Creazione di barriere e monitoraggio degli URL predefiniti

# AWS Linee guida prescrittive

# AWS Linee guida prescrittive: Creazione di barriere e monitoraggio degli URL predefiniti

# Table of Contents

Introduzione ..... 1
Destinatari principali ..... 1
Obiettivi ..... 1
Prerequisiti ..... 2
Panoramica delle impostazioni predefinite URLs ..... 3
Motivazioni per l'utilizzo di richieste predefinite ..... 4
Confronto con credenziali temporanee AWS STS ..... 5
Confronto con soluzioni basate esclusivamente sulla firma ..... 5
Identificazione delle richieste predefinite ..... 7
Identificazione delle richieste che hanno utilizzato un URL predefinito ..... 7
Identificazione di altri tipi di richieste predefinite ..... 8
Identificazione dei modelli di richiesta ..... 8
Le migliori pratiche per l'utilizzo di richieste predefinite ..... 13
Le migliori pratiche di base ..... 13
Applica il principio del privilegio minimo ..... 13
Implementa un perimetro di dati ..... 14
Guardrail aggiuntivi ..... 14
Guardrail per S3:SignatureAge ..... 14
Politiche di controllo delle risorse ..... 18
Guardrail per S3:AuthType ..... 19
Combinazione di guardrail ed eccezioni predefiniti con altri guardrail ..... 22
Limitazioni a S3:SignatureAge ..... 22
Indirizzare i bucket su larga scala ..... 23
Registrazione delle interazioni e delle mitigazioni ..... 24
Mitigazioni ..... 24
Domande frequenti ..... 26
È possibile utilizzare una richiesta prefirmata più volte? È un rischio per la sicurezza? ..... 26
Una richiesta predefinita può essere utilizzata da un utente diverso dall'utente previsto? ..... 26
Un utente autorizzato può utilizzare una richiesta predefinita per esfiltrare i dati? ..... 26
Posso negare l'accesso da un URL predefinito se sospetto che sia stato condiviso in modo non autorizzato? ..... 27
Risorse ..... 29
Documentazione Amazon S3 ..... 29
Altri riferimenti ..... 8

Appendice A: Come Servizi AWS usare presigned URLs ..... 30
Console Amazon S3 ..... 30
Amazon S3 Object Lambda ..... 31
AWS Lambda Interregione CopyObject ..... 32
AWS Lambda GetFunction ..... 32
Amazon ECR ..... 33
Amazon Redshift Spectrum ..... 33
Amazon SageMaker AI Studio ..... 34
Appendice B: Come influiscono i controlli predefiniti URLs Servizi AWS ..... 35
Guardrail per s3:SignatureAge ..... 35
Guardrail per S3:authType quando non si utilizzano restrizioni di rete ..... 35
Cronologia dei documenti ..... 37
Glossario ..... 38
# ..... 38
A ..... 39
B ..... 42
C ..... 44
D ..... 47
E ..... 51
F ..... 53
G ..... 55
H ..... 56
I ..... 58
L ..... 60
M ..... 62
O ..... 66
P ..... 69
Q ..... 71
R ..... 72
S ..... 75
T ..... 79
U ..... 80
V ..... 81
W ..... 81
Z ..... 82
..... lxxxiv

# Creazione di barriere e monitoraggio per i predefiniti URLs

Ryan Baker, Amazon Web Services ()AWS

Agosto 2025 (cronologia dei documenti)

La sicurezza è una preoccupazione fondamentale per tutte le aziende e un pilastro fondamentale di AWS Well-Architected Framework. In qualità di ingegnere della sicurezza, vorrai implementare barriere amministrative in linea con i requisiti di controllo organizzativo. Nel AWS Well-Architected Framework, i guardrail definiscono i confini che limitano l'attività.

Questa guida fornisce informazioni di base e best practice per l'utilizzo di oggetti predefiniti URLs, utilizzati con oggetti Amazon Simple Storage Service (Amazon S3). Le impostazioni predefinite URLs consentono agli utenti o alle applicazioni che hanno accesso a credenziali valide di generare richieste firmate in anticipo e accettate fino a un orario di scadenza definito. Un caso d'uso comune di presigned URLs consiste nell'estendere l'accesso a oggetti o risorse condividendo queste richieste. Le richieste predefinite condivise vengono generate da sistemi o utenti che dispongono dei diritti per eseguire una richiesta specifica e possono quindi essere inviate ad altri sistemi o utenti per estendere la capacità di eseguire la stessa richiesta.

In questa guida imparerai:

- I concetti di preimpostato URLs
- Casi d'uso per il preimpostato URLs
- Guardrail consigliati e opzionali
- Opzioni di monitoraggio
- Esempi di utilizzo di presigned Servizi AWS URLs

## Destinatari principali

Questa guida è destinata agli architect e agli ingegneri della sicurezza responsabili dell'implementazione dei controlli di sicurezza nel Cloud AWS.

## Obiettivi

In qualità di ingegnere della sicurezza, vuoi conoscere il modo in cui i costruttori di soluzioni implementano la sicurezza e il tipo di accesso di cui dispongono gli utenti finali. Questa guida tratta

un tipo di accesso, predefinito URLs, che viene spesso utilizzato con Amazon S3. Presigned URLs offre ai costruttori opzioni per collegare in modo efficiente i meccanismi di autenticazione.

In Amazon S3, i predefiniti URLs rappresentano una categoria unica di richieste. I tecnici della sicurezza possono monitorare e gestire queste richieste per garantire che vengano utilizzate solo dove appropriato e necessario. L'obiettivo di questa guida è aiutare gli ingegneri della sicurezza a fornire questo tipo di supervisione di alto livello.

Dopo aver letto questa guida, dovresti capire cos'è un URL predefinito, quando viene utilizzato in genere e le motivazioni del suo utilizzo.

## Prerequisiti

Se la tua azienda non ha definito una politica di sicurezza, obiettivi di controllo o standard, come descritto nella guida Implementing security controls on AWS, ti consigliamo di completare tali attività di governance prima di procedere con questa guida.

Prima di iniziare, dovresti anche conoscere le migliori pratiche consigliate e facoltative per il controllo e il monitoraggio. Per ulteriori informazioni, consulta:

- Politiche di controllo dei servizi (AWS Organizations documentazione)
- Politiche di controllo delle risorse (AWS Organizations documentazione)
- Politiche Bucket per Amazon S3 (documentazione Amazon S3)
- Registrazione delle richieste con registrazione degli accessi al server (documentazione Amazon S3)
- Registrazione delle chiamate API Amazon S3 AWS CloudTrail utilizzando (documentazione Amazon S3)

# Panoramica delle impostazioni predefinite URLs

Un URL predefinito è un tipo di richiesta HTTP riconosciuta dal servizio AWS Identity and Access Management (IAM). Ciò che differenzia questo tipo di richiesta da tutte le altre AWS richieste è il parametro di X-Amz-Expires query. Come per le altre richieste autenticate, le richieste URL prefirmate includono una firma. Per le richieste URL prefirmate, questa firma viene trasmessa in. `X-Amz-Signature` La firma utilizza le operazioni crittografiche Signature Version 4 per codificare tutti gli altri parametri della richiesta.

> **Note**
>
> - La versione 2 di Signature è attualmente in fase di obsolescenza, ma in alcuni casi è ancora supportata. Regioni AWS Questa guida si applica alla firma della versione 4 di Signature.
> - Il servizio di ricezione potrebbe elaborare intestazioni non firmate, ma il supporto per questa opzione è limitato e mirato, in linea con le migliori pratiche. Salvo diversa indicazione, si supponga che tutte le intestazioni debbano essere firmate affinché una richiesta venga accettata.

Il `X-Amz-Expires` parametro consente di elaborare una firma come valida con una deviazione maggiore dalla data e ora codificata. Altri aspetti della validità della firma vengono ancora valutati. Le credenziali di firma, se temporanee, non devono essere scadute al momento dell'elaborazione della firma. Le credenziali di firma devono essere allegate a un principale IAM che disponga di un'autorizzazione sufficiente al momento dell'elaborazione.

Le prefirmate URLs sono un sottoinsieme di richieste prefirmate

Un URL predefinito non è l'unico metodo per firmare una richiesta per un periodo futuro. Amazon S3 supporta anche le richieste POST, anch'esse generalmente predefinite. Una firma POST predefinita consente caricamenti conformi a una politica firmata e ha una data di scadenza incorporata in tale politica.

Le firme per le richieste possono avere date future, sebbene ciò non sia comune. Finché le credenziali sottostanti sono valide, l'algoritmo di firma non proibisce appuntamenti futuri. Tuttavia, queste richieste non possono essere elaborate con successo fino alla loro finestra temporale valida, il che rende impraticabili le datazioni future per la maggior parte dei casi d'uso.

Cosa consente una richiesta predefinita?

Una richiesta prefirmata può consentire solo azioni consentite dalle credenziali utilizzate per firmare la richiesta. Se le credenziali negano in modo implicito o esplicito l'azione specificata dalla richiesta prefirmata, la richiesta prefirmata viene rifiutata al momento dell'invio. Questo vale per quanto segue:

- Politiche di sessione associate alle credenziali
- Politiche basate sull'identità associate al principale associato alle credenziali
- Politiche relative alle risorse che influiscono sulla sessione o sul principale
- Politiche di controllo del servizio che influiscono sulla sessione o sul principale
- Politiche di controllo delle risorse che influiscono sulla sessione o sul principale

# Motivazioni per l'utilizzo di richieste predefinite

In qualità di ingegnere della sicurezza, dovresti essere consapevole di ciò che spinge i costruttori di soluzioni a utilizzare presigned. URLs Comprendere cosa è necessario e cosa è facoltativo ti aiuterà a comunicare con i costruttori di soluzioni. Le motivazioni potrebbero includere quanto segue:

- Supportare un meccanismo di autenticazione non IAM beneficiando al contempo della scalabilità in Amazon S3. Una delle motivazioni principali è comunicare direttamente con Amazon S3 per beneficiare della scalabilità integrata fornita da questo servizio. Senza questa comunicazione diretta, una soluzione dovrebbe supportare il carico derivante dalla ritrasmissione dei byte inviati e delle chiamate. PutObjectGetObject A seconda del carico totale, questo requisito aggiunge sfide di scalabilità che un costruttore di soluzioni potrebbe voler evitare.

  Altri mezzi di comunicazione diretta con Amazon S3, come l'utilizzo di credenziali temporanee AWS Security Token Service in AWS STS() o firme Signature Version 4 URLs esterne, potrebbero non essere appropriati per il tuo caso d'uso. Amazon S3 identifica gli utenti tramite AWS credenziali, mentre le richieste predefinite presuppongono l'identificazione tramite meccanismi diversi dalle credenziali. AWS Colmare questa differenza mantenendo al contempo la comunicazione diretta dei dati è possibile tramite richieste predefinite.
- Per trarre vantaggio dalla comprensione nativa di un browser di. URLs URLs sono compresi dai browser, mentre AWS STS le credenziali e le firme Signature Version 4 non lo sono. Ciò è utile durante l'integrazione con soluzioni basate su browser. Le soluzioni alternative richiedono più codice, utilizzeranno più memoria per file di grandi dimensioni e potrebbero essere trattate in modo diverso da estensioni come malware e antivirus.

## Confronto con credenziali temporanee AWS STS

Le credenziali temporanee sono simili alle richieste prefirmate. Entrambi scadono, consentono l'ambito di accesso e vengono comunemente utilizzati per collegare credenziali non IAM a utilizzi che richiedono credenziali AWS.

È possibile stabilire un ambito ristretto di AWS STS credenziali temporanee per un singolo oggetto e azione S3, ma ciò può comportare problemi di scalabilità perché presenta dei limiti. AWS STS APIs (Per ulteriori informazioni, consulta l'articolo Come posso risolvere gli errori di limitazione delle API o «Frequenza superata» per IAM e AWS STS sul sito Web AWS re:post.) Inoltre, ogni credenziale generata richiede una chiamata AWS STS API, che aggiunge latenza e una nuova dipendenza che potrebbe influire sulla resilienza. Una AWS STS credenziale temporanea ha anche una scadenza minima di 15 minuti, mentre una richiesta predefinita può supportare durate più brevi (60 secondi sono pratici nelle giuste condizioni).

## Confronto con soluzioni basate esclusivamente sulla firma

L'unico componente intrinsecamente segreto di una richiesta prefirmata è la firma Signature Version 4. Se un cliente conosce gli altri dettagli di una richiesta e gli viene fornita una firma valida che corrisponde a tali dettagli, può inviare una richiesta valida. Senza una firma valida, non può.

