiche di un determinato tipo che si applicano a un account. Se gestisci le tue risorse principalmente manualmente, puoi rivedere la politica in vigore visitando le politiche Resource Groups & Tag Editor:Tag nella console. Se utilizzi l'infrastruttura come codice (IaC) o lo scripting per gestire le risorse, puoi utilizzare la chiamata API. `AWS::Organizations::DescribeEffectivePolicy`

Implementazione e applicazione dei tag

In questa sezione, presenteremo gli strumenti disponibili per le seguenti strategie di gestione delle risorse: manuale, infrastructure-as code (IaC) e integrazione continua/distribuzione continua (CI/CD). La dimensione chiave di questi approcci è un tasso di implementazione sempre più frequente.

Risorse gestite manualmente

Si tratta in genere di carichi di lavoro che rientrano nelle fasi fondamentali o di migrazione dell'adozione. Spesso si tratta di semplici carichi di lavoro in gran parte statici creati utilizzando procedure scritte tradizionali o di carichi di lavoro migrati così come sono utilizzando strumenti come quelli CloudEndure provenienti da un ambiente locale. Gli strumenti di migrazione, come Migration Hub e CloudEndure, possono applicare tag come parte del processo di migrazione. Tuttavia, se i tag non sono stati applicati durante la migrazione originale o lo schema di etichettatura è cambiato da allora, il Tag Editor (una funzionalità diAWS Management Console) consente di cercare risorse utilizzando una varietà di criteri di ricerca e di aggiungere, modificare o eliminare tag in blocco. I criteri di ricerca possono includere risorse con o senza la presenza di un particolare tag o valore. L'API AWS Resource Tagging consente di eseguire queste funzioni a livello di codice.

Man mano che questi carichi di lavoro vengono modernizzati, vengono introdotti tipi di risorse come i gruppi di Auto Scaling. Questi tipi di risorse consentono una maggiore elasticità e una migliore resilienza. Il gruppo auto scaling gestisce le istanze Amazon EC2 per tuo conto, tuttavia potresti comunque desiderare che le istanze EC2 vengano etichettate in modo coerente con le risorse create manualmente. Un modello di lancio di Amazon EC2 fornisce i mezzi per specificare i tag che Auto Scaling deve applicare alle istanze che crea.

Quando le risorse di un carico di lavoro vengono gestite manualmente, può essere utile automatizzare l'etichettatura delle risorse. Sono disponibili varie soluzioni. Un approccio è quello di utilizzareRegole di AWS Config, che può verificare `required_tags` e quindi avviare una funzione Lambda per applicarli. Regole di AWS Configè descritto più dettagliatamente più avanti in questo white paper.

risorse gestite dall'infrastruttura come codice (IaC)

AWS CloudFormationfornisce un linguaggio comune per il provisioning di tutte le risorse dell'infrastruttura AWS nell'ambiente. CloudFormation i modelli sono file JSON o YAML che creano AWS risorse in modo automatizzato. Quando si creano AWS risorse utilizzando CloudFormation modelli, è possibile utilizzare la proprietà CloudFormation Resource Tags per applicare tag ai tipi di risorse supportati al momento della creazione. La gestione dei tag e delle risorse con IAc aiuta a garantire la coerenza.

Quando le risorse vengono create daAWS CloudFormation, il servizio applica automaticamente un set di tag AWS definiti alle risorse create dal AWS CloudFormation modello. Questi sono:

```
aws:cloudformation:stack-name
```

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

È possibile definire facilmente un gruppo di risorse in base allo AWS CloudFormation stack. Questi tag AWS definiti vengono ereditati dalle risorse create dallo stack. Tuttavia, per le istanze Amazon EC2 all'interno di un gruppo Auto Scaling, è `AWS::AutoScaling::AutoScalingGroup` TagPropertynecessario impostarlo nella definizione del gruppo Auto Scaling nel modello. AWS CloudFormation In alternativa, se utilizzi un modello di avvio EC2 con il gruppo Auto Scaling, puoi definire i tag nella sua definizione. Si consiglia di utilizzare i modelli di avvio EC2 con gruppi di Auto Scaling o con AWS un servizio container. Questi servizi possono contribuire a garantire l'etichettatura coerente delle istanze Amazon EC2 e supportano anche l'Auto Scaling su più tipi di istanze e opzioni di acquisto, che possono migliorare la resilienza e ottimizzare i costi di elaborazione.

AWS CloudFormationGli hook forniscono agli sviluppatori un mezzo per mantenere gli aspetti chiave delle loro applicazioni coerenti con gli standard della loro organizzazione. Gli hook possono essere configurati per fornire un avviso o impedire l'implementazione. Questa funzionalità è ideale per verificare gli elementi chiave di configurazione nei modelli, ad esempio se un gruppo di Auto Scaling è configurato per applicare tag definiti dal cliente a tutte le istanze Amazon EC2 che lancerà o per garantire che tutti i bucket Amazon S3 siano creati con le impostazioni di crittografia richieste. In entrambi i casi, la valutazione di questa conformità viene spostata alle fasi iniziali del processo di distribuzione, con accorgimenti preliminari alla distribuzione. AWS CloudFormation

AWS CloudFormationfornisce la capacità di rilevare quando una risorsa (vedere Risorse che supportano il rilevamento delle deviazioni) fornita da un modello è stata modificata e le risorse non corrispondono più alle configurazioni del modello previste. Questo fenomeno è noto come deriva. Se usi l'automazione per applicare tag alle risorse gestite tramite IAc, le stai modificando, introducendo drift. Quando si utilizza IaC, attualmente si consiglia di gestire eventuali requisiti di tagging come parte dei modelli IaC, implementare AWS CloudFormation hook e pubblicare set di regole AWS CloudFormation Guard che possono essere utilizzati dall'automazione.

risorse gestite dalla pipeline CI/CD

Con l'aumentare della maturità del carico di lavoro, è probabile che vengano adottate tecniche come l'integrazione continua e l'implementazione continua (CI/CD). Queste tecniche aiutano a ridurre il rischio di implementazione semplificando l'implementazione di piccole modifiche più frequentemente con una maggiore automazione dei test. Una strategia di osservabilità che rileva comportamenti imprevisti introdotti da una distribuzione può ripristinare automaticamente l'implementazione con un impatto minimo sull'utente. Quando si arriva alla fase di implementazione decine di volte al giorno,

l'applicazione retroattiva dei tag semplicemente non è più pratica. Tutto deve essere espresso sotto forma di codice o configurazione, deve essere controllato dalla versione e, ove possibile, testato e valutato prima dell'implementazione in produzione. Nel modello combinato di sviluppo e operazioni (DevOps), molte pratiche riguardano considerazioni operative sotto forma di codice e le convalidano nelle prime fasi del ciclo di vita dell'implementazione.

Idealmente, dovresti eseguire questi controlli il più presto possibile (come illustrato con gli AWS CloudFormation hook), in modo da avere la certezza che il AWS CloudFormation modello soddisfi le tue politiche prima che lascino il computer dello sviluppatore.

AWS CloudFormationGuard 2.0 offre i mezzi per scrivere regole di conformità preventive per tutto ciò che è possibile definire. CloudFormation Il modello è convalidato in base alle regole dell'ambiente di sviluppo. Chiaramente, questa funzionalità ha una vasta gamma di applicazioni, ma in questo white paper esamineremo solo alcuni esempi per garantire che venga sempre utilizzata `AWS::AutoScaling::AutoScalingGroup TagProperty`.