Le soluzioni predefinite URLs e quelle basate sulla sola firma sono crittograficamente simili. Tuttavia, le soluzioni basate sulla sola firma presentano vantaggi pratici, come la possibilità di utilizzare un'intestazione HTTP anziché un parametro di stringa di query per trasmettere la firma (vedere la sezione Interazioni e mitigazioni della registrazione). Gli amministratori devono inoltre considerare che le stringhe di query vengono trattate più comunemente come metadati, mentre le intestazioni vengono trattate meno comunemente come tali.

D'altra parte, AWS SDKs offri meno supporto per la generazione e l'utilizzo diretto delle firme. La creazione di una soluzione basata esclusivamente sulle firme richiede più codice personalizzato. Da un punto di vista pratico, l'utilizzo di librerie anziché codice personalizzato per motivi di sicurezza è una best practice generale, pertanto il codice per le soluzioni basate esclusivamente sulla firma richiede un esame più approfondito.

Le soluzioni basate esclusivamente sulla firma non utilizzano la stringa di `X-Amz-Expires` query e non forniscono un periodo di validità esplicito. IAM gestisce i periodi di validità implicita delle firme che non hanno un orario di scadenza esplicito. Questi periodi impliciti non vengono pubblicati. In genere non cambiano, ma vengono gestiti pensando alla sicurezza, quindi non dovresti dipendere dai

periodi di validità. Esiste un compromesso tra il controllo esplicito sulla data di scadenza e la gestione della scadenza da parte di IAM.

In qualità di amministratore, potresti preferire una soluzione basata esclusivamente sulla firma. Tuttavia, in senso pratico, dovrai supportare le soluzioni così come sono state create.

# Identificazione delle richieste predefinite

## Identificazione delle richieste che hanno utilizzato un URL predefinito

Amazon S3 offre due meccanismi integrati per il monitoraggio dell'utilizzo a livello di richiesta: i log AWS CloudTrail di accesso al server Amazon S3 e gli eventi relativi ai dati. Entrambi i meccanismi possono identificare l'utilizzo di URL predefiniti.

Per filtrare i log per l'utilizzo di URL predefiniti, puoi utilizzare il tipo di autenticazione. Per i log di accesso al server, esamina il campo Authentication Type, che in genere viene denominato authtype quando è definito in una tabella Amazon Athena. Perché CloudTrail, esamina sul AuthenticationMethodcampo. `additionalEventData` In entrambi i casi, il valore del campo per le richieste che utilizzano URL predefiniti è`QueryString`, mentre `AuthHeader` è il valore per la maggior parte delle altre richieste.

`QueryString`l'utilizzo non è sempre associato a URL predefiniti. Per limitare la ricerca solo all'utilizzo di URL predefiniti, trova le richieste che contengono il parametro della stringa di query. `X-Amz-Expires` Per i log di accesso al server, esamina Request-URI e cerca le richieste che hanno un `X-Amz-Expires` parametro nella stringa di query. Per CloudTrail, esamina l'`requestParameters`elemento alla ricerca di un elemento. `X-Amz-Expires`

```
{"Records": [{…, "requestParameters": {…, "X-Amz-Expires": "300"}}, …]}
```

La seguente query Athena applica questo filtro:

```
SELECT * FROM {athena-table} WHERE
  authtype = 'QueryString' AND
  request_uri LIKE '%X-Amz-Expires=%';
```

Per AWS CloudTrail Lake, la seguente query applica questo filtro:

```
SELECT * FROM {data-store-event-id} WHERE
  additionalEventData['AuthenticationMethod'] = 'QueryString' AND
  requestParameters['X-Amz-Expires'] IS NOT NULL
```

# Identificazione di altri tipi di richieste predefinite

La richiesta POST ha anche un tipo di autenticazione univocoHtmlForm, nei log di accesso al server Amazon S3 e. CloudTrail Questo tipo di autenticazione è meno comune, quindi potresti non trovare queste richieste nel tuo ambiente.

La seguente query Athena applica il filtro per: HtmlForm

```
SELECT * FROM {athena-table} WHERE
  authtype = 'HtmlForm';
```

Per CloudTrail Lake, la seguente query applica il filtro:

```
SELECT * FROM {data-store-event-id} WHERE
  additionalEventData['AuthenticationMethod'] = 'HtmlForm'
```

# Identificazione dei modelli di richiesta

È possibile trovare le richieste predefinite utilizzando le tecniche illustrate nella sezione precedente. Tuttavia, per rendere utili questi dati, ti consigliamo di trovare degli schemi. I semplici TOP 10 risultati della tua query potrebbero fornire un'idea, ma se ciò non bastasse, utilizza le opzioni di raggruppamento nella tabella seguente.

| Opzione di raggruppamento | Registri di accesso al server | CloudTrailLago | Descrizione |
|---|---|---|---|
| Agente utente | GROUP BY useragent | GROUP BY userAgent | Questa opzione di raggruppamento consente di trovare l'origine e lo scopo delle richieste. L'agente utente è fornito dall'utente e non è affidabile come meccanismo di autentica zione o autorizza |

| Opzione di raggruppamento | Registri di accesso al server | CloudTrailLago | Descrizione |
|---|---|---|---|
| | | | zione. Tuttavia, può rivelare molto se stai cercando modelli, perché la maggior parte dei client utilizza una stringa unica che è almeno parzialmente leggibile dall'uomo. |
| Richiedente | `GROUP BY requester` | `GROUP BY userIdentity['arn']` | Questa opzione di raggruppamento aiuta a trovare i responsabili IAM che hanno firmato le richieste. Se il tuo obiettivo è bloccare queste richieste o creare un'eccezione per le richieste esistenti, queste query forniscono informazioni sufficienti a tale scopo. Quando utilizzi i ruoli in conformità alle best practice IAM, il ruolo ha un proprietario chiaramente identificato e puoi utilizzare tali informazioni per saperne di più. |

| Opzione di raggruppamento | Registri di accesso al server | CloudTrailLago | Descrizione |
| --- | --- | --- | --- |
| Indirizzo IP di origine | `GROUP BY remoteip` | `GROUP BY sourceIPAddress` | Questa opzione raggruppa in base all'ultimo hop di traduzione di rete prima di raggiungere Amazon S3.<br>• Se il traffico passa attraverso un gateway NAT, questo sarà l'indirizzo del gateway NAT.<br>• Se il traffico passa attraverso un gateway Internet, questo sarà l'indirizzo IP pubblico che ha inviato il traffico al gateway Internet.<br>• Se il traffico proviene dall'esterno AWS, questo sarà l'indirizzo Internet pubblico associato all'origine.<br>• Se passa su un endpoint VPC (Virtual Private |

| Opzione di raggruppamento | Registri di accesso al server | CloudTrailLago | Descrizione |
| --- | --- | --- | --- |
| | | | Cloud) gateway, questo sarà l'indirizzo IP dell'istanza nel VPC.<br><br>• Se passa attraverso un'interfaccia virtuale pubblica (VIF), questo sarà l'IP locale del richiedente o di qualsiasi intermediario, ad esempio un server proxy o un firewall che espone solo il suo indirizzo IP.<br><br>• Se passa attraverso un endpoint VPC di interfaccia, questo potrebbe essere l'indirizzo IP di un'istanza nel VPC. Potrebbe anche essere un indirizzo IP di un altro VPC o di una rete locale. Come per le VIF pubbliche, questo potrebbe essere l'indirizzo IP di |

| Opzione di raggruppamento | Registri di accesso al server | CloudTrailLago | Descrizione |
|---|---|---|---|
| | | | qualsiasi intermediario.<br><br>Questi dati sono utili se il tuo obiettivo è imporre controlli di rete. Potrebbe essere necessario combinare questa opzione con dati come `endpoint` (per i registri di accesso al server) o `vpcEndpointId` (per CloudTrail Lake) per chiarire l'origine, poiché reti diverse potrebbero duplicare gli indirizzi IP privati. |
| nome del bucket S3 | `GROUP BY bucket_name` | `GROUP BY requestParameters['bucketName']` | Questa opzione di raggruppamento consente di trovare i bucket che hanno ricevuto richieste. Ciò consente di identificare la necessità di eccezioni. |

# Le migliori pratiche per l'utilizzo di richieste predefinite

Questa sezione illustra le migliori pratiche per l'utilizzo di richieste predefinite che un tecnico della sicurezza dovrebbe prendere in considerazione. Le linee guida includono:

- Le migliori pratiche di base, che sono pratiche che ogni organizzazione dovrebbe seguire.
- Barriere aggiuntive, pratiche da prendere in considerazione, ma che si potrebbe decidere di implementare parzialmente o con eccezioni. Esse hanno lo scopo di fornire un controllo e una difesa aggiuntivi in profondità, ma devono essere bilanciate rispetto alla complessità complessiva.
- Registrazione delle interazioni, che potrebbero derivare da dispositivi o servizi che rientrano nella responsabilità dell'utente o del cliente nel modello di responsabilità condivisa. Questa sezione include le precauzioni per limitare le informazioni accessibili tramite i registri.

## Le migliori pratiche di base

Le best practice generali che costituiscono controlli efficaci per altre richieste AWS API si applicano anche alle richieste predefinite. Questa sezione esamina due delle pratiche più rilevanti: i privilegi minimi e i perimetri dei dati. Queste pratiche creano una profondità di controlli che altre pratiche estendono.

### Applica il principio del privilegio minimo

Il primo passo per limitare l'uso di richieste predefinite consiste nel limitare l'accesso ad Amazon S3 in generale. Un URL predefinito non può fornire l'accesso a risorse che non sono state concesse al principale che ha generato la firma per l'URL predefinito. Né può fornire l'accesso a una risorsa in un modo che non è stato concesso a tale principale. Pertanto, applicare le migliori pratiche per concedere a tali committenti il minimo privilegio è un'efficace barriera.

Il processo di creazione di un URL predefinito è un'operazione algoritmica basata su uno standard pubblicato (Signature Version 4) per la generazione di firme. Pertanto, non è possibile porre limiti alla generazione di URL predefiniti. Tuttavia, per essere pertinente, un URL predefinito deve essere valido e consentire l'accesso alle risorse, quindi la validità di un URL predefinito è anche un efficace guardrail.

Per ulteriori informazioni sui privilegi minimi, consulta Garantire l'accesso con privilegi minimi nel pilastro Framework, Security. AWS Well-Architected

## Implementa un perimetro di dati

Un'estensione del privilegio minimo consiste nel mantenere un perimetro di dati coerente con le esigenze dell'organizzazione. Gli URL predefiniti sono compatibili con i perimetri dei dati. Come per le altre richieste, la validità di una richiesta URL predefinita viene valutata al momento della richiesta. Se le proprietà della rete, della risorsa, della sessione di ruolo e del principale cambiano, vengono valutate nel momento e utilizzando il metodo con cui viene ricevuta la richiesta.

Ad esempio, supponiamo che un servizio in esecuzione in un container Amazon Elastic Kubernetes Service (Amazon EKS) firmi una richiesta. La richiesta viene successivamente inviata dal sistema di personal computer dell'utente connesso a Internet. In questo caso, la SourceIp condizione aws: valuta l'indirizzo IP pubblico visibile della richiesta dal sistema personale dell'utente, non l'indirizzo IP del servizio nel contenitore Amazon EKS.

Allo stesso modo, se i tag del principale o della risorsa cambiano prima dell'invio della richiesta, i valori aggiornati, non originali, verranno applicati alla richiesta tramite le ResourceTag/tag-key condizioni aws: PrincipalTag/tag-key e aws:.

# Guardrail aggiuntivi

Quando le richieste predefinite vengono utilizzate in modo appropriato dai creatori di soluzioni e dagli utenti, forniscono un meccanismo sicuro per consentire agli utenti di accedere ai dati. Inoltre, la capacità di generare richieste prefirmate non fornisce ai mandanti un accesso che non avevano già.

In tale contesto, sono necessari controlli aggiuntivi? La giustificazione dei controlli aggiuntivi non si basa sulla necessità di negare l'accesso, ma di fornire la possibilità di monitorare, approvare l'utilizzo e stabilire limiti e ridurre il rischio di errori degli utenti. In questo modo puoi contribuire a garantire che l'utilizzo sia appropriato e necessario.

I seguenti guardrail ti aiutano a raggiungere questo obiettivo. Prima di abilitare questi controlli, potresti voler determinare l'utilizzo esistente identificando le richieste predefinite. Questa identificazione aiuta a prepararsi all'impatto del guardrail sull'utilizzo esistente o a pianificare le eccezioni laddove necessario.

## Guardrail per S3:SignatureAge

Una caratteristica distintiva delle richieste predefinite è che descrivono un tempo di scadenza. La firma della richiesta contiene una data. Questa data viene trasmessa come parametro della stringa

di `X-Amz-Date` query per gli URL prefirmati e come intestazione Date o x-amz-date per un POST prefirmato.

Amazon S3 fornisce una chiave di condizione, S3:SignatureAge, che puoi utilizzare per limitare il tempo massimo tra la data di firma e la scadenza effettiva della richiesta. Questa condizione non può mai aumentare il periodo di validità, ma può ridurlo.

Nella seguente politica, la chiave `s3:signatureAge` condizionale limita le richieste predefinite a 15 minuti di validità. Gli esempi seguenti utilizzano tutti 15 minuti per limitare la validità a un intervallo di tempo simile a quello supportato dalla firma standard.

La seconda dichiarazione della policy nega qualsiasi accesso a Signature Version 2. Questa versione del protocollo di firma è obsoleta, ma in alcuni è ancora supportata. Regioni AWS Ti consigliamo di bloccarlo esplicitamente prima che diventi completamente obsoleto.

È possibile applicare la seguente politica come politica di controllo del AWS Organizations servizio (SCP). Gli utenti possono comunque utilizzare richieste predefinite e implementare soluzioni che dipendono da tali richieste, purché il tempo tra la generazione della firma e l'utilizzo sia inferiore a 15 minuti. A seconda dell'implementazione, questa limitazione potrebbe non avere alcun impatto, potrebbe rendere inutilizzabile una soluzione o causare errori occasionali che possono essere riprovati.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyPresignedOver15Minutes",
      "Effect": "Deny",
      "Action": "s3:*",
      "Resource": "*",
      "Condition": {
        "NumericGreaterThan": {
          "s3:signatureAge": "900000"
        }
      }
    },
    {
      "Sid": "DenySignatureVersion2",
      "Effect": "Deny",
      "Action": "s3:*",
      "Resource": "*",
      "Condition": {
```

```
        "StringEquals": {
           "s3:signatureversion": "AWS"
        }
      }
    }
  ]
}
```

## Eccezioni

Se una soluzione richiede più tempo prima della scadenza ed è quindi influenzata dalla politica precedente, si consiglia di fornire un metodo per approvare le eccezioni. Per evitare di enumerare le eccezioni in un SCP, usa aws:, come nella seguente politicaPrincipalTag, per gestire le eccezioni in modo scalabile. Altri AWS esempi, come gli esempi di policy perimetrali dei dati di AWS, utilizzano questa strategia.

Se implementi una politica di eccezione utilizzandoaws:PrincipalTag, devi controllare l'accesso all'impostazione dei tag sui principali. I tag di questo tipo possono provenire direttamente dai principali e possono essere controllati da un SCP, come in questo esempio di controllo dei valori dei tag che possono essere impostati. Un tag di questo tipo può anche provenire dai tag di sessione, che vengono impostati da un provider di identità (IdP) o quando vengono utilizzati. AWS STS Il controllo dell'accesso a aws:PrincipalTag è un argomento complesso. Tuttavia, un'organizzazione con esperienza nell'uso del controllo degli accessi basato sugli attributi (ABAC) disporrà dell'esperienza e dei controlli necessari per consentirne l'uso appropriato aws:PrincipalTag per questo caso d'uso.

Nell'esempio seguente, la aws:PrincipalTag condizione crea un'eccezione che consente a qualsiasi principale con il tag denominato (long-presigned-allowed) assegnato e impostato su. true Con questa eccezione, la restrizione sull'età della firma non viene applicata.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyPresignedOver15Minutes",
      "Effect": "Deny",
      "Action": "s3:*",
      "Resource": "*",
      "Condition": {
        "NumericGreaterThan": {
          "s3:signatureAge": "900000"
        },
```

```
        "StringNotEquals": {
          "aws:PrincipalTag/long-presigned-allowed": "true"
        }
      }
    }
  ]
}
```

## Policy di bucket

È possibile applicare le policy relative ai bucket a tutti o a determinati bucket utilizzando una policy come nell'esempio seguente. A differenza di una SCP, una policy bucket riguarda anche l'utilizzo principale del servizio. L'Appendice A non documenta l'utilizzo previsto del principale servizio da parte delle richieste predefinite, ma se si volesse implementare un controllo per dimostrare tale limite, la seguente politica fornirebbe tale controllo. Inoltre, a differenza di un SCP, ai responsabili del tuo account di gestione può applicarsi una policy relativa ai bucket.

ABAC-based le eccezioni funzionano nelle policy bucket allo stesso modo di un SCP. L'obiettivo di una bucket policy potrebbe essere quello di applicarsi ai responsabili esterni all'organizzazione, quindi le eccezioni ABAC dovrebbero essere limitate ai principi per i quali si applicano i controlli ABAC.

Nell'esempio seguente, la `aws:PrincipalTag` condizione della prima istruzione crea un'eccezione per un principale con il tag named () assegnato e impostato su. `long-presigned-allowed` `true` Con questa eccezione, la restrizione sull'età della firma non viene applicata. La seconda dichiarazione applica questa restrizione a tutti i responsabili esterni all' AWS organizzazione proprietaria del bucket. L'ambito di questa seconda istruzione deve corrispondere ai controlli ABAC per impostare il tag denominato per i principali.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyPresignedOver15MinWithExceptions",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::{bucket-name}/*",
      "Condition": {
        "NumericGreaterThan": {
          "s3:signatureAge": "900000"
```

```
        },
        "StringNotEquals": {
          "aws:PrincipalTag/long-presigned-allowed": "true"
        }
      }
    },
    {
      "Sid": "DenyPresignedOver15MinutesOutsideOrg",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::{bucket-name}/*",
      "Condition": {
        "NumericGreaterThan": {
          "s3:signatureAge": "900000"
        },
        "StringNotEquals": {
          "aws:PrincipalOrgID": "${aws:ResourceOrgID}"
        }
      }
    }
  ]
}
```

## Politiche di controllo delle risorse

È possibile applicare una policy ai bucket su larga scala utilizzando le [politiche di controllo delle risorse (](#)RCP). Analogamente agli SCP e a differenza delle policy relative ai bucket, gli RCP non riguardano l'utilizzo principale del servizio. Gli RCP influiscono sui principali non di servizio di qualsiasi account, ma non influiscono sulle risorse dell'account di gestione. Per ulteriori informazioni, consulta la [documentazione relativa ad AWS Organizations](#).

Come per le policy bucket, se utilizzate `aws:PrincipalTags` per creare eccezioni per i principali, tenete presente l'ambito dei controlli ABAC sull'etichettatura dei principali.

Il seguente RCP limita l'utilizzo degli URL predefiniti in tutti i bucket S3 di un'organizzazione limitando la durata della firma a 15 minuti.

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

```
      "Sid": "DenyPresignedOver15MinWithExceptions",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::*/*",
      "Condition": {
        "NumericGreaterThan": {
          "s3:signatureAge": "900000"
        },
        "StringNotEquals": {
          "aws:PrincipalTag/long-presigned-allowed": "true",
        }
      }
    },
    {
      "Sid": "DenyPresignedOver15MinutesOutsideOrg",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::*/*",
      "Condition": {
        "NumericGreaterThan": {
          "s3:signatureAge": "900000"
        },
        "StringNotEquals": {
          "aws:PrincipalOrgID": "${aws:ResourceOrgID}"
        }
      }
    }
  ]
}
```

## Guardrail per S3:AuthType

Gli URL prefirmati utilizzano l'autenticazione della stringa di query e i POST prefirmati utilizzano sempre l'autenticazione POST. Amazon S3 supporta la negazione delle richieste in base al tipo di autenticazione tramite la chiave di condizione S3:AuthType. `REST-QUERY-STRING`è il `s3:authType` valore per le stringhe di query ed `POST` è il valore per POST. `s3:authType`

È possibile applicare la seguente politica come SCP. La policy consente solo `s3:authType` l'autenticazione basata sull'intestazione. Configura inoltre un metodo per fornire eccezioni a singoli utenti o ruoli.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyNonHeaderAuth",
      "Effect": "Deny",
      "Action": "s3:*",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "s3:authType": "REST-HEADER",
          "aws:PrincipalTag/non-header-auth-allowed": "true"
        }
      }
    }
  ]
}
```

Il rifiuto delle richieste in base al tipo di autenticazione influisce su qualsiasi soluzione o funzionalità che utilizza il tipo di autenticazione negata. Ad esempio, la negazione `REST-QUERY-STRING` impedisce agli utenti di eseguire caricamenti o download dalla console Amazon S3. Se desideri che gli utenti utilizzino la console Amazon S3, non utilizzare questo guardrail o fai un'eccezione per gli utenti. D'altra parte, se non desideri che gli utenti utilizzino la console Amazon S3, puoi `REST-QUERY-STRING` negarla agli utenti.

Forse stai già negando agli utenti l'accesso diretto alle risorse di Amazon S3. In questo caso, un guardrail per il tipo di autenticazione è ridondante. Tuttavia, un'istruzione `s3:authType` deny fornisce un'utilità di difesa approfondita perché le implementazioni per negare l'accesso diretto di solito riguardano molte istruzioni di controllo, alcune con eccezioni.

I ruoli utilizzati per i carichi di lavoro in genere non richiedono l'accesso alla stringa di query o all'autenticazione. `POST` Le eccezioni sono ruoli che supportano servizi progettati per utilizzare richieste predefinite. È possibile creare eccezioni specifiche per tali ruoli.

È inoltre possibile applicare una policy sui bucket a tutti i bucket o a determinati bucket utilizzando una politica come la seguente:

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

```
      "Sid": "DenyNonHeaderAuth",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::{bucket-name}/*",
      "Condition": {
        "StringNotEquals": {
          "s3:authType": "REST-HEADER",
          "aws:PrincipalTag/non-header-auth-allowed": "true"
        }
      }
    }
  ]
}
```

Questa policy bucket ha l'effetto di negare l'uso delle UploadPartCopyAPI CopyObjectand per creare copie tra regioni diverse. La replica di Amazon S3 non è interessata perché non si basa su queste API.

Se desideri utilizzare una policy bucket come quella precedente e continuare a supportare la policy interregionale CopyObjecto l'UploadPartCopyAPI, aggiungi una condizione simile alla seguente: `aws:ViaAWSService`

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyNonHeaderAuth",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::{bucket-name}/*",
      "Condition": {
        "StringNotEquals": {
          "s3:authType": "REST-HEADER",
          "aws:PrincipalTag/non-header-auth-allowed": "true"
        },
        "Bool": {
          "aws:ViaAWSService": "false"
        },
      }
    }
  ]
```