Di seguito è riportato un esempio di regola CloudFormation Guard:

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

rule tags_asg_automation_EnvironmentId when %all_asgs !empty {
    let required_tags = %all_asgs.Properties.Tags.*[
        Key == 'example-inc:automation:EnvironmentId' ]
    %required_tags[*] {
        PropagateAtLaunch == 'true'
        Value IN ['Prod', 'Dev', 'Test', 'Sandbox']
        <<Tag must have a permitted value
          Tag must have PropagateAtLaunch set to 'true'>>
    }
}

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

Nell'esempio di codice, filtriamo il modello per tutte le risorse del tipo `AutoScalingGroup` e quindi abbiamo due regole:

- **`tags_asg_automation_EnvironmentId`**- Verifica che un tag con questa chiave esista, che abbia un valore all'interno dell'elenco di valori consentito e che `PropagateAtLaunch` sia impostato su `true`
- **`tags_asg_costAllocation_CostCenter`**- Verifica che esista un tag con questa chiave, che abbia un valore che inizia con il valore del prefisso definito e che `PropagateAtLaunch` sia impostato su `true`

Applicazione

Come descritto in precedenza, Resource Groups & Tag Editor fornisce i mezzi per identificare dove le risorse non soddisfano i requisiti di tagging definiti nelle politiche di tag applicate alle unità organizzative dell'organizzazione. L'accesso allo strumento console Resource Groups & Tag Editor dall'interno di un account membro dell'organizzazione mostra le politiche che si applicano a quell'account e la risorsa all'interno dell'account che non soddisfa i requisiti della politica sui tag. Se si accede dall'account di gestione (e se Tag policies ha Access abilitato nei servizi sottoAWS Organizations), è possibile visualizzare la conformità alle politiche sui tag per tutti gli account collegati dell'organizzazione.

All'interno della stessa Tag Policy, puoi abilitare l'applicazione per tipi di risorse specifici. Nel seguente esempio di policy, abbiamo aggiunto l'applicazione in modo tale che tutte le risorse, di qualsiasi tipo`ec2:instance`, `ec2:volume` debbano essere conformi alla policy. Esistono alcune limitazioni note, ad esempio la presenza di un tag su una risorsa affinché possa essere valutata dalla politica dei tag. Per un elenco, consulta Risorse che supportano l'applicazione delle politiche sui tag.

ExampleInc-Allocazione dei costi. json

Di seguito è riportato un esempio di politica dei tag che riporta e/o applica i tag di allocazione dei costi:

```
{
  "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 Configè un servizio che consente di valutare, controllare e valutare le configurazioni delle AWS risorse (vedere Tipi di risorse supportati da AWS Config). Nel caso del tagging, possiamo usarlo per identificare le risorse prive di tag con chiavi specifiche, utilizzando la `required_tags` regola (fai riferimento ai tipi di risorse supportati da required_tags). Dall'esempio precedente, potremmo verificare l'esistenza della chiave su tutte le istanze Amazon EC2. Nei casi in cui la chiave non esiste, l'istanza verrà registrata come non conforme. Questo AWS CloudFormation modello descrive una AWS Config regola per verificare la presenza delle chiavi obbligatorie descritte nella tabella, su bucket Amazon S3, istanze Amazon EC2 e volumi 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
```

Per gli ambienti in cui le risorse vengono gestite manualmente, è possibile migliorare una AWS Config regola per aggiungere automaticamente la chiave del tag mancante alle risorse utilizzando una correzione automatica tramite una funzione. AWS Lambda Sebbene funzioni bene per i carichi di lavoro statici, è progressivamente meno efficace man mano che si inizia a gestire le risorse tramite IaC e pipeline di implementazione.

AWS Organizations— Le policy di controllo dei servizi (SCP) sono un tipo di politica organizzativa che è possibile utilizzare per gestire le autorizzazioni all'interno dell'organizzazione. Gli SCP offrono controllo centralizzato sulle autorizzazioni massime disponibili per tutti gli account dell'organizzazione o unità organizzativa (OU). Gli SCP influiscono solo sugli utenti e i ruoli gestiti da account che fanno parte dell'organizzazione. Sebbene non influiscano direttamente sulle risorse, limitano le autorizzazioni degli utenti e dei ruoli, incluse le autorizzazioni per l'etichettatura delle azioni. Per quanto riguarda l'etichettatura, gli SCP possono fornire una granularità aggiuntiva per l'applicazione dei tag oltre a quella fornita dalle politiche sui tag.

Nell'esempio seguente, la policy negherà le `ec2:RunInstances` richieste in cui il `example-inc:cost-allocation:CostCenter` tag non è presente.

Quanto segue è un SCP di negazione:

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

Non è possibile recuperare fin dalla progettazione l'effettiva politica di controllo del servizio che si applica a un account collegato. Laddove si imponga l'utilizzo di tag con SCP, è necessario che la documentazione sia disponibile per gli sviluppatori in modo che possano garantire che le loro risorse soddisfino le politiche applicate ai loro account. Fornire accesso in sola lettura agli CloudTrail eventi all'interno del proprio account può aiutare gli sviluppatori a eseguire il debug quando le loro risorse non sono conformi.

Misurare l'efficacia dei tag e apportare miglioramenti

Dopo aver implementato una strategia di tagging, è importante misurarne l'efficacia rispetto ai casi d'uso target. La misura dell'efficacia varierà in base al caso d'uso. Ad esempio:

- Attribuzione dei costi: è possibile misurare la copertura codificata delle risorse in base alla spesa utilizzando strumenti come AWS Cost Exploreril rapporto sui AWScosti e sull'utilizzo. Ad esempio, puoi tenere traccia della percentuale di risorse con o senza tag che generano addebiti, in particolare monitorando chiavi di tag specifiche.
- Automazione: potresti voler verificare se il risultato desiderato è stato raggiunto. Ad esempio, se le istanze Amazon EC2 non di produzione sono sospese al di fuori dell'orario di lavoro, verifica gli orari di inizio e fine delle istanze.

Resource Groups & Tag Editor all'interno dell'account di gestione offre funzionalità aggiuntive per analizzare la conformità alle politiche sui tag per tutti gli account collegati dell'organizzazione.

In base ai risultati della misurazione dell'efficacia dei tag, individuate se sono necessari miglioramenti o modifiche in uno qualsiasi dei passaggi, come la definizione dei casi d'uso, l'implementazione o l'applicazione dello schema di tagging. Apportate le modifiche necessarie e ripetete il ciclo fino a raggiungere l'efficacia desiderata. Nell'esempio con l'attribuzione dei costi, puoi considerare il miglioramento percentuale.

Poiché sono gli sviluppatori e gli operatori a dover eseguire l'effettiva etichettatura delle risorse, è fondamentale che se ne assumano la responsabilità. Questa non è l'unica responsabilità aggiuntiva che i team in genere si assumono nel loro percorso di AWS adozione. Sono importanti anche una maggiore responsabilità per la sicurezza e i costi di sviluppo e funzionamento delle loro applicazioni. Organizations utilizza spesso obiettivi e traguardi come mezzo per motivare l'adozione di nuove pratiche, quindi questo può valere anche in questo caso.