```
}
```

## Combinazione di guardrail ed eccezioni predefiniti con altri guardrail

Se non avete intenzione di applicare un guardrail in generale ai vostri utenti e ruoli, potreste volerlo applicare alle eccezioni di altri guardrail comuni, in modo che tali eccezioni non supportino le richieste predefinite.

Se hai restrizioni di rete ma consenti eccezioni per partner esterni o casi d'uso speciali, dovresti bloccare la stringa di query o l'`POST`autenticazione quando vengono applicate tali eccezioni, a meno che non siano specificamente identificate come obbligatorie.

## Limitazioni a S3:SignatureAge

Gli amministratori troveranno utile comprendere in modo più completo le implicazioni di. `s3:signatureAge` Ogni richiesta firmata include`X-Amz-Date`, che dovrebbe indicare l'ora corrente. Questo valore viene inserito dal cliente e dal firmatario della richiesta. AWS rifiuta le richieste che ritiene abbiano orari non validi. Tuttavia, un firmatario potrebbe generare firme in anticipo in un momento futuro. Amazon S3 rifiuta le richieste che specificano un orario futuro se vengono inviate con troppo anticipo. Tuttavia, se la richiesta non viene inviata fino al momento in cui viene apposta la firma, la firma potrebbe essere generata prima e inviata successivamente.

`s3:signatureAge`limita l'età massima di registrazione `X-Amz-Date` di una firma solo per le richieste predefinite. Le richieste più vecchie dell'età specificata vengono rifiutate, anche se la scadenza `X-Amz-Expires` o una `POST` politica le avrebbe dichiarate valide. `s3:signatureAge`non modifica il periodo di validità per le richieste che non includono una scadenza esplicita. Inoltre, non controlla il valore utilizzato da un client per la firma. `X-Amz-Date`

Se l'orologio di sistema è sbagliato o se un client richiede intenzionalmente date future, l'ora firmata potrebbe non essere l'ora in cui è stata generata la firma. Ciò limita la capacità di controllo delle soluzioni`s3:signatureAge`. Una soluzione che utilizza l'ora corrente per generare le firme è limitata nel modo previsto: le firme rimangono valide per il numero di millisecondi specificato in. `s3:signatureAge` Una soluzione che non utilizza l'ora corrente avrà limiti diversi. Una restrizione è che le credenziali utilizzate per firmare la firma devono essere ancora valide. In qualità di amministratore, puoi controllare la validità massima delle credenziali temporanee emesse. Puoi consentire che le credenziali siano valide per un massimo di 36 ore o limitarne la validità a un massimo di 15 minuti. La scadenza delle credenziali temporanee non dipende dal valore di. `X-Amz-Date`

Le credenziali permanenti non hanno questa restrizione. Utilizzare solo credenziali temporanee è una procedura consigliata e puoi revocare esplicitamente qualsiasi credenziale permanente, il che invaliderebbe anche tutte le firme basate su tali credenziali.

Sebbene `s3:signatureAge` sia misurato in millisecondi, non è pratico impostarlo su un valore inferiore a 60 secondi, anche se si dispone di un orologio ben sincronizzato e di un utilizzo a bassa latenza. Le impostazioni inferiori a 60 secondi comportano il rischio di rifiutare richieste valide. Se si prevedono ritardi tra la generazione della firma e l'invio della richiesta o problemi con la sincronizzazione dell'orologio, è necessario tenerne conto nella gestione di. `s3:signatureAge`

## Indirizzare i bucket su larga scala

Gli SCP e gli RCP possono essere utilizzati `aws:PrincipalTag` per creare eccezioni per gli utenti. Non è possibile utilizzare i tag su un bucket per controllare l'accesso tramite `aws:ResourceTag` – per il controllo degli accessi vengono utilizzati solo i tag degli oggetti. In genere non è scalabile aggiungere un tag a ogni oggetto a cui si desidera applicare questo controllo.

Una soluzione adatta a molti casi d'uso consiste nell'applicare la policy e l'eccezione a livello di account, modificando gli account a cui si applica SCP o RCP o utilizzando aws:ResourceAccount, aws: o aws: ResourceOrgPaths ID. ResourceOrg Ad esempio, un SCP o RCP potrebbe essere applicato a un set di account di produzione.

Un'altra soluzione consiste nell'utilizzare una AWS Config regola personalizzata per implementare un controllo investigativo o un controllo reattivo. L'obiettivo sarebbe che ogni bucket contenga una policy sui bucket con il guardrail appropriato. Oltre a testare il contenuto di una bucket policy, la AWS Config regola personalizzata può recuperare i tag dal bucket ed escludere il bucket dalla regola se il bucket è etichettato con un valore specifico. Se tale regola non supera il controllo di conformità, potrebbe contrassegnare il bucket come non conforme o richiamare una correzione per aggiungere il guardrail alla policy del bucket.

> **Note**
>
> Non puoi limitare il contenuto dei tag delle richieste a. PutBucketTagging Per mantenere il controllo sulla modalità di etichettatura di un bucket, devi limitare l'accesso a `PutBucketTagging` e DeleteBucketTagging.

# Registrazione delle interazioni e delle mitigazioni

Un URL predefinito contiene una firma e può essere utilizzato, nel periodo precedente alla scadenza, per eseguire l'operazione API specifica per cui è stato firmato. Deve essere considerata una credenziale di accesso temporanea. La firma deve rimanere privata solo per le parti che hanno bisogno di conoscerla. Nella maggior parte degli ambienti, si tratta del client che invia la richiesta e del server che la riceve. L'invio della firma come parte di una sessione HTTPS diretta ne mantiene la natura privata, poiché solo un partecipante alla sessione HTTPS ha visibilità sull'URI che trasmette la firma.

Per gli URL predefiniti, la firma viene trasmessa come parametro della `X-Amz-Signature` stringa di query. I parametri della stringa di query sono componenti di un URI. Il rischio è che i client possano registrare l'URI e la firma con esso. I client hanno accesso all'intera richiesta HTTP e possono registrare qualsiasi parte della richiesta, dei dati e delle intestazioni (incluse le intestazioni di autenticazione). Tuttavia, questo è per convenzione meno comune. La registrazione degli URI è più comune ed è necessaria in casi come la registrazione degli accessi. I client devono utilizzare la redazione o il mascheramento per rimuovere la firma prima di registrare gli URI.

In alcuni ambienti, gli utenti consentono agli intermediari (proxy) di ottenere visibilità nelle loro sessioni HTTPS. L'abilitazione dei proxy richiede un elevato livello di accesso privilegiato ai sistemi client, poiché richiedono configurazione e certificati affidabili. L'installazione della configurazione proxy e dei certificati affidabili, nel contesto locale dell'ambiente intermediario del client, consente un livello di privilegio molto elevato. Per questo motivo, l'accesso a tali intermediari dovrebbe essere strettamente controllato.

Lo scopo di un intermediario è in genere quello di bloccare le uscite indesiderate e di tracciare altre uscite. Pertanto, è normale che tali intermediari registrino le richieste. Sebbene gli intermediari possano, come i client, registrare qualsiasi contenuto, intestazione e dato (tutti elementi molto sensibili), è più comune che registrino gli URI, come quelli che includono il `X-Amz-Signature` parametro della stringa di query.

## Mitigazioni

È consigliabile che la registrazione URI oscuri il parametro della stringa di `X-Amz-Signature` query, l'intera stringa di query o tratti le informazioni come altamente riservate, come nel caso dell'accesso diretto al server intermedio. Sebbene queste protezioni siano altamente consigliate, il fatto che gli URL predefiniti scadano riduce i rischi di esposizione dei log, a condizione che l'esposizione venga ritardata abbastanza a lungo da far scadere le firme.

Anche Amazon S3 rileva le firme e deve gestirle in modo appropriato. I log di accesso al server Amazon S3 includono l'URI della richiesta ma lo oscurano, come consigliato. `X-Amz-Signature` Lo stesso vale quando gli eventi CloudTrail relativi ai dati vengono registrati per Amazon S3. Puoi configurare Amazon CloudWatch Logs per mascherare i dati utilizzando identificatori di dati personalizzati.

La seguente espressione regolare corrisponde a `X-Amz-Signature` quella visualizzata in un URI:

```
X-Amz-Signature=[a-f0-9]{64}
```

La seguente espressione regolare aggiunge modelli di raggruppamento per identificare più specificamente il testo da sostituire:

```
(?:X-Amz-Signature=)([a-f0-9]{64})
```

Se è presente una voce del registro di accesso come la seguente:

```
X-Amz-Signature=733255ef022bec3f2a8701cd61d4b371f3f28c9f193a1f02279211d48d5193d7
```

La prima espressione regolare traduce la voce del registro degli accessi in:

```
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

La seconda espressione regolare, sui sistemi che supportano gruppi non di acquisizione, traduce la voce del registro di accesso in:

```
X-Amz-Signature=XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

# Domande frequenti

## È possibile utilizzare una richiesta prefirmata più volte? È un rischio per la sicurezza?

Sì, una firma in una richiesta prefirmata può essere utilizzata più di una volta. Se si tratti di un rischio per la sicurezza è una questione contestuale. Anche altri metodi di accesso ai servizi AWS consentono la ripetizione. Un utente o un carico di lavoro con AWS credenziali può inviare molte richieste a Servizi AWS e ognuna di queste richieste potrebbe essere duplicata.

Se il tuo caso d'uso richiede l'esecuzione una sola volta, dovresti implementare altri meccanismi per imporre l'uso singolo. L'uso singolo non è una funzionalità delle richieste predefinite. In qualità di ingegnere della sicurezza, dovresti esaminare i casi d'uso e le implementazioni, ma in molti casi l'uso multiplo si adatta a un uso accettabile.

## Una richiesta predefinita può essere utilizzata da un utente diverso dall'utente previsto?

Una firma in una richiesta prefirmata può essere inviata da chiunque ne sia in possesso. Sarà accettata solo se supera altre forme di convalida, come i controlli perimetrali dei dati. Se la firma è scaduta, le credenziali di firma sono scadute o le credenziali di firma non hanno accesso alle risorse richieste, la richiesta verrà rifiutata.

Lo stesso vale per altri metodi di autenticazione con. Servizi AWS Le credenziali condivise in modo inappropriato consentono l'accesso inappropriato. La best practice di base consiste nel condividere credenziali e firme solo con il pubblico previsto. Se non puoi fidarti del fatto che il pubblico a cui sei destinato protegga i dati privati e non li condivida con altri, ciò comprometterà qualsiasi forma di autenticazione.

## Un utente autorizzato può utilizzare una richiesta predefinita per esfiltrare i dati?

La protezione dei dati richiede un'azione efficace. Consentire l'accesso per gli scopi previsti mantenendo un perimetro di dati richiede un approccio completo. L'accesso con privilegi minimi, i controlli perimetrali dei dati e l'utilizzo di sole credenziali di accesso temporanee sono best practice

generali che si applicano alla protezione dei dati. L'uso appropriato di questi controlli limita inoltre la capacità degli utenti di eseguire azioni tramite le richieste predefinite che generano.

Questo perché l'accesso fornito da una richiesta prefirmata è un sottoinsieme dell'accesso concesso alle credenziali utilizzate per firmare la richiesta. In questo contesto, le migliori pratiche che si applicano all'accesso ai dati in genere si applicano alle richieste prefirmate, ma le richieste prefirmate non creano un nuovo accesso ai dati.

- La scadenza massima è limitata alla scadenza delle credenziali di firma. Se le credenziali di firma vengono revocate, le firme basate su tali credenziali non sono più valide.
- Se le autorizzazioni per il principale IAM associato alle credenziali di firma non includono l'esecuzione dell'azione associata alla richiesta prefirmata, l'invocazione di una richiesta prefirmata genera una risposta di «accesso negato». La risposta dipende dallo stato attuale delle autorizzazioni al momento della chiamata, che non ha alcuna relazione con il momento in cui è stata generata la firma della richiesta prefirmata.
- Le proprietà del principale vengono valutate in base al principale associato alle credenziali di firma.
- Le proprietà di una sessione di ruolo vengono valutate in base alla sessione di ruolo associata alle credenziali di firma.
- Le proprietà della rete vengono valutate in base al modo in cui è stata ricevuta la richiesta, come per le richieste normali.

In questo contesto, l'esame dei rischi associati alle richieste predefinite è limitato alle aree in cui sono firmate con credenziali diverse dalle credenziali dell'utente e forniscono un accesso che non faceva parte delle principali credenziali dell'utente. Questo esame dovrebbe essere applicato alla progettazione del servizio, del carico di lavoro o della soluzione che genera firme per conto dell'utente, anziché alla funzionalità di richiesta predefinita stessa.

## Posso negare l'accesso da un URL predefinito se sospetto che sia stato condiviso in modo non autorizzato?

Sì. Ciò richiede l'invalidazione delle credenziali con cui è stato firmato l'URL. Esistono diversi modi per eseguire questa operazione:

- Rimuovi le autorizzazioni dal principale IAM a cui appartengono le credenziali. Se il principale IAM non ha più accesso alla risorsa e all'operazione per cui l'URL è firmato, l'URL non può eseguire quell'operazione. Ciò influisce su tutti gli usi corrispondenti di quel principale IAM.

- Se le credenziali utilizzate per firmare l'URL sono AWS STS credenziali temporanee, puoi revocare le autorizzazioni di sessione per le credenziali temporanee emesse prima di un orario specifico per il principale IAM. A seconda del caso d'uso, potrebbero esserci altre sessioni valide che vengono invalidate prima della normale scadenza, ma le nuove sessioni non ne risentiranno. La revoca delle autorizzazioni di sessione invalida anche URLs quelle firmate utilizzando le credenziali associate a tali sessioni, ma le nuove sessioni associate a nuove URLs sessioni non ne risentiranno.
- Se le credenziali utilizzate per firmare l'URL sono credenziali permanenti, disattiva la chiave di accesso. Ciò influisce su tutto l'utilizzo legato a tali credenziali.

# Risorse

## Documentazione Amazon S3

- Richieste di autenticazione (AWS Signature Version 4)
- Autenticazione delle richieste: utilizzo dei parametri di interrogazione (AWS Signature versione 4)
- Richieste di autenticazione: caricamenti basati su browser tramite POST (Signature Version 4)AWS
- Chiavi di policy specifiche per l'autenticazione di Amazon S3 Signature versione 4
- Lavorare con URL predefiniti

## Altri riferimenti

- Creazione di un perimetro di dati su AWS (white paper)AWS
- SEC03-BP02 Concedi l'accesso con privilegi minimi (Well Architected Framework, pilastro Security)AWS
- SEC03-BP05 Definite le barriere di autorizzazione per la vostra organizzazione (Well Architected Framework, Security Pillar)AWS

# Appendice A: Come Servizi AWS usare presigned URLs

Questa appendice fornisce informazioni Servizi AWS e funzionalità che utilizzano presigned. URLs Queste informazioni hanno due scopi:

- Fornire agli ingegneri della sicurezza che implementano i controlli informazioni sui possibili impatti di tali controlli.
- Per sensibilizzare l'opinione pubblica sulle situazioni in cui questo rischio potrebbe essere rilevante per le interazioni di registrazione degli URL.

> **Important**
>
> Questa appendice non fornisce un elenco completo Servizi AWS o il loro utilizzo di presigned. URLs Inoltre, non copre soluzioni personalizzate o di terze parti.

## Console Amazon S3

Principale: utente della console

Scadenza predefinita: 5 minuti

> **Dichiarazione di non responsabilità**
>
> Questa sezione documenta il comportamento attuale della console Amazon S3. AWS i comportamenti della console sono soggetti a modifiche senza preavviso.

La console Amazon S3 supporta il download e il caricamento di oggetti. I download utilizzano un URL predefinito con una scadenza di 300 secondi (5 minuti). L'URL viene generato da una richiesta a`https://<bucket-region>.console.aws.amazon.com/s3/batchOpsServlet-proxy`.

Tale richiesta viene avviata quando l'utente fa clic su un pulsante di download, quindi l'URL non viene generato in anticipo o inviato al client fino a quando non viene effettuata la richiesta esplicita di download.

I caricamenti sono simili, tranne per il fatto che la console invia due richieste: `OPTIONS` come controllo CORS prima del volo e. `PUT` Entrambe le richieste utilizzano la stessa firma.

Le credenziali utilizzate per la firma sono credenziali temporanee associate all'utente attualmente connesso. I dettagli sul metodo per ottenere tali credenziali temporanee non rientrano nell'ambito di questa guida.

## Amazon S3 Object Lambda

Principale: chiamante del punto di accesso

Scadenza predefinita: 61 secondi

> **Note**
>
> A partire dal 7 novembre 2025, S3 Object Lambda è disponibile solo per i clienti esistenti che attualmente utilizzano il servizio e per alcuni AWS Partner Network partner (APN). Per funzionalità simili a S3 Object Lambda, scopri di più qui — Modifica della disponibilità di Amazon S3 Object Lambda.

Amazon S3 Object Lambda utilizza AWS Lambda funzioni per elaborare e trasformare automaticamente i dati quando vengono recuperati da Amazon S3. Quando S3 Object Lambda richiama una funzione, alla funzione viene fornito un URL predefinito `inputS3Url` () che può utilizzare per scaricare l'oggetto originale dal punto di accesso di supporto.

Questi prefirmati URLs sono firmati per il punto di accesso Amazon S3 di supporto, fornito quando si configura S3 Object Lambda. (Non è lo stesso del punto di accesso Object Lambda). Invece di utilizzare un ruolo associato alla funzione Lambda, l'URL viene firmato utilizzando l'identità del chiamante originale e le autorizzazioni dell'utente verranno applicate quando viene utilizzato l'URL. Se nell'URL sono presenti intestazioni firmate, la funzione Lambda deve includere queste intestazioni nella chiamata ad Amazon S3.

L'URL predefinito restituito ha una scadenza di 61 secondi (un secondo in più rispetto alla durata massima per una funzione S3 Object Lambda). L'URL generato può essere utilizzato solo con il punto di accesso di supporto. Il chiamante del punto di accesso S3 Object Lambda deve avere accesso a questo punto di accesso. Puoi limitare tale accesso al contesto di S3 Object Lambda utilizzando la condizione. `"aws:CalledVia": ["s3-object-lambda.amazonaws.com"]` Quando tale condizione è associata a un punto di accesso o a un bucket di supporto, un utente non può accedere direttamente al punto di accesso o al bucket di supporto.

Il valore di questo approccio è che non è necessario concedere alla funzione Lambda l'accesso al bucket o all'access point S3. Il ruolo associato alla funzione Lambda richiederà le autorizzazioni per WriteGetObjectResponse, ma non le richiede per. GetObject

Quando S3 Object Lambda genera URLs presigned, non aggiunge restrizioni di rete, quindi è possibile utilizzare un URL al di fuori della funzione Lambda. Tuttavia, tutte le restrizioni imposte al chiamante di S3 Object Lambda restano valide. Ad esempio, se la tua funzione Lambda viene eseguita in un VPC e limiti il chiamante all'utilizzo di un endpoint VPC, chiunque sia in possesso dell'URL predefinito dovrebbe avere la possibilità di inviarlo tramite quell'endpoint VPC. Questa VpcSourceIprestrizione si applica anche a and. SourceIp

> **Note**
>
> Per utilizzare una funzione S3 Object Lambda in un VPC, il VPC deve disporre di un percorso verso gli endpoint S3 pubblici da chiamare. WriteGetObjectResponse Ciò non indica che i requisiti per l'utilizzo di un endpoint VPC non si applichino alle richieste di recupero dei dati dal bucket.

## AWS Lambda Interregione CopyObject

Principale: internoAWS

Scadenza predefinita: 3600 secondi

Quando usi l'UploadPartCopyAPI CopyObjector per copiare Regioni AWS, Amazon S3 utilizza URLs presigned internamente. Questi APIs possono essere richiamati direttamente da SDKs o dai comandi e. AWS CLI `aws s3api copy-object` `aws s3api upload-part` Questi APIs non vengono utilizzati per Amazon S3 Replication, ma vengono utilizzati dai `aws s3 sync` comandi AWS CLI `aws s3 cp` and quando l'origine e la destinazione sono bucket S3. Sono inoltre supportati da `TransferManager` implementazioni in vari campi. AWS SDKs

## AWS Lambda GetFunction

Principale: interno AWS

Scadenza predefinita: 10 minuti

AWS Lambda archivia la versione utente in un bucket S3 di proprietà del team Lambda, prima di generare le risorse distribuite nei contenitori Lambda. Quando vuoi accedere al codice

della tua funzione, chiami l'API. GetFunction Questa API risponde con`Code.Location`, che contiene un URL predefinito valido per 10 minuti (questa scadenza è il comportamento corrente e non un contratto pubblicato). Se non desideri il codice, puoi utilizzare una combinazione di GetFunctionConfigurationGetFunctionConcurrency, e ListTagsper recuperare gli altri dati restituiti da. `GetFunction`

L'URL restituito non è firmato con le credenziali dell'utente attualmente connesso, ma per conto dell'utente da Lambda. Per questo motivo, le chiavi di condizione (ad esempio`aws:SourceIP`) applicate all'utente attualmente connesso o le credenziali di sessione temporanea dell'utente non si applicano all'URL generato. Ciò è vero indipendentemente dal fatto che le chiavi di condizione vengano applicate GetFunctionsolo a o a tutti gli utilizzi delle API AWS per l'utente o la sessione.

La console Lambda utilizza GetFunctionanche l'URL predefinito che restituisce. La console utilizza le credenziali temporanee associate all'utente attualmente connesso per effettuare la chiamata. GetFunction I dettagli sull'ottenimento di tali credenziali temporanee non rientrano nell'ambito di questo documento.

## Amazon ECR

Principale: interno AWS

Scadenza predefinita: 1 ora

Amazon Elastic Container Registry (Amazon ECR) fornisce GetDownloadUrlForLayerl'API, che restituisce un URL predefinito valido per un'ora e supporta il download di un singolo livello da un'immagine Amazon ECR. Tuttavia, questa operazione viene utilizzata dal proxy Amazon ECR e generalmente non viene utilizzata dagli utenti per estrarre e inviare immagini.

## Amazon Redshift Spectrum

Principal: Ruolo passato a CREATE EXTERNAL SCHEMA tramite `IAM_ROLE`

Scadenza predefinita: 1 ora

Amazon Redshift Spectrum utilizza URLs presigned internamente e vieta restrizioni sulla combinazione del bucket e del ruolo Amazon Redshift che limiterebbero il presigned. URLs Puoi utilizzare un `s3:signatureAge` valore di 16 minuti, ma valori molto bassi non sono affidabili. Il valore minimo che è possibile utilizzare dipende dalla tempistica e dalla dimensione della query. Sebbene un valore inferiore a 16 minuti funzioni per molti scenari, richiede dei test. Il ruolo può e

deve essere limitato all'utilizzo solo da parte di Redshift Spectrum, che non rivela ciò che genera, attenuando URLs così la tipica giustificazione per valori di scadenza inferiori.

## Amazon SageMaker AI Studio

Amazon SageMaker AI Studio supporta due azioni API: CreatePresignedDomainUrle CreatePresignedNotebookInstanceUrl. Tuttavia, queste APIs non sono correlate alla funzionalità URL prefirmata Signature Version 4. Questi APIs creano un URL che utilizza un `authToken` parametro, ma non supportano nessuno dei parametri di query standard di Signature Version 4.

`authToken`è un meccanismo diverso ma presenta delle somiglianze con URLs presigned. Viene inviato come parametro della stringa di query e supporta un tempo di scadenza di 5 minuti.

SageMaker L'intelligenza artificiale supporta le restrizioni di rete. Se imponi una restrizione all'`sagemaker:CreatePresignedDomainUrl`azione, tale azione si applica sia alla chiamata CreatePresignedDomainUrlche all'uso dell'URL generato. Se un URL viene generato da una rete valida e quindi inviato da una rete non valida, la chiamata API per generare l'URL ha esito positivo, ma la richiesta che invia l'URL ha esito negativo. Lo stesso vale per CreatePresignedNotebookInstanceUrle per l'`sagemaker:CreatePresignedNotebookInstanceUrl`azione.

Per ulteriori informazioni, consulta la documentazione sull'SageMaker intelligenza artificiale.

# Appendice B: Come influiscono i controlli predefiniti URLs Servizi AWS

Questa appendice descrive le interazioni tra i controlli Servizi AWS che utilizzano presigned URLs, come descritto nell'Appendice A, e i controlli descritti in precedenza in questa guida.

## Guardrail per s3:SignatureAge

La console Amazon S3 non viene interrotta dalla scadenza massima di 5 minuti impostata dalla `s3:signatureAge` chiave di condizione. La console Amazon S3 genera dati predefiniti URLs quando scegli il pulsante Download e applica la propria scadenza di 5 minuti. Una durata massima inferiore a 2 minuti potrebbe creare errori casuali in base alla sincronizzazione dell'orologio e alle latenze.

Amazon S3 Object Lambda utilizza un tempo di scadenza di 61 secondi, quindi l'impostazione di condizioni su un `s3:signatureAge` valore di 61 secondi o più non causerà alcuna interruzione. Le durate più brevi potrebbero essere meno affidabili e causare guasti intermittenti.

Amazon S3 Cross-region CopyObjectnon è disturbato da una scadenza massima di 5 minuti. Tuttavia, durate più brevi potrebbero creare errori casuali in base alla sincronizzazione e alle latenze dell'orologio.

In AWS Lambda, GetFunctionfornisce un URL agli oggetti esterni all'account del cliente, in modo che le politiche del cliente non influiscano su quanto generato. URLs

Amazon Redshift Spectrum è stato testato con `s3:signatureAge` una condizione di 16 minuti. Tuttavia, durate più brevi potrebbero causare interruzioni.

## Guardrail per S3:authType quando non si utilizzano restrizioni di rete

La console Amazon S3 è generalmente interessata dal guardrail. `s3:authType` La console esegue il routing verso Amazon S3 in base alla configurazione della rete locale. Se la rete locale viene instradata verso Amazon S3 in un modo consentito dalla restrizione di rete, la console Amazon S3 continuerebbe a funzionare. Tuttavia, se viene instradata tramite un proxy o la rete Internet pubblica

in un modo non consentito, l'utilizzo verrebbe bloccato. Tuttavia, il blocco dell'utilizzo è probabilmente l'intento di questa politica.

Amazon S3 Object Lambda è interessato se la funzione Lambda non è connessa a un VPC appropriato. In questa configurazione, il VPC deve disporre di un gateway NAT, non per accedere al bucket S3, ma per chiamare. WriteGetObjectResponse

Amazon S3 Cross-region CopyObjectviene interrotto se questo guardrail viene applicato a una bucket policy senza l'eccezione consigliata per when is true. **`aws:viaAWSService`**

Amazon Redshift Spectrum è interessato dal guardrail a meno `s3:authType` che non venga utilizzato un routing VPC avanzato. Attualmente, Redshift Spectrum supporta il routing VPC avanzato solo con cluster serverless, non con cluster con provisioning.

# Cronologia dei documenti

La tabella seguente descrive le modifiche significative apportate a questa guida. Per ricevere notifiche sugli aggiornamenti futuri, puoi abbonarti a un feed RSS.

| Modifica | Descrizione | Data |
| --- | --- | --- |
| Aggiornamenti e chiarimenti | Nella sezione Guardrail aggiuntivi, sono state aggiunte informazioni RCPs e chiarito le eccezioni. | 8 agosto 2025 |
| Pubblicazione iniziale | — | 23 luglio 2024 |

# AWS Glossario delle linee guida prescrittive

I seguenti sono termini di uso comune nelle strategie, nelle guide e nei modelli forniti da AWS Prescriptive Guidance. Per suggerire voci, utilizza il link Fornisci feedback alla fine del glossario.

## Numeri

7 R

Sette strategie di migrazione comuni per trasferire le applicazioni sul cloud. Queste strategie si basano sulle 5 R identificate da Gartner nel 2011 e sono le seguenti:

- Refactor/re-architect — Sposta un'applicazione e modificane l'architettura sfruttando appieno le funzionalità native del cloud per migliorare l'agilità, le prestazioni e la scalabilità. Ciò comporta in genere la portabilità del sistema operativo e del database. Esempio: migra il tuo database Oracle locale all'edizione Amazon PostgreSQL-Compatible Aurora.
- Ridefinire la piattaforma (lift and reshape): trasferisci un'applicazione nel cloud e introduci un certo livello di ottimizzazione per sfruttare le funzionalità del cloud. Esempio: migra il tuo database Oracle locale ad Amazon Relational Database Service (Amazon RDS) per Oracle in. Cloud AWS
- Riacquistare (drop and shop): passa a un prodotto diverso, in genere effettuando la transizione da una licenza tradizionale a un modello SaaS. Esempio: migra il tuo sistema di gestione delle relazioni con i clienti (CRM) su. Salesforce.com
- Eseguire il rehosting (lift and shift): trasferisci un'applicazione sul cloud senza apportare modifiche per sfruttare le funzionalità del cloud. Esempio: migra il tuo database Oracle locale su Oracle su un'istanza EC2 in. Cloud AWS
- Trasferire (eseguire il rehosting a livello hypervisor): trasferisci l'infrastruttura sul cloud senza acquistare nuovo hardware, riscrivere le applicazioni o modificare le operazioni esistenti. Esegui la migrazione dei server da una piattaforma locale a un servizio cloud per la stessa piattaforma. Esempio: migra un'applicazione suMicrosoft Hyper-V. AWS
- Riesaminare (mantenere): mantieni le applicazioni nell'ambiente di origine. Queste potrebbero includere applicazioni che richiedono una rifattorizzazione significativa che desideri rimandare a un momento successivo e applicazioni legacy che desideri mantenere, perché non vi è alcuna giustificazione aziendale per effettuarne la migrazione.
- Ritirare: disattiva o rimuovi le applicazioni che non sono più necessarie nell'ambiente di origine.

# A

A2A () Agent-to-Agent

Un protocollo statico per la collaborazione tra agenti che supporta la delega delle attività e il trasferimento dello stato.

ABAC

Vedi controllo degli accessi basato sugli attributi.

servizi astratti

Vedi servizi gestiti.

ACIDO

Vedi atomicità, consistenza, isolamento, durata.

migrazione attiva-attiva

Un metodo di migrazione del database in cui i database di origine e di destinazione vengono mantenuti sincronizzati (utilizzando uno strumento di replica bidirezionale o operazioni di doppia scrittura) ed entrambi i database gestiscono le transazioni provenienti dalle applicazioni di connessione durante la migrazione. Questo metodo supporta la migrazione in piccoli batch controllati anziché richiedere una conversione una tantum. È più flessibile ma richiede più lavoro rispetto alla migrazione attiva-passiva.

migrazione attiva-passiva

Un metodo di migrazione del database in cui i database di origine e di destinazione vengono mantenuti sincronizzati, ma solo il database di origine gestisce le transazioni provenienti dalle applicazioni di connessione mentre i dati vengono replicati nel database di destinazione. Il database di destinazione non accetta alcuna transazione durante la migrazione.

Agente

Un sistema di intelligenza artificiale in grado di ragionare, pianificare e intraprendere azioni in modo autonomo utilizzando strumenti per raggiungere gli obiettivi.

Agente Ops

Pratiche operative per la creazione, il test, l'implementazione e l'esecuzione di agenti di intelligenza artificiale in produzione su larga scala.

funzione aggregata

Una funzione SQL che opera su un gruppo di righe e calcola un singolo valore restituito per il gruppo. Esempi di funzioni aggregate includono `SUM` e. `MAX`

Intelligenza artificiale

Vedi intelligenza artificiale.

AIOps

Guarda le operazioni di intelligenza artificiale.

anonimizzazione

Il processo di eliminazione permanente delle informazioni personali in un set di dati. L'anonimizzazione può aiutare a proteggere la privacy personale. I dati anonimi non sono più considerati dati personali.

anti-modello

Una soluzione utilizzata frequentemente per un problema ricorrente in cui la soluzione è controproducente, inefficace o meno efficace di un'alternativa.

controllo delle applicazioni

Un approccio alla sicurezza che consente l'uso solo di applicazioni approvate per proteggere un sistema dal malware.

portfolio di applicazioni

Una raccolta di informazioni dettagliate su ogni applicazione utilizzata da un'organizzazione, compresi i costi di creazione e manutenzione dell'applicazione e il relativo valore aziendale. Queste informazioni sono fondamentali per il processo di scoperta e analisi del portfolio e aiutano a identificare e ad assegnare la priorità alle applicazioni da migrare, modernizzare e ottimizzare.

intelligenza artificiale (IA)

Il campo dell'informatica dedicato all'uso delle tecnologie informatiche per svolgere funzioni cognitive tipicamente associate agli esseri umani, come l'apprendimento, la risoluzione di problemi e il riconoscimento di schemi. Per ulteriori informazioni, consulta la sezione Che cos'è l'intelligenza artificiale?

operazioni di intelligenza artificiale (AIOps)

Il processo di utilizzo delle tecniche di machine learning per risolvere problemi operativi, ridurre gli incidenti operativi e l'intervento umano e aumentare la qualità del servizio. Per ulteriori

informazioni su come viene utilizzato AIOps nella strategia di migrazione AWS , consulta la guida all'integrazione delle operazioni.

crittografia asimmetrica

Un algoritmo di crittografia che utilizza una coppia di chiavi, una chiave pubblica per la crittografia e una chiave privata per la decrittografia. Puoi condividere la chiave pubblica perché non viene utilizzata per la decrittografia, ma l'accesso alla chiave privata deve essere altamente limitato.

atomicità, consistenza, isolamento, durabilità (ACID)

Un insieme di proprietà del software che garantiscono la validità dei dati e l'affidabilità operativa di un database, anche in caso di errori, interruzioni di corrente o altri problemi.

Controllo degli accessi basato su attributi (ABAC)

La pratica di creare autorizzazioni dettagliate basate su attributi utente, come reparto, ruolo professionale e nome del team. Per ulteriori informazioni, consulta ABAC for AWS nella documentazione AWS Identity and Access Management (IAM).

fonte di dati autorevole

Una posizione in cui è archiviata la versione principale dei dati, considerata la fonte di informazioni più affidabile. È possibile copiare i dati dalla fonte di dati autorevole in altre posizioni allo scopo di elaborarli o modificarli, ad esempio anonimizzandoli, oscurandoli o pseudonimizzandoli.

Zona di disponibilità

Una posizione distinta all'interno di un edificio Regione AWS che è isolata dai guasti in altre zone di disponibilità e offre una connettività di rete economica e a bassa latenza verso altre zone di disponibilità nella stessa regione.

AWS Cloud Adoption Framework (CAF)AWS

Un framework di linee guida e best practice AWS per aiutare le organizzazioni a sviluppare un piano efficiente ed efficace per passare con successo al cloud. AWS CAF organizza le linee guida in sei aree di interesse chiamate prospettive: business, persone, governance, piattaforma, sicurezza e operazioni. Le prospettive relative ad azienda, persone e governance si concentrano sulle competenze e sui processi aziendali; le prospettive relative alla piattaforma, alla sicurezza e alle operazioni si concentrano sulle competenze e sui processi tecnici. Ad esempio, la prospettiva relativa alle persone si rivolge alle parti interessate che gestiscono le risorse umane (HR), le funzioni del personale e la gestione del personale. In questa prospettiva, AWS CAF fornisce linee guida per lo sviluppo delle persone, la formazione e le comunicazioni per aiutare a preparare

l'organizzazione all'adozione del cloud di successo. Per ulteriori informazioni, consulta il sito web di AWS CAF e il white paper AWS CAF.

AWS Workload Qualification Framework (WQF)AWS

Uno strumento che valuta i carichi di lavoro di migrazione dei database, consiglia strategie di migrazione e fornisce stime del lavoro. AWS WQF è incluso in (). AWS Schema Conversion Tool AWS SCT Analizza gli schemi di database e gli oggetti di codice, il codice dell'applicazione, le dipendenze e le caratteristiche delle prestazioni e fornisce report di valutazione.

# B

bot difettoso

Un bot che ha lo scopo di disturbare o causare danni a individui o organizzazioni.

BCP

Vedi la pianificazione della continuità operativa.

grafico comportamentale

Una vista unificata, interattiva dei comportamenti delle risorse e delle interazioni nel tempo. Puoi utilizzare un grafico comportamentale con Amazon Detective per esaminare tentativi di accesso non riusciti, chiamate API sospette e azioni simili. Per ulteriori informazioni, consulta Dati in un grafico comportamentale nella documentazione di Detective.

sistema big-endian

Un sistema che memorizza per primo il byte più importante. Vedi anche endianness.

Classificazione binaria

Un processo che prevede un risultato binario (una delle due classi possibili). Ad esempio, il modello di machine learning potrebbe dover prevedere problemi come "Questa e-mail è spam o non è spam?" o "Questo prodotto è un libro o un'auto?"

filtro Bloom

Una struttura di dati probabilistica ed efficiente in termini di memoria che viene utilizzata per verificare se un elemento fa parte di un set.

blue/green dispiegamento

Una strategia di implementazione in cui si creano due ambienti separati ma identici. La versione corrente dell'applicazione viene eseguita in un ambiente (blu) e la nuova versione dell'applicazione nell'altro ambiente (verde). Questa strategia consente di ripristinare rapidamente il sistema con un impatto minimo.