Casi d'uso dei tag

Argomenti

Tag per l'allocazione dei costi e la gestione finanziaria

Uno dei primi casi d'uso di etichettatura che le organizzazioni affrontano spesso è la visibilità e la gestione dei costi e dell'utilizzo. Di solito ci sono alcuni motivi per questo:

- In genere si tratta di uno scenario ben compreso e i requisiti sono ben noti. Ad esempio, i team finanziari vogliono vedere il costo totale dei carichi di lavoro e dell'infrastruttura che si estendono su più servizi, funzionalità, account o team. Un modo per ottenere questa visibilità dei costi consiste nell'etichettare in modo coerente le risorse.
- I tag e i relativi valori sono chiaramente definiti. Di solito, i meccanismi di allocazione dei costi esistono già nei sistemi finanziari di un'organizzazione, ad esempio il monitoraggio per centro di costo, unità aziendale, team o funzione organizzativa.
- Ritorno sull'investimento rapido e dimostrabile. È possibile tenere traccia delle tendenze di ottimizzazione dei costi nel tempo quando le risorse vengono etichettate in modo coerente, ad esempio per le risorse che sono state dimensionate correttamente, ridimensionate automaticamente o inserite in una pianificazione.

Capire come si sostengono i costi AWS consente di prendere decisioni finanziarie informate. Conoscere i costi sostenuti a livello di risorse, carico di lavoro, team o organizzazione migliora la comprensione del valore fornito al livello applicabile rispetto ai risultati aziendali raggiunti.

I team di progettazione potrebbero non avere esperienza nella gestione finanziaria delle proprie risorse. Affidare una persona con competenze specialistiche nella gestione AWS finanziaria, in grado di formare i team di progettazione e sviluppo sui fondamenti della gestione AWS finanziaria e creare un rapporto tra finanza e ingegneria per promuovere la cultura della, FinOps aiuterà a raggiungere risultati misurabili per l'azienda e incoraggerà i team a sviluppare tenendo conto dei costi. La definizione di buone pratiche finanziarie è trattata in modo approfondito dal Cost Optimization Pillar

del Well-Architected Framework, ma toccheremo alcuni dei principi fondamentali in questo white paper.

Tag di allocazione dei costi

L'allocazione dei costi si riferisce all'assegnazione o alla distribuzione dei costi sostenuti agli utenti o ai beneficiari di tali costi secondo un processo definito. Nel contesto di questo white paper, dividiamo l'allocazione dei costi in due tipi: showback e chargeback.

Gli strumenti e i meccanismi di showback aiutano ad aumentare la consapevolezza dei costi. Chargeback aiuta a recuperare i costi e favorisce la consapevolezza dei costi. Showback riguarda la presentazione, il calcolo e la rendicontazione degli addebiti sostenuti da un'entità specifica, ad esempio un'unità aziendale, un'applicazione, un utente o un centro di costo. Ad esempio: «il team di progettazione dell'infrastruttura si è occupato di X dollari di AWS spesa il mese scorso». Il chargeback riguarda l'addebito effettivo dei costi sostenuti a tali entità tramite processi contabili interni dell'organizzazione, come i sistemi finanziari o i voucher contabili. Ad esempio: «X $ sono stati detratti dal budget del team di progettazione dell'infrastruttura». AWS In entrambi i casi, etichettare le risorse in modo appropriato può aiutare ad allocare i costi a un'entità, con l'unica differenza se ci si aspetta che qualcuno effettui o meno un pagamento.

La governance finanziaria dell'organizzazione potrebbe richiedere una contabilità trasparente dei costi sostenuti a livello di applicazione, unità aziendale, centro di costo e team. L'esecuzione dell'attribuzione dei costi supportata dai tag di allocazione dei costi fornisce i dati necessari per attribuire con precisione i costi sostenuti da un'entità a partire da risorse adeguatamente etichettate.

- Responsabilità: assicuratevi che i costi siano assegnati ai responsabili dell'utilizzo delle risorse. Un singolo punto di assistenza o gruppo può essere responsabile della revisione e della rendicontazione delle spese.
- Trasparenza finanziaria: mostra una visione chiara delle allocazioni di liquidità verso l'IT creando dashboard efficaci e analisi dei costi significative per la leadership.
- Investimenti IT informati: monitora il ROI in base al progetto, all'applicazione o alla linea di business e consenti ai team di prendere decisioni aziendali migliori, ad esempio stanziando maggiori fondi per applicazioni che generano entrate.

In sintesi, i tag di allocazione dei costi possono aiutarti a dirti:

- Chi possiede la spesa ed è responsabile dell'ottimizzazione?

- Quale carico di lavoro, applicazione o prodotto è destinato alla spesa? Quale ambiente o palcoscenico?
- Quali aree di spesa stanno crescendo più rapidamente?
- Quanta spesa può essere detratta da un AWS budget in base alle tendenze passate?
- Qual è stato l'impatto degli sforzi di ottimizzazione dei costi su particolari carichi di lavoro, applicazioni o prodotti?

L'attivazione dei tag delle risorse per l'allocazione dei costi aiuta a definire le pratiche di misurazione all'interno dell'organizzazione che possono essere utilizzate per fornire la visibilità dell'AWSutilizzo e aumentare la trasparenza nella responsabilità delle spese. Si concentra inoltre sulla creazione di un livello di granularità appropriato per quanto riguarda la visibilità dei costi e dell'utilizzo e sull'influenza dei comportamenti di consumo del cloud attraverso la reportistica sull'allocazione dei costi e il monitoraggio dei KPI.

Creazione di una strategia di allocazione dei costi

Definizione e implementazione di un modello di allocazione dei costi

Crea account e struttura dei costi per le risorse in cui vengono impiegate. AWS Stabilisci la relazione tra i costi derivanti dalla AWS spesa, il modo in cui tali costi sono stati sostenuti e chi o cosa ha sostenuto tali costi. Le strutture di costo comuni si basano su AWS OrganizationsAccount AWS, ambienti ed entità all'interno delle organizzazioni, ad esempio una linea di business o un carico di lavoro. Le strutture dei costi possono essere basate su più attributi per consentire l'esame dei costi in diversi modi o a diversi livelli di granularità, ad esempio ripartendo i costi dei singoli carichi di lavoro in base alla linea di business in cui operano.

Quando scegli una struttura dei costi in linea con i risultati desiderati, valuta i meccanismi di allocazione dei costi in base alla facilità di implementazione rispetto alla precisione desiderata. Ciò potrebbe includere considerazioni relative alla responsabilità, alla disponibilità degli strumenti e ai cambiamenti culturali. I tre modelli più diffusi di allocazione dei costi da cui i AWS clienti di solito partono sono:

- Basato sull'account: questo modello richiede il minimo sforzo e offre un'elevata precisione per gli showback e i chargeback, ed è adatto per le organizzazioni che hanno una struttura di account definita (ed è coerente con le raccomandazioni del white paper Organizing Your AWS Environment Using Multiple Accounts). Ciò fornisce una chiara visibilità dei costi per account. Per la visibilità e l'allocazione dei costi, è possibile utilizzare AWS Cost Exploreri report sui costi e sull'utilizzo e i

AWSbudget per il monitoraggio e il monitoraggio dei costi. Questi strumenti forniscono opzioni di filtraggio e raggruppamento per. Account AWS Dal punto di vista dell'allocazione dei costi, questo modello non deve basarsi su un'etichettatura accurata delle singole risorse.

- Basato su unità aziendali o team: costi allocabili a team, unità aziendali o organizzazioni all'interno di un'azienda. Questo modello richiede uno sforzo moderato, offre un'elevata precisione per gli showback e i chargeback ed è adatto per le organizzazioni che hanno una struttura di account definita (in genere utilizzataAWS Organizations), con separazione tra vari team, applicazioni e tipi di carico di lavoro. Ciò offre una chiara visibilità dei costi tra team e applicazioni e, come ulteriore vantaggio, riduce il rischio di raggiungere le quote di servizio all'interno di un'unica AWS soluzione. Account AWS Ad esempio, ogni team può avere cinque account (`prod`,,, `staging` `testdev`,`sandbox`) e non ci sono due team e applicazioni che condivideranno lo stesso account. Con tale struttura, AWSCost Categories fornirà quindi la funzionalità per raggruppare gli account o altri tag («meta-tagging») in categorie, che possono essere tracciate negli strumenti citati nell'esempio precedente. È importante notare che AWS Organizations consente l'etichettatura di account e unità organizzative (OU), tuttavia questi tag non saranno applicabili per l'allocazione dei costi e i report di fatturazione (ovvero, non è possibile raggruppare o filtrare i costi per unità organizzative). AWS Cost Explorer AWS A tal fine è necessario utilizzare le Cost Categories.
- Basato su tag: questo modello richiede uno sforzo maggiore rispetto ai due precedenti e fornirà un'elevata precisione per gli showback e i chargeback a seconda dei requisiti e dell'obiettivo finale. Sebbene consigliamo vivamente di adottare le pratiche descritte nel white paper Organization Your AWS Environment Using Multiple Accounts, realisticamente i clienti si trovano spesso a dover affrontare strutture di account miste e complesse che richiedono tempo per migrare. L'implementazione di una strategia di tagging rigorosa ed efficace è la chiave in questo scenario, seguita dall'attivazione dei tag pertinenti per l'allocazione dei costi nella console Billing and Cost Management (AWS Organizationsinfatti, i tag possono essere attivati per l'allocazione dei costi solo dall'account Management Payer). Dopo l'attivazione dei tag per l'allocazione dei costi, è possibile utilizzare gli strumenti per la visibilità e l'allocazione dei costi menzionati nei metodi precedenti per gli showback e i chargeback. Tieni presente che i tag di allocazione dei costi non sono retroattivi e verranno visualizzati negli strumenti di reporting di fatturazione e monitoraggio dei costi solo dopo essere stati attivati per l'allocazione dei costi.

Per riassumere, se è necessario tenere traccia dei costi per unità aziendale, è possibile utilizzare AWSCost Categories per raggruppare di conseguenza gli account collegati all'interno AWS dell'organizzazione e visualizzare questo raggruppamento nei report di fatturazione. Quando si creano account separati per ambienti di produzione e non di produzione, è inoltre possibile filtrare i costi relativi agli ambienti utilizzando strumenti come AWS Cost Explorer, o tenere traccia di tali costi

utilizzando Budgets. AWS Infine, se il tuo caso d'uso richiede un monitoraggio dei costi più granulare, ad esempio per singoli carichi di lavoro o applicazioni, puoi etichettare di conseguenza le risorse all'interno di tali account, attivare le chiavi di tag per l'allocazione dei costi nell'account di gestione e quindi filtrare tale costo per chiavi di tag negli strumenti di reporting di fatturazione.

Definizione dei processi di rendicontazione dei costi e monitoraggio

Inizia con l'identificazione dei tipi di costi importanti per gli stakeholder interni (ad esempio, spesa giornaliera, costo per account, costo per X, costi ammortizzati). In questo modo, è possibile mitigare i rischi di bilancio associati a spese impreviste o anomale più rapidamente rispetto all'attesa della fattura definitiva. AWS I tag forniscono l'attribuzione che abilita questi scenari di reporting. Le informazioni ottenute dalla rendicontazione possono aiutarvi a mitigare l'impatto di spese anomale e impreviste sui budget finanziari. Quando si verifica un aumento imprevisto dei costi, è importante valutare se si è verificato un aumento imprevisto del valore fornito, in modo da determinare se e quali azioni sono necessarie.

Quando sviluppi una strategia di tagging per supportare l'allocazione dei costi, tieni presente i seguenti elementi:

- AWS Organizations- L'allocazione dei costi all'interno di più account può essere eseguita per account, gruppi di account o gruppo di tag creati per le risorse di tali account. I tag creati per le risorse che risiedono in singoli account in AWS Organizations possono essere utilizzati per l'allocazione dei costi solo dall'account di gestione.
- AWSAccount: l'allocazione dei costi all'interno di uno Account AWS può essere eseguita utilizzando dimensioni aggiuntive come servizi o regioni. È possibile etichettare ulteriormente le risorse all'interno di un account e lavorare con i gruppi di tali tag di risorse.
- Tag di allocazione dei costi: sia i tag creati dall'utente che i tag AWS generati possono essere attivati per l'allocazione dei costi, se necessario. L'attivazione dei tag per l'allocazione dei costi nella console di fatturazione (dell'account di gestioneAWS Organizations) facilita lo showback e i chargeback.
- Categorie di costo: le categorie di AWS costo consentono di raggruppare gli account e i tag di raggruppamento («meta-tagging») all'interno di un'AWSorganizzazione, il che offre inoltre la possibilità di analizzare i costi relativi a queste categorie tramite strumenti come AWS Budgets e Cost and AWS Cost Explorer Usage Report. AWS

Esecuzione di showback e chargeback per unità aziendali, team o organizzazioni all'interno dell'azienda

Attribuisci i costi utilizzando il processo di allocazione dei costi supportato dalla struttura dei costi e dai tag di allocazione dei costi. I tag possono essere utilizzati per fornire informazioni ai team che non sono direttamente responsabili del pagamento dei costi, ma sono responsabili per averli sostenuti. Questo approccio consente di conoscere il loro contributo alla spesa e il modo in cui tali costi vengono sostenuti. Effettua il chargeback ai team direttamente responsabili dei costi per recuperare le spese relative alle risorse che hanno consumato e per informare i team su tali costi e su come sono stati sostenuti.

Misurazione e diffusione dei KPI di efficienza o valore

Concorda una serie di parametri di costo unitario o KPI per misurare l'impatto dei tuoi investimenti nella gestione finanziaria nel cloud. Questo esercizio crea un linguaggio comune tra gli stakeholder tecnologici e aziendali e racconta una storia basata sull'economia, anziché una storia incentrata esclusivamente sulla spesa assoluta e aggregata. Per ulteriori informazioni, consultate questo blog che illustra come le metriche unitarie possono aiutare a creare l'allineamento tra le funzioni aziendali.

Allocazione di spese non allocabili

A seconda delle pratiche contabili dell'organizzazione, diversi tipi di addebito potrebbero richiedere un trattamento diverso. Identifica le risorse o le categorie di costo che non possono essere etichettate. A seconda dei servizi utilizzati e di quelli che si prevede di utilizzare, concordate i meccanismi su come trattare e misurare tali spese non allocabili. Ad esempio, controlla l'elenco delle risorse supportate da AWS Resource Groupsand Tag Editor nella Guida per l'utente di AWS Resource Groupsand Tags.

Un esempio comune di categoria di costo che non può essere etichettata sono alcune commissioni per sconti basati su impegni, come Reserved Instances (RI) e Savings Plans (SP). Sebbene le tariffe di abbonamento e le tariffe SP e RI non utilizzate non possano essere contrassegnate prima che compaiano negli strumenti di reporting di fatturazione, è possibile monitorare in seguito come gli sconti RI e SP si applicano agli account, alle risorse e ai relativi tag. AWS Organizations Ad esempio, AWS Cost Explorer è possibile esaminare il costo ammortizzato, raggruppare la spesa in base ai tag key pertinenti e applicare filtri pertinenti al proprio caso d'uso. Nel rapporto sui AWS costi e sull'utilizzo (CUR), puoi filtrare le righe che corrispondono all'utilizzo coperto dagli sconti RI e SP (leggi di più nella sezione sui casi d'uso della documentazione CUR) e selezionare le colonne che riguardano solo te. Ogni chiave tag attivata per l'allocazione dei costi verrà presentata in una colonna separata alla fine del rapporto CUR, in modo analogo a come viene presentata in altri report

di fatturazione precedenti, come il rapporto di allocazione dei costi mensile. Per ulteriori riferimenti, consulta i AWSWell-Architected Labs per esempi di come ottenere informazioni su costi e utilizzo dai dati CUR.