bot

Un'applicazione software che esegue attività automatizzate su Internet e simula l'attività o l'interazione umana. Alcuni bot sono utili o utili, come i web crawler che indicizzano le informazioni su Internet. Alcuni altri bot, noti come bot dannosi, hanno lo scopo di disturbare o causare danni a individui o organizzazioni.

botnet

Reti di bot infettate da malware e controllate da un'unica parte, nota come bot herder o bot operator. Le botnet sono il meccanismo più noto per scalare i bot e il loro impatto.

ramo

Un'area contenuta di un repository di codice. Il primo ramo creato in un repository è il ramo principale. È possibile creare un nuovo ramo a partire da un ramo esistente e quindi sviluppare funzionalità o correggere bug al suo interno. Un ramo creato per sviluppare una funzionalità viene comunemente detto ramo di funzionalità. Quando la funzionalità è pronta per il rilascio, il ramo di funzionalità viene ricongiunto al ramo principale. Per ulteriori informazioni, consulta Informazioni sulle filiali (documentazione). GitHub

accesso break-glass

In circostanze eccezionali e tramite una procedura approvata, un mezzo rapido per consentire a un utente di accedere a un sito a Account AWS cui in genere non dispone delle autorizzazioni necessarie. Per ulteriori informazioni, consulta l'indicatore Implementare le procedure break-glass nella guida. AWS Well-Architected

strategia brownfield

L'infrastruttura esistente nell'ambiente. Quando si adotta una strategia brownfield per un'architettura di sistema, si progetta l'architettura in base ai vincoli dei sistemi e dell'infrastruttura attuali. Per l'espansione dell'infrastruttura esistente, è possibile combinare strategie brownfield e greenfield.

cache del buffer

L'area di memoria in cui sono archiviati i dati a cui si accede con maggiore frequenza.

capacità di business

Azioni intraprese da un'azienda per generare valore (ad esempio vendite, assistenza clienti o marketing). Le architetture dei microservizi e le decisioni di sviluppo possono essere guidate dalle capacità aziendali. Per ulteriori informazioni, consulta la sezione Organizzazione in base alle funzionalità aziendali del whitepaper Esecuzione di microservizi containerizzati su AWS.

pianificazione della continuità operativa (BCP)

Un piano che affronta il potenziale impatto di un evento che comporta l'interruzione dell'attività, come una migrazione su larga scala, sulle operazioni e consente a un'azienda di riprendere rapidamente le operazioni.

# C

CAF

Vedi AWS Cloud Adoption Framework.

implementazione canaria

Il rilascio lento e incrementale di una versione agli utenti finali. Quando sei sicuro, distribuisci la nuova versione e sostituisci la versione corrente nella sua interezza.

CoE

Vedi Cloud Center of Excellence.

CDC

Vedi Change Data Capture.

Change Data Capture (CDC)

Il processo di tracciamento delle modifiche a un'origine dati, ad esempio una tabella di database, e di registrazione dei metadati relativi alla modifica. È possibile utilizzare CDC per vari scopi, ad esempio il controllo o la replica delle modifiche in un sistema di destinazione per mantenere la sincronizzazione.

ingegneria del caos

Introduzione intenzionale di guasti o eventi dirompenti per testare la resilienza di un sistema. Puoi usare AWS Fault Injection Service (AWS FIS) per eseguire esperimenti che stressano i tuoi AWS carichi di lavoro e valutarne la risposta.

CI/CD

Vedi integrazione continua e distribuzione continua.

classificazione

Un processo di categorizzazione che aiuta a generare previsioni. I modelli di ML per problemi di classificazione prevedono un valore discreto. I valori discreti sono sempre distinti l'uno dall'altro. Ad esempio, un modello potrebbe dover valutare se in un'immagine è presente o meno un'auto.

Sviluppatore cittadino

Un utente aziendale che crea applicazioni di intelligenza artificiale utilizzando piattaforme senza code/low codice senza competenze tecniche specializzate.

crittografia lato client

Crittografia dei dati localmente, prima che il bersaglio li Servizio AWS riceva.

centro di eccellenza del cloud (CCoE)

Un team multidisciplinare che guida le iniziative di adozione del cloud in tutta l'organizzazione, tra cui lo sviluppo di best practice per il cloud, la mobilitazione delle risorse, la definizione delle tempistiche di migrazione e la guida dell'organizzazione attraverso trasformazioni su larga scala. Per ulteriori informazioni, consulta i post di CCoE sull' Cloud AWS Enterprise Strategy Blog.

cloud computing

La tecnologia cloud generalmente utilizzata per l'archiviazione remota di dati e la gestione dei dispositivi IoT. Il cloud computing è generalmente collegato alla tecnologia di edge computing.

modello operativo cloud

In un'organizzazione IT, il modello operativo utilizzato per creare, maturare e ottimizzare uno o più ambienti cloud. Per ulteriori informazioni, consulta Building your Cloud Operating Model.

fasi di adozione del cloud

Le quattro fasi che le organizzazioni in genere attraversano quando migrano verso Cloud AWS:

- Progetto: esecuzione di alcuni progetti relativi al cloud per scopi di dimostrazione e apprendimento
- Fondamento: effettuare investimenti fondamentali per dimensionare l'adozione del cloud (ad esempio, creazione di una zona di destinazione, definizione di un CCoE, definizione di un modello operativo)
- Migrazione: migrazione di singole applicazioni

- Re-invention — Ottimizzazione di prodotti e servizi e innovazione nel cloud

Queste fasi sono state definite da Stephen Orban nel post del blog The Journey Toward Cloud-First & the Stages of Adoption sul blog Enterprise Strategy. Cloud AWS Per informazioni sulla loro relazione con la strategia di AWS migrazione, consulta la guida alla preparazione alla migrazione.

CMDB

Vedi database di gestione della configurazione.

repository di codice

Una posizione in cui il codice di origine e altri asset, come documentazione, esempi e script, vengono archiviati e aggiornati attraverso processi di controllo delle versioni. Gli archivi cloud più comuni includono GitHub oBitbucket Cloud. Ogni versione del codice è denominata ramo. In una struttura a microservizi, ogni repository è dedicato a una singola funzionalità. Una singola CI/CD pipeline può utilizzare più repository.

cache fredda

Una cache del buffer vuota, non ben popolata o contenente dati obsoleti o irrilevanti. Ciò influisce sulle prestazioni perché l'istanza di database deve leggere dalla memoria o dal disco principale, il che richiede più tempo rispetto alla lettura dalla cache del buffer.

dati freddi

Dati a cui si accede raramente e che in genere sono storici. Quando si eseguono interrogazioni di questo tipo di dati, le interrogazioni lente sono in genere accettabili. Lo spostamento di questi dati su livelli o classi di storage meno costosi e con prestazioni inferiori può ridurre i costi.

visione artificiale (CV)

Un campo dell'intelligenza artificiale che utilizza l'apprendimento automatico per analizzare ed estrarre informazioni da formati visivi come immagini e video digitali. Ad esempio, Amazon SageMaker AI fornisce algoritmi di elaborazione delle immagini per CV.

deriva della configurazione

Per un carico di lavoro, una modifica della configurazione rispetto allo stato previsto. Potrebbe causare la non conformità del carico di lavoro e in genere è graduale e involontaria.

database di gestione della configurazione (CMDB)

Un repository che archivia e gestisce le informazioni su un database e il relativo ambiente IT, inclusi i componenti hardware e software e le relative configurazioni. In genere si utilizzano i dati di un CMDB nella fase di individuazione e analisi del portafoglio della migrazione.

Pacchetto di conformità

Una raccolta di AWS Config regole e azioni correttive che puoi assemblare per personalizzare i controlli di conformità e sicurezza. È possibile distribuire un pacchetto di conformità come singola entità in una regione Account AWS and o all'interno di un'organizzazione utilizzando un modello YAML. Per ulteriori informazioni, consulta i Conformance Pack nella documentazione. AWS Config

integrazione e distribuzione continue () CI/CD

Il processo di automazione delle fasi di origine, compilazione, test, gestione temporanea e produzione del processo di rilascio del software. CI/CD viene comunemente descritto come una pipeline. CI/CD può aiutarvi ad automatizzare i processi, migliorare la produttività, migliorare la qualità del codice e velocizzare le consegne. Per ulteriori informazioni, consulta Vantaggi della distribuzione continua. CD può anche significare continuous deployment (implementazione continua). Per ulteriori informazioni, consulta Distribuzione continua e implementazione continua a confronto.

CV

Vedi visione artificiale.

# D

dati a riposo

Dati stazionari nella rete, ad esempio i dati archiviati.

classificazione dei dati

Un processo per identificare e classificare i dati nella rete in base alla loro criticità e sensibilità. È un componente fondamentale di qualsiasi strategia di gestione dei rischi di sicurezza informatica perché consente di determinare i controlli di protezione e conservazione appropriati per i dati. La classificazione dei dati è un componente del pilastro della sicurezza nel AWS Well-Architected Framework. Per ulteriori informazioni, consulta Classificazione dei dati.

deriva dei dati

Una variazione significativa tra i dati di produzione e i dati utilizzati per addestrare un modello di machine learning o una modifica significativa dei dati di input nel tempo. La deriva dei dati può ridurre la qualità, l'accuratezza e l'equità complessive nelle previsioni dei modelli ML.

dati in transito

Dati che si spostano attivamente attraverso la rete, ad esempio tra le risorse di rete.

rete di dati

Un framework architettonico che fornisce la proprietà distribuita e decentralizzata dei dati con gestione e governance centralizzate.

riduzione al minimo dei dati

Il principio della raccolta e del trattamento dei soli dati strettamente necessari. Praticare la riduzione al minimo dei dati in the Cloud AWS può ridurre i rischi per la privacy, i costi e l'impronta di carbonio delle analisi.

perimetro dei dati

Una serie di barriere preventive nell' AWS ambiente che aiutano a garantire che solo le identità attendibili accedano alle risorse attendibili delle reti previste. Per ulteriori informazioni, consulta Building a data perimeter on. AWS

pre-elaborazione dei dati

Trasformare i dati grezzi in un formato che possa essere facilmente analizzato dal modello di ML. La pre-elaborazione dei dati può comportare la rimozione di determinate colonne o righe e l'eliminazione di valori mancanti, incoerenti o duplicati.

provenienza dei dati

Il processo di tracciamento dell'origine e della cronologia dei dati durante il loro ciclo di vita, ad esempio il modo in cui i dati sono stati generati, trasmessi e archiviati.

soggetto dei dati

Un individuo i cui dati vengono raccolti ed elaborati.

data warehouse

Un sistema di gestione dei dati che supporta la business intelligence, come l'analisi. I data warehouse contengono in genere grandi quantità di dati storici e vengono generalmente utilizzati per interrogazioni e analisi.

linguaggio di definizione del database (DDL)

Istruzioni o comandi per creare o modificare la struttura di tabelle e oggetti in un database.

linguaggio di manipolazione del database (DML)

Istruzioni o comandi per modificare (inserire, aggiornare ed eliminare) informazioni in un database.

DDL

Vedi linguaggio di definizione del database.

deep ensemble

Combinare più modelli di deep learning per la previsione. È possibile utilizzare i deep ensemble per ottenere una previsione più accurata o per stimare l'incertezza nelle previsioni.

deep learning

Un sottocampo del ML che utilizza più livelli di reti neurali artificiali per identificare la mappatura tra i dati di input e le variabili target di interesse.

difesa in profondità

Un approccio alla sicurezza delle informazioni in cui una serie di meccanismi e controlli di sicurezza sono accuratamente stratificati su una rete di computer per proteggere la riservatezza, l'integrità e la disponibilità della rete e dei dati al suo interno. Quando si adotta questa strategia AWS, si aggiungono più controlli a diversi livelli della AWS Organizations struttura per proteggere le risorse. Ad esempio, un approccio di difesa approfondita potrebbe combinare autenticazione a più fattori, segmentazione della rete e crittografia.

amministratore delegato

In AWS Organizations, un servizio compatibile può registrare un account AWS membro per amministrare gli account dell'organizzazione e gestire le autorizzazioni per quel servizio. Questo account è denominato amministratore delegato per quel servizio specifico. Per ulteriori informazioni e un elenco di servizi compatibili, consulta Servizi che funzionano con AWS Organizations nella documentazione di AWS Organizations .

implementazione

Il processo di creazione di un'applicazione, di nuove funzionalità o di correzioni di codice disponibili nell'ambiente di destinazione. L'implementazione prevede l'applicazione di modifiche in una base di codice, seguita dalla creazione e dall'esecuzione di tale base di codice negli ambienti applicativi.

Ambiente di sviluppo

Vedi ambiente.

controllo di rilevamento

Un controllo di sicurezza progettato per rilevare, registrare e avvisare dopo che si è verificato un evento. Questi controlli rappresentano una seconda linea di difesa e avvisano l'utente in caso di eventi di sicurezza che aggirano i controlli preventivi in vigore. Per ulteriori informazioni, consulta Controlli di rilevamento in Implementazione dei controlli di sicurezza in AWS.

mappatura del flusso di valore dello sviluppo (DVSM)

Un processo utilizzato per identificare e dare priorità ai vincoli che influiscono negativamente sulla velocità e sulla qualità nel ciclo di vita dello sviluppo del software. DVSM estende il processo di mappatura del flusso di valore originariamente progettato per pratiche di produzione snella. Si concentra sulle fasi e sui team necessari per creare e trasferire valore attraverso il processo di sviluppo del software.

gemello digitale

Una rappresentazione virtuale di un sistema reale, ad esempio un edificio, una fabbrica, un'attrezzatura industriale o una linea di produzione. I gemelli digitali supportano la manutenzione predittiva, il monitoraggio remoto e l'ottimizzazione della produzione.