Creazione di report

Oltre agli AWS strumenti disponibili per agevolare gli showback e i chargeback, è disponibile una serie di altre soluzioni AWS create e di terze parti che possono aiutare a monitorare il costo delle risorse con tag e misurare l'efficacia della strategia di tagging. A seconda dei requisiti e dell'obiettivo finale dell'organizzazione, è possibile investire tempo e risorse nella creazione di soluzioni personalizzate o acquistare strumenti forniti da uno dei Management Tools Competency Partner. Cloud AWS Se decidi di creare il tuo strumento di allocazione dei costi da un'unica fonte di verità con parametri controllati pertinenti per l'azienda, il rapporto sui AWS costi e sull'utilizzo (CUR) fornisce i dati più dettagliati su costi e utilizzo e consente la creazione di dashboard di ottimizzazione personalizzate, consentendo il filtraggio e il raggruppamento per account, servizi, categorie di costi, tag di allocazione dei costi e molte altre dimensioni. Tra le soluzioni basate su CUR sviluppate da AWS che possono essere utilizzate come uno di questi strumenti, consulta Cloud Intelligence Dashboards sul sito Web Well-Architected AWS Labs.

Tag per operazioni e supporto

Un AWS ambiente avrà più account, risorse e carichi di lavoro con requisiti operativi diversi. I tag possono essere utilizzati per fornire contesto e indicazioni a supporto dei team operativi per migliorare la gestione dei servizi. I tag possono essere utilizzati anche per garantire la trasparenza della governance operativa delle risorse gestite.

Alcuni dei principali fattori che determinano una definizione coerente dei tag operativi sono:

- Per filtrare le risorse durante le attività di infrastruttura automatizzata. Ad esempio, durante la distribuzione, l'aggiornamento o l'eliminazione di risorse. Un altro è il ridimensionamento delle risorse per l'ottimizzazione dei costi e la riduzione dell'utilizzo fuori orario. Vedi la soluzione AWSInstance Scheduler per un esempio funzionante.
- Identificazione di risorse isolate o obsolete. Le risorse che hanno superato la durata di vita definita o che sono state segnalate per l'isolamento da meccanismi interni devono essere etichettate in modo appropriato in modo da assistere il personale di supporto nelle indagini. Le risorse obsolete devono essere etichettate prima dell'isolamento, dell'archiviazione e della cancellazione.
- Requisiti di supporto per un gruppo di risorse. Le risorse hanno spesso requisiti di supporto diversi, ad esempio questi requisiti possono essere negoziati tra i team o impostati come parte della

criticità di un'applicazione. Ulteriori indicazioni sui modelli operativi sono disponibili nell'Operational Excellence Pillar.

- Migliora il processo di gestione degli incidenti. Etichettando le risorse con tag che offrono una maggiore trasparenza nel processo di gestione degli incidenti, i team di supporto e gli ingegneri, nonché i team di Major Incident Management (MIM), possono gestire gli eventi in modo più efficace.
- Backup. I tag possono essere utilizzati anche per identificare la frequenza di backup delle risorse e la destinazione delle copie di backup o il luogo in cui ripristinare i backup. Linee guida prescrittive per gli approcci di Backup e ripristino su. AWS
- Applicazione di patch. L'applicazione di patch alle istanze mutabili in esecuzione AWS è fondamentale sia per la strategia generale di patching che per la correzione delle vulnerabilità zero-day. Una guida più approfondita sulla più ampia strategia di patching è disponibile nella guida prescrittiva. La correzione delle vulnerabilità zero-day viene discussa in questo blog.
- Osservabilità operativa. La traduzione di una strategia KPI operativa in tag di risorse aiuterà i team operativi a monitorare meglio se gli obiettivi vengono raggiunti per migliorare i requisiti aziendali. Lo sviluppo di una strategia KPI è un argomento a parte, ma tende a concentrarsi su un'azienda che opera in uno stato stazionario o su cui misurare l'impatto e i risultati del cambiamento. I KPI Dashboards (AWSWell-Architected labs) e l'Operations KPI Workshop (un servizio proattivo di Enterprise AWS Support) riguardano entrambi le prestazioni di misurazione in uno stato stazionario. L'articolo del blog di strategia AWS aziendale Measuring the Success of Your Transformation esplora la misurazione dei KPI per un programma di trasformazione, come la modernizzazione dell'IT o la migrazione dall'ambiente locale a. AWS

Attività di infrastruttura automatizzate

I tag possono essere utilizzati in un'ampia gamma di attività di automazione per la gestione dell'infrastruttura. L'uso di AWSSystems Manager, ad esempio, ti consentirà di gestire automazioni e runbook sulle risorse specificate dalla coppia chiave-valore definita che crei. Per i nodi gestiti, è possibile definire un set di tag per tracciare o indirizzare i nodi in base al sistema operativo e all'ambiente. È quindi possibile eseguire uno script di aggiornamento per tutti i nodi di un gruppo o esaminare lo stato di tali nodi. Le risorse di Systems Manager possono anche essere etichettate per affinare e tracciare ulteriormente le attività automatizzate.

L'automazione del ciclo di vita iniziale e finale delle risorse ambientali può fornire una significativa riduzione dei costi a qualsiasi organizzazione. Instance Scheduler on AWS è un esempio di soluzione in grado di avviare e arrestare istanze Amazon EC2 e Amazon RDS quando non sono necessarie.

Ad esempio, gli ambienti di sviluppo che utilizzano istanze Amazon EC2 o Amazon RDS che non devono essere eseguite nei fine settimana non sfruttano il potenziale di risparmio sui costi offerto dalla chiusura di tali istanze. Analizzando le esigenze dei team e dei loro ambienti e etichettando correttamente queste risorse per automatizzarne la gestione, puoi utilizzare il budget in modo efficace.

Un esempio di tag di pianificazione utilizzato dallo scheduler di istanze su un'istanza Amazon EC2:

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

Ciclo di vita dei carichi di lavoro

Verifica l'accuratezza dei dati operativi di supporto. Assicurati che vengano effettuate revisioni periodiche dei tag associati al ciclo di vita del carico di lavoro e che le parti interessate siano coinvolte in tali revisioni.

Tabella 7 — Rivedi i tag operativi come parte del ciclo di vita del carico di lavoro

Caso d'uso	Chiave tag	Rationale	Valori di esempio
Proprietario dell'account	`example-inc:account-owner:owner`	Il proprietario dell'account e delle relative risorse.	`ops-center` , `dev-ops`, `app-team`
Recensione del proprietario dell'account	`example-inc:account-owner:review`	Verifica che i dati relativi alla proprietà dell'account siano aggiornati e corretti.	<review date in the correct format defined in your tagging library>

Caso d'uso	Chiave tag	Rationale	Valori di esempio
Titolare dei dati	`example-inc:data-owner:owner`	Il proprietario dei dati che risiedono negli account.	`bi-team`, `logistics` , `security`
Recensione del proprietario dei dati	`example-inc:data-owner:review`	Verifica che i dettagli sulla proprietà dei dati siano aggiornati e corretti.	<review date in the correct format defined in your tagging library>

Assegnazione di tag agli account sospesi prima della migrazione all'unità organizzativa sospesa

Prima di sospendere un account e passare all'unità organizzativa sospesa, come descritto nel white paper Organization Your AWS Environment Using Multiple Accounts, è necessario aggiungere dei tag all'account per facilitare il tracciamento interno e il controllo del ciclo di vita di un account. Ad esempio, un URL relativo o un riferimento al ticket sul sistema di ticketing ITSM di un'organizzazione, che mostra l'audit trail di un'applicazione sospesa.

Tabella 8 - Aggiungi tag operativi quando il ciclo di vita del carico di lavoro entra in una nuova fase

Caso d'uso	Chiave tag	Rationale	Valori di esempio
Proprietario dell'account	`example-inc:account-owner:owner`	Il proprietario dell'account e delle relative risorse.	`ops-center` , `dev-ops`, `app-team`
Titolare dei dati	`example-inc:data-owner:owner`	Il proprietario dei dati che risiedono negli account.	`bi-team`, `logistics` , `security`
Data di sospensione	`example-inc:suspension:date`	La data in cui l'account è stato sospeso	<suspended date in the correct format defined in your tagging library>

Caso d'uso	Chiave tag	Rationale	Valori di esempio
Approvazione per la sospensione	`example-inc:suspension:approval`	Il link all'approvazione della sospensione dell'account	`workload/deprecation`

Gestione degli incidenti

I tag possono svolgere un ruolo fondamentale in tutte le fasi della gestione degli incidenti, a partire dalla registrazione degli incidenti, dalla definizione delle priorità, dall'indagine, dalla comunicazione, dalla risoluzione alla chiusura.

I tag possono indicare dove registrare un incidente, il team o i team che devono essere informati dell'incidente e la priorità di escalation definita. È importante ricordare che i tag non sono crittografati, quindi considera quali informazioni memorizzi in essi. Inoltre, nelle organizzazioni, nei team e nelle linee di reporting, le responsabilità cambiano, quindi valuta la possibilità di archiviare un collegamento a un portale sicuro in cui queste informazioni possano essere gestite in modo più efficace. Questi tag non devono essere esclusivi. Ad esempio, l'ID dell'applicazione potrebbe essere utilizzato per cercare i percorsi di escalation in un portale di gestione dei servizi IT. Accertatevi che nelle definizioni operative sia chiaro che questo tag viene utilizzato per diversi scopi.

I tag dei requisiti operativi possono anche essere dettagliati, per aiutare i responsabili degli incidenti e il personale operativo a perfezionare ulteriormente i propri obiettivi in risposta a un incidente o evento.

I link relativi (all'URL della Knowledge System Base) per runbook e playbook possono essere inclusi come tag per aiutare i team che hanno risposto a identificare il processo, la procedura e la documentazione corrispondenti.

Tabella 9 - Utilizza i tag operativi per informare la gestione degli incidenti

Caso d'uso	Chiave tag	Rationale	Valori di esempio
Gestione degli incidenti	`example-inc:incident-management:escalationlog`	Il sistema utilizzato dal team di supporto per registrare gli incidenti	`jira`, `servicenow` , `zendesk`

Caso d'uso	Chiave tag	Rationale	Valori di esempio
Gestione degli incidenti	`example-inc:incident-management:escalationpath`	Percorso di escalation	`ops-center` , `dev-ops`, `app-team`
Allocazione dei costi e gestione degli incidenti	`example-inc:cost-allocation:CostCenter`	Monitora i costi per centro di costo. Questo è un esempio di tag a doppio uso in cui il centro di costo viene utilizzato come codice applicativo per la registrazione degli incidenti	`123-*`
Pianificazione del backup	`example-inc:backup:schedule`	Pianificazione del backup della risorsa	`Daily`
Playbook/ Gestione degli incidenti	`example-inc:incident-management:playbook`	Playbook documentato	`webapp/incident/playbook`

Applicazione di patch

Organizations può automatizzare la propria strategia di patching per ambienti di elaborazione mutabili e mantenere le istanze mutabili in linea con la linea di base delle patch definita per quell'ambiente applicativo utilizzando Systems Manager Patch Manager e. AWS AWS Lambda Una strategia di etichettatura per le istanze mutabili all'interno di questi ambienti può essere gestita assegnando tali istanze a Patch Groups e Maintenance Windows. Vedi i seguenti esempi per una divisione Dev → Test → Prod. AWSsono disponibili linee guida prescrittive per la gestione delle patch delle istanze mutabili.

Tabella 10 - I tag operativi possono essere specifici dell'ambiente

Sviluppo	Gestione temporanea	Produzione

{
"Tags": [
{
"Key": "Maintenance
Window",
"ResourceId":
"i-012345678ab9ab1
11",
"ResourceType":
"instance",
"Value": "cron(30 23 ?
* TUE#1 *)"
},
{
"Key": "Name",
"ResourceId":
"i-012345678ab9ab2
22",
"ResourceType":
"instance",
"Value": "WEBAPP"
},
{
"Key": "Patch Group",
"ResourceId":
"i-012345678ab9ab3
33",
"ResourceType":
"instance",
"Value": "WEBAPP-DEV-
AL2"
}
]
}
	{
	"Tags": [
	{
	"Key": "Maintenance
	Window",
	"ResourceId":
	"i-012345678ab9ab4
	44",
	"ResourceType":
	"instance",
	"Value": "cron(30 23 ?
	* TUE#2 *)"
	},
	{
	"Key": "Name",
	"ResourceId":
	"i-012345678ab9ab5
	55",
	"ResourceType":
	"instance",
	"Value": "WEBAPP"
	},
	{
	"Key": "Patch Group",
	"ResourceId":
	"i-012345678ab9ab6
	66",
	"ResourceType":
	"instance",
	"Value": "WEBAPP-TEST-
	AL2"
	}
	]
	}
		{
		"Tags": [
		{
		"Key": "Maintenance
		Window",
		"ResourceId":
		"i-012345678ab9ab7
		77",
		"ResourceType":
		"instance",
		"Value": "cron(30 23 ?
		* TUE#3 *)"
		},
		{
		"Key": "Name",
		"ResourceId":
		"i-012345678ab9ab8
		88",
		"ResourceType":
		"instance",
		"Value": "WEBAPP"
		},
		{
		"Key": "Patch Group",
		"ResourceId":
		"i-012345678ab9ab9
		99",
		"ResourceType":
		"instance",
		"Value": "WEBAPP-PROD-
		AL2"
		}
		]
		}

Le vulnerabilità zero-day possono essere gestite anche definendo dei tag a complemento della strategia di patching. Per una guida dettagliata, consulta Evita le vulnerabilità zero-day applicando le patch di sicurezza lo stesso giorno utilizzando Systems AWS Manager.

Osservabilità operativa

L'osservabilità è necessaria per ottenere informazioni utili sulle prestazioni degli ambienti e aiutarvi a rilevare e analizzare i problemi. Ha anche uno scopo secondario che consente di definire e misurare gli indicatori chiave di prestazione (KPI) e gli obiettivi del livello di servizio (SLO) come l'uptime. Per la maggior parte delle organizzazioni, i KPI operativi importanti sono il tempo medio di rilevamento (MTTD) e il tempo medio di ripristino (MTTR) a seguito di un incidente.