tabella delle dimensioni

In uno schema a stella, una tabella più piccola che contiene gli attributi dei dati quantitativi in una tabella dei fatti. Gli attributi della tabella delle dimensioni sono in genere campi di testo o numeri discreti che si comportano come testo. Questi attributi vengono comunemente utilizzati per il vincolo delle query, il filtraggio e l'etichettatura dei set di risultati.

disastro

Un evento che impedisce a un carico di lavoro o a un sistema di raggiungere gli obiettivi aziendali nella sua sede principale di implementazione. Questi eventi possono essere disastri naturali, guasti tecnici o il risultato di azioni umane, come errori di configurazione involontari o attacchi di malware.

disaster recovery (DR)

La strategia e il processo utilizzati per ridurre al minimo i tempi di inattività e la perdita di dati causati da un disastro. Per ulteriori informazioni, consulta Disaster Recovery of Workload su AWS: Recovery in the Cloud in the AWS Well-Architected Framework.

DML

Vedi linguaggio di manipolazione del database.

progettazione basata sul dominio

Un approccio allo sviluppo di un sistema software complesso collegandone i componenti a domini in evoluzione, o obiettivi aziendali principali, perseguiti da ciascun componente. Questo concetto è stato introdotto da Eric Evans nel suo libro Domain-Driven Design: Tackling Complexity in the Heart of Software (Boston: Addison-Wesley Professional, 2003). Per informazioni su come utilizzare la progettazione basata sul dominio con lo strangler fig pattern, consulta Modernizzare i servizi Web Microsoft ASP.NET (ASMX) legacy in modo incrementale utilizzando contenitori e Amazon API Gateway.

DOTT.

Vedi disaster recovery.

rilevamento della deriva

Tracciamento delle deviazioni da una configurazione di base. Ad esempio, puoi utilizzarlo AWS CloudFormation per rilevare la deriva nelle risorse di sistema oppure puoi usarlo AWS Control Tower per rilevare cambiamenti nella tua landing zone che potrebbero influire sulla conformità ai requisiti di governance.

DVSM

Vedi la mappatura del flusso di valore dello sviluppo.

# E

EDA

Vedi analisi esplorativa dei dati.

MODIFICA

Vedi scambio elettronico di dati.

edge computing

La tecnologia che aumenta la potenza di calcolo per i dispositivi intelligenti all'edge di una rete IoT. Rispetto al cloud computing, l'edge computing può ridurre la latenza di comunicazione e migliorare i tempi di risposta.

scambio elettronico di dati (EDI)

Lo scambio automatizzato di documenti aziendali tra organizzazioni. Per ulteriori informazioni, vedere Cos'è lo scambio elettronico di dati.

crittografia

Un processo di elaborazione che trasforma i dati in chiaro, leggibili dall'uomo, in testo cifrato.

chiave crittografica

Una stringa crittografica di bit randomizzati generata da un algoritmo di crittografia. Le chiavi possono variare di lunghezza e ogni chiave è progettata per essere imprevedibile e univoca.

endianità

L'ordine in cui i byte vengono archiviati nella memoria del computer. Big-endian i sistemi memorizzano per primi il byte più importante. Little-endian i sistemi memorizzano per primi il byte meno importante.

endpoint

Vedi service endpoint.

servizio endpoint

Un servizio che puoi ospitare in un cloud privato virtuale (VPC) da condividere con altri utenti. Puoi creare un servizio endpoint con AWS PrivateLink e concedere autorizzazioni ad altri Account AWS o a AWS Identity and Access Management (IAM) principali. Questi account o principali possono connettersi al servizio endpoint in privato creando endpoint VPC di interfaccia. Per ulteriori informazioni, consulta Creazione di un servizio endpoint nella documentazione di Amazon Virtual Private Cloud (Amazon VPC).

pianificazione delle risorse aziendali (ERP)

Un sistema che automatizza e gestisce i processi aziendali chiave (come contabilità, MES e gestione dei progetti) per un'azienda.

crittografia envelope

Il processo di crittografia di una chiave di crittografia con un'altra chiave di crittografia. Per ulteriori informazioni, vedete Envelope encryption nella documentazione AWS Key Management Service (AWS KMS).

ambiente

Un'istanza di un'applicazione in esecuzione. Di seguito sono riportati i tipi di ambiente più comuni nel cloud computing:

- ambiente di sviluppo: un'istanza di un'applicazione in esecuzione disponibile solo per il team principale responsabile della manutenzione dell'applicazione. Gli ambienti di sviluppo vengono

utilizzati per testare le modifiche prima di promuoverle negli ambienti superiori. Questo tipo di ambiente viene talvolta definito ambiente di test.

- ambienti inferiori: tutti gli ambienti di sviluppo di un'applicazione, ad esempio quelli utilizzati per le build e i test iniziali.
- ambiente di produzione: un'istanza di un'applicazione in esecuzione a cui gli utenti finali possono accedere. In una CI/CD pipeline, l'ambiente di produzione è l'ultimo ambiente di distribuzione.
- ambienti superiori: tutti gli ambienti a cui possono accedere utenti diversi dal team di sviluppo principale. Si può trattare di un ambiente di produzione, ambienti di preproduzione e ambienti per i test di accettazione da parte degli utenti.

epica

Nelle metodologie agili, categorie funzionali che aiutano a organizzare e dare priorità al lavoro. Le epiche forniscono una descrizione di alto livello dei requisiti e delle attività di implementazione. Ad esempio, le epopee della sicurezza AWS CAF includono la gestione delle identità e degli accessi, i controlli investigativi, la sicurezza dell'infrastruttura, la protezione dei dati e la risposta agli incidenti. Per ulteriori informazioni sulle epiche, consulta la strategia di migrazione AWS , consulta la guida all'implementazione del programma.

ERP

Vedi pianificazione delle risorse aziendali.

analisi esplorativa dei dati (EDA)

Il processo di analisi di un set di dati per comprenderne le caratteristiche principali. Si raccolgono o si aggregano dati e quindi si eseguono indagini iniziali per trovare modelli, rilevare anomalie e verificare ipotesi. L'EDA viene eseguita calcolando statistiche di riepilogo e creando visualizzazioni di dati.

# F

tabella dei fatti

Il tavolo centrale con schema a stella. Memorizza dati quantitativi sulle operazioni aziendali. In genere, una tabella dei fatti contiene due tipi di colonne: quelle che contengono misure e quelle che contengono una chiave esterna per una tabella di dimensioni.

fallire velocemente

Una filosofia che utilizza test frequenti e incrementali per ridurre il ciclo di vita dello sviluppo. È una parte fondamentale di un approccio agile.

limite di isolamento dei guasti

Nel Cloud AWS, un limite come una zona di disponibilità Regione AWS, un piano di controllo o un piano dati che limita l'effetto di un errore e aiuta a migliorare la resilienza dei carichi di lavoro. Per ulteriori informazioni, consulta AWS Fault Isolation Boundaries.

ramo di funzionalità

Vedi filiale.

caratteristiche

I dati di input che usi per fare una previsione. Ad esempio, in un contesto di produzione, le caratteristiche potrebbero essere immagini acquisite periodicamente dalla linea di produzione.

importanza delle caratteristiche

Quanto è importante una caratteristica per le previsioni di un modello. Di solito viene espresso come punteggio numerico che può essere calcolato con varie tecniche, come Shapley Additive Explanations (SHAP) e gradienti integrati. Per ulteriori informazioni, consulta Interpretabilità del modello di machine learning con AWS.

trasformazione delle funzionalità

Per ottimizzare i dati per il processo di machine learning, incluso l'arricchimento dei dati con fonti aggiuntive, il dimensionamento dei valori o l'estrazione di più set di informazioni da un singolo campo di dati. Ciò consente al modello di ML di trarre vantaggio dai dati. Ad esempio, se suddividi la data "2021-05-27 00:15:37" in "2021", "maggio", "giovedì" e "15", puoi aiutare l'algoritmo di apprendimento ad apprendere modelli sfumati associati a diversi componenti dei dati.

prompt con pochi scatti

Fornire a un LLM un numero limitato di esempi che dimostrino l'attività e il risultato desiderato prima di chiedergli di eseguire un'attività simile. Questa tecnica è un'applicazione dell'apprendimento contestuale, in cui i modelli imparano da esempi (immagini) incorporati nei prompt. Few-shot i suggerimenti possono essere efficaci per attività che richiedono una formattazione, un ragionamento o una conoscenza del dominio specifici. Vedi anche zero-shot prompting.

FGAC

Vedi il controllo granulare degli accessi.

controllo granulare degli accessi (FGAC)

L'uso di più condizioni per consentire o rifiutare una richiesta di accesso.

migrazione flash-cut

Un metodo di migrazione del database che utilizza la replica continua dei dati tramite l'acquisizione dei dati delle modifiche per migrare i dati nel più breve tempo possibile, anziché utilizzare un approccio graduale. L'obiettivo è ridurre al minimo i tempi di inattività.

FM

Vedi il modello di base.

modello di fondazione (FM)

Una grande rete neurale di deep learning che si è addestrata su enormi set di dati generalizzati e non etichettati. Le FM sono in grado di eseguire un'ampia varietà di attività generali, come comprendere il linguaggio, generare testo e immagini e conversare in linguaggio naturale. Per ulteriori informazioni, consulta Cosa sono i modelli Foundation.

Gateway FM

Un intermediario centralizzato che controlla e normalizza l'accesso ai modelli di base. Conosciuto anche come gateway LLM.

# G

IA generativa

Un sottoinsieme di modelli di intelligenza artificiale che sono stati addestrati su grandi quantità di dati e che possono utilizzare un semplice messaggio di testo per creare nuovi contenuti e artefatti, come immagini, video, testo e audio. Per ulteriori informazioni, consulta Cos'è l'IA generativa.

blocco geografico

Vedi restrizioni geografiche.

limitazioni geografiche (blocco geografico)

In Amazon CloudFront, un'opzione per impedire agli utenti di determinati paesi di accedere alle distribuzioni di contenuti. Puoi utilizzare un elenco consentito o un elenco di blocco per specificare

i paesi approvati e vietati. Per ulteriori informazioni, consulta Limitare la distribuzione geografica dei contenuti nella CloudFront documentazione.

Flusso di lavoro di GitFlow

Un approccio in cui gli ambienti inferiori e superiori utilizzano rami diversi in un repository di codice di origine. Il flusso di lavoro Gitflow è considerato obsoleto e il flusso di lavoro basato su trunk è l'approccio moderno e preferito.

immagine dorata

Un'istantanea di un sistema o di un software che viene utilizzata come modello per distribuire nuove istanze di quel sistema o software. Ad esempio, nella produzione, un'immagine dorata può essere utilizzata per fornire software su più dispositivi e contribuire a migliorare la velocità, la scalabilità e la produttività nelle operazioni di produzione dei dispositivi.

strategia greenfield

L'assenza di infrastrutture esistenti in un nuovo ambiente. Quando si adotta una strategia greenfield per un'architettura di sistema, è possibile selezionare tutte le nuove tecnologie senza il vincolo della compatibilità con l'infrastruttura esistente, nota anche come brownfield. Per l'espansione dell'infrastruttura esistente, è possibile combinare strategie brownfield e greenfield.

guardrail

Una regola di livello elevato che consente di governare risorse, policy e conformità tra le unità organizzative (OU). I guardrail preventivi applicano le policy per garantire l'allineamento agli standard di conformità. Vengono implementati utilizzando le policy di controllo dei servizi e i limiti delle autorizzazioni IAM. I guardrail di rilevamento rilevano le violazioni delle policy e i problemi di conformità e generano avvisi per porvi rimedio. Sono implementati utilizzando Amazon AWS Config AWS Security Hub CSPM GuardDuty AWS Trusted Advisor, Amazon Inspector e controlli personalizzati AWS Lambda .

guardrail (AI)

Meccanismi di sicurezza che filtrano, convalidano e limitano gli input e gli output degli agenti per contribuire a garantire un comportamento dell'IA responsabile e sicuro.

# H

AH

Vedi disponibilità elevata.

migrazione di database eterogenea

Migrazione del database di origine in un database di destinazione che utilizza un motore di database diverso (ad esempio, da Oracle ad Amazon Aurora). La migrazione eterogenea fa in genere parte di uno sforzo di riprogettazione e la conversione dello schema può essere un'attività complessa. AWS offre AWS SCT che aiuta con le conversioni dello schema.

alta disponibilità (HA)

La capacità di un carico di lavoro di funzionare in modo continuo, senza intervento, in caso di sfide o disastri. I sistemi HA sono progettati per il failover automatico, fornire costantemente prestazioni di alta qualità e gestire carichi e guasti diversi con un impatto minimo sulle prestazioni.

modernizzazione storica

Un approccio utilizzato per modernizzare e aggiornare i sistemi di tecnologia operativa (OT) per soddisfare meglio le esigenze dell'industria manifatturiera. Uno storico è un tipo di database utilizzato per raccogliere e archiviare dati da varie fonti in una fabbrica.

dati di esclusione

Una parte di dati storici etichettati che viene trattenuta da un set di dati utilizzata per addestrare un modello di apprendimento automatico. È possibile utilizzare i dati di holdout per valutare le prestazioni del modello confrontando le previsioni del modello con i dati di holdout.

human-in-the-loop (HITL)

Un modello di flusso di lavoro in cui l'esecuzione degli agenti viene sospesa per la revisione e l'approvazione umana nei punti decisionali critici.

migrazione di database omogenea

Migrazione del database di origine in un database di destinazione che condivide lo stesso motore di database (ad esempio, da Microsoft SQL Server ad Amazon RDS per SQL Server). La migrazione omogenea fa in genere parte di un'operazione di rehosting o ridefinizione della piattaforma. Per migrare lo schema è possibile utilizzare le utilità native del database.

dati caldi

Dati a cui si accede frequentemente, ad esempio dati in tempo reale o dati di traduzione recenti. Questi dati richiedono in genere un livello o una classe di storage ad alte prestazioni per fornire risposte rapide alle query.

hotfix

Una soluzione urgente per un problema critico in un ambiente di produzione