In termini di osservabilità, il contesto è importante, poiché vengono raccolti i dati e quindi vengono raccolti i tag associati. Indipendentemente dal servizio, dall'applicazione o dal livello di applicazione su cui ti stai concentrando, puoi filtrare e analizzare per quel set di dati specifico. I tag possono essere utilizzati per automatizzare l'onboarding di CloudWatch Alarms in modo che i team giusti possano essere avvisati quando vengono superate determinate soglie metriche. Ad esempio, una chiave di tag `example-inc:ops:alarm-tag` e il relativo valore potrebbero indicare la creazione dell'allarme. CloudWatch Una soluzione che lo dimostra è descritta in Utilizzare i tag per creare e mantenere CloudWatch allarmi Amazon per le istanze Amazon EC2.

La configurazione di troppi allarmi può facilmente creare una tempesta di avvisi, quando un gran numero di allarmi o notifiche sovraccarica rapidamente gli operatori e ne riduce l'efficacia complessiva mentre gli operatori sono impegnati a classificare manualmente e a dare priorità ai singoli allarmi. È possibile fornire un contesto aggiuntivo per gli allarmi sotto forma di tag, il che significa che è possibile definire regole all'interno di Amazon EventBridge per garantire che venga prestata attenzione al problema originario anziché alle dipendenze a valle.

Il ruolo delle operazioni parallele DevOps viene spesso trascurato, ma per molte organizzazioni i team operativi centrali forniscono ancora una prima risposta fondamentale al di fuori del normale orario lavorativo. (Maggiori dettagli su questo modello sono disponibili nel white paper Operational Excellence.) A differenza del DevOps team responsabile del carico di lavoro, in genere non dispone della stessa conoscenza approfondita, quindi il contesto fornito dai tag all'interno di dashboard e avvisi può indirizzarli al runbook corretto per il problema o avviare un runbook automatizzato (consulta il post del blog Automating Amazon Alarms with). CloudWatch AWS Systems Manager

Tag per la sicurezza dei dati, la gestione del rischio e il controllo degli accessi

Organizations ha esigenze e obblighi diversi da soddisfare per quanto riguarda la gestione appropriata dell'archiviazione e dell'elaborazione dei dati. La classificazione dei dati è un importante

precursore per diversi casi d'uso, come il controllo degli accessi, la conservazione dei dati, l'analisi dei dati e la conformità.

Sicurezza dei dati e gestione dei rischi

All'interno di un AWS ambiente, probabilmente avrai account con requisiti di conformità e sicurezza diversi. Ad esempio, potreste avere una sandbox per sviluppatori e un account che ospita l'ambiente di produzione per un carico di lavoro altamente regolamentato, come l'elaborazione dei pagamenti. Isolandoli in diversi account, è possibile applicare controlli di sicurezza distinti, limitare l'accesso ai dati sensibili e ridurre l'ambito di controllo per i carichi di lavoro regolamentati.

L'adozione di un unico standard per tutti i carichi di lavoro può comportare delle sfide. Sebbene molti controlli si applichino allo stesso modo in un ambiente, alcuni controlli sono eccessivi o irrilevanti per gli account che non devono soddisfare specifici quadri normativi e per gli account in cui non saranno mai presenti dati personali identificabili (ad esempio, una sandbox per sviluppatori o account di sviluppo del carico di lavoro). Ciò porta in genere a risultati di sicurezza falsi positivi che devono essere valutati e chiusi senza alcuna azione, il che distoglie lo sforzo dai risultati da esaminare.

Tabella 11 — Esempi di tag per la sicurezza dei dati e la gestione del rischio

Caso d'uso	Chiave tag	Rationale	Valori di esempio
Gestione degli incidenti	`example-inc:incident-management:escalationlog`	Il sistema utilizzato dal team di supporto per registrare gli incidenti	`jira`, `servicenow` , `zendesk`
Gestione degli incidenti	`example-inc:incident-management:escalationpath`	Percorso di escalation	`ops-center` , `dev-ops`, `app-team`
Classificazione dei dati	`example-inc:data:classification`	Classificazione dei dati per la conformità e la governance	`Public`, `Private`, `Confidential` , `Restricted`
Conformità	`example-inc:compliance:framework`	Identifica il framework di conformità a cui è	`PCI-DSS`, `HIPAA`

Caso d'uso	Chiave tag	Rationale	Valori di esempio
		soggetto il carico di lavoro	

La gestione manuale di diversi controlli in un AWS ambiente richiede molto tempo ed è soggetta a errori. Il passaggio successivo consiste nell'automatizzare l'implementazione dei controlli di sicurezza appropriati e configurare l'ispezione delle risorse in base alla classificazione di tale account. Applicando tag agli account e alle risorse al loro interno, l'implementazione dei controlli può essere automatizzata e configurata in modo appropriato per il carico di lavoro.

Esempio:

Un carico di lavoro include un bucket Amazon S3 con il `example-inc:data:classification` tag con il valore. `Private` L'automazione degli strumenti di sicurezza implementa una AWS Config regola `s3-bucket-public-read-prohibited` che controlla le impostazioni Block Public Access del bucket Amazon S3, la policy del bucket e l'elenco di controllo dell'accesso al bucket (ACL), confermando che la configurazione del bucket è appropriata per la classificazione dei dati. Per garantire che il contenuto del bucket sia coerente con la classificazione, Amazon Macie può essere configurato per verificare la presenza di informazioni di identificazione personale (PII). Il blog Using Amazon Macie to Validate S3 Bucket Data Classification esplora questo modello in modo più approfondito.

Alcuni ambienti normativi, come quello assicurativo e sanitario, potrebbero essere soggetti a politiche obbligatorie di conservazione dei dati. La conservazione dei dati tramite tag, combinata con le policy del ciclo di vita di Amazon S3, può essere un modo semplice ed efficace per definire le transizioni degli oggetti verso un livello di storage diverso. Le regole del ciclo di vita di Amazon S3 possono essere utilizzate anche per far scadere gli oggetti per l'eliminazione dei dati dopo la scadenza del periodo di conservazione obbligatorio. Per una guida approfondita su questo processo, consulta Semplifica il ciclo di vita dei dati utilizzando i tag degli oggetti con Amazon S3 Lifecycle.

Inoltre, durante la valutazione o la risoluzione di problemi di sicurezza, i tag possono fornire all'investigatore un contesto importante che aiuta a qualificare il rischio e a coinvolgere i team appropriati per indagare o mitigare i risultati.

Tag per la gestione delle identità e il controllo degli accessi

Quando si gestisce il controllo degli accessi in un AWS ambiente conAWS IAM Identity Center, i tag possono abilitare diversi modelli di scalabilità. È possibile applicare diversi modelli di delega, alcuni

basati sull'etichettatura. Li affronteremo individualmente e forniremo collegamenti per ulteriori letture su ciascuno di essi.

ABAC per risorse individuali

Gli utenti e i ruoli IAM Identity Center supportano il controllo degli accessi basato sugli attributi (ABAC), che consente di definire l'accesso alle operazioni e alle risorse in base ai tag. ABAC aiuta a ridurre la necessità di aggiornare le politiche di autorizzazione e consente di basare l'accesso sugli attributi dei dipendenti presenti nell'elenco aziendale. Se state già utilizzando una strategia multi-account, ABAC può essere utilizzato in aggiunta al controllo degli accessi basato sui ruoli (RBAC) per fornire a più team che operano sullo stesso account un accesso granulare a risorse diverse. Ad esempio, gli utenti di IAM Identity Center o i ruoli IAM possono includere condizioni per limitare l'accesso a istanze Amazon EC2 specifiche che altrimenti dovrebbero essere elencate esplicitamente in ciascuna policy per potervi accedere.

Poiché un modello di autorizzazione ABAC dipende dai tag per l'accesso alle operazioni e alle risorse, è importante fornire barriere per prevenire accessi involontari. Gli SCP possono essere utilizzati per proteggere i tag in tutta l'organizzazione, consentendone la modifica solo in determinate condizioni. I blog Protezione dei tag delle risorse utilizzati per l'autorizzazione utilizzando una policy di controllo dei servizi in AWS Organizations e Limiti delle autorizzazioni per le entità IAM forniscono informazioni su come implementarla.

Laddove le istanze Amazon EC2 di lunga durata vengono utilizzate per supportare pratiche operative più tradizionali, questo approccio può essere utilizzato, il blog Configure IAM Identity Center ABAC for Amazon EC2 instances and Systems Manager Session Manager tratta in modo più dettagliato questa forma di controllo degli accessi basato sugli attributi. Come accennato in precedenza, non tutti i tipi di risorse supportano l'etichettatura e, tra quelli che lo fanno, non tutti supportano l'applicazione tramite politiche di tag, quindi è una buona idea valutarlo prima di iniziare a implementare questa strategia su unAccount AWS.

Per informazioni sui servizi che supportano ABAC, consulta AWSServizi compatibili con IAM.

Conclusioni

AWSle risorse possono essere etichettate per vari scopi, dall'implementazione di una strategia di allocazione dei costi al supporto dell'automazione o all'autorizzazione dell'accesso alle risorse. AWS L'implementazione di una strategia di tagging può essere difficile per alcune organizzazioni, a causa del numero di gruppi di stakeholder coinvolti e di considerazioni come l'approvvigionamento dei dati e la governance dei tag.

In questo white paper, abbiamo delineato le raccomandazioni relative alla progettazione e all'implementazione di una strategia di tagging in un'organizzazione basata su pratiche operative, casi d'uso definiti, parti interessate coinvolte nel processo e strumenti e servizi forniti da. AWS Quando si tratta di una strategia di tagging, si tratta di un processo di iterazione e miglioramento, in cui si parte in piccolo dalla priorità immediata, si identificano i casi d'uso pertinenti all'interno dell'organizzazione e quindi si implementa e amplia lo schema di tagging in base alle proprie esigenze, misurando e migliorando continuamente l'efficacia. Abbiamo sottolineato che un set ben definito di tag all'interno della tua organizzazione ti consentirà di mettere in relazione AWS l'utilizzo e il consumo con i team responsabili delle risorse e dello scopo aziendale per cui esistono, al fine di allinearli alla strategia e al valore dell'organizzazione.

Fattori determinanti

I contributori a questo documento includono:

- Chris Pates, Responsabile tecnico tecnico senior, Amazon Web Services
- Vijay Shekhar Rao, responsabile del supporto aziendale, Amazon Web Services
- Nataliya Godunok, responsabile tecnico senior, Amazon Web Services
- Yogish Kutkunje Pai, architetto senior delle soluzioni, Amazon Internet Services Private Limited
- Jamie Ibbs, Responsabile tecnico tecnico senior, Amazon Web Services

Approfondimenti

Per ulteriori informazioni, fare riferimento a

- AWSre:Invent 2020: Working backwards: l'approccio di Amazon all'innovazione
- AWSGuida prescrittiva: applicazione automatica delle patch per istanze mutabili nel cloud ibrido utilizzando Systems Manager AWS
- AWSCentro di architettura

AWSWell-Architected

- AWSFramework Well-Architected
- Pilastro dell'eccellenza operativa - AWS Well-Architected Framework
- Piano per il disaster recovery (DR) - Pilastro dell'affidabilità AWS Well-Architected
- Pilastro dell'ottimizzazione dei costi - AWS Well-Architected Framework
- AWSWell-Architected Labs: AWS abilita i tag di allocazione dei costi generati
- AWSWell-Architected Labs: politiche sui tag
- AWSWell-Architected LabsAWS: libreria di query CUR

AWSblog

- AWS HealthAware: personalizza AWS Health gli avvisi per gli account aziendali e personali AWS
- Come etichettare automaticamente le risorse Amazon EC2 in risposta agli eventi delle API
- AWSTag di allocazione dei costi generato e definito dall'utente
- Etichettatura e rendicontazione dei costi con AWS Organizations
- Applicazione di patch alle istanze di Windows EC2 utilizzando Patch Manager AWS Systems Manager
- Evita le vulnerabilità zero-day applicando le patch di sicurezza lo stesso giorno utilizzando AWS Systems Manager

Documentazione di AWS

- Utilizzo dei tag di allocazione dei costi e della gestione e della gestione dei costi AWS Billing and Cost Management

- Cosa sono i report di AWS costi e utilizzo
- AWS Resource Groups Documentazione di riferimento delle API
- Come posso utilizzare i tag delle policy IAM per limitare il modo in cui è possibile creare un'istanza EC2 o un volume EBS?
- Modelli di aggiornamento mutabili e immutabili

Other (Altro)

- Bryar, C. e Carr, B. (2021). Lavorare a ritroso: approfondimenti, storie e segreti da Inside Amazon. Londra Macmillan.
- AWS CloudFormationGuardia () GitHub

Revisioni del documento

Per ricevere una notifica sugli aggiornamenti del white paper, è possibile iscriversi al feed RSS.

Modifica	Descrizione	Data
Aggiornamento minore	Aggiornamenti alla gestione delle identità	30 marzo 2023
Revisione minore	Riferimento aggiornato in ABAC per le singole risorse.	24 febbraio 2023
Revisione minore	Guida aggiornata per allinears i alle best practice IAM. Per ulteriori informazioni, consulta la sezione Best practice per la sicurezza in IAM	6 febbraio 2023
Revisione principale	È stato aggiunto un riferimento più specifico per i tipi di risorse supportati dalla AWS Config regola`required_tags` .	18 gennaio 2023
Revisione principale	Aggiornato per includere le pratiche e le funzionalità di servizio più recenti, in particola re nell'area dell'identità.	29 settembre 2022
Aggiornamento minore	Formattazione fissa della tabella nella versione PDF.	25 aprile 2022
Revisione principale	Struttura del documento aggiornata e sezioni ampliate sulla strategia di etichetta tura e sui casi d'uso. Sono state aggiunte ulteriori linee guida prescrittive basate sugli	22 aprile 2022

	strumenti, le tecniche e le risorse disponibili più recenti.	
Pubblicazione iniziale	Whitepaper pubblicato per la prima volta.	1 dicembre 2018

> **Note**
>
> Per iscriverti agli aggiornamenti RSS, devi avere un plugin RSS abilitato per il browser che stai utilizzando.

Note

I clienti hanno la responsabilità di effettuare la propria valutazione indipendente delle informazioni contenute nel presente documento. Questo documento: (a) è solo a scopo informativo, (b) rappresenta le attuali offerte e pratiche di AWS prodotto, che sono soggette a modifiche senza preavviso, e (c) non crea alcun impegno o assicurazione da parte AWS delle sue affiliate, fornitori o licenzianti. AWSi prodotti o i servizi sono forniti «così come sono» senza garanzie, dichiarazioni o condizioni di alcun tipo, esplicite o implicite. Le responsabilità e le responsabilità dei AWS propri clienti sono regolate da AWS accordi e il presente documento non fa parte di, né modifica, alcun accordo tra AWS e i suoi clienti.

Glossario per AWS

Per la terminologia AWS più recente, consultare il glossario AWS nella documentazione di riferimento per Glossario AWS.

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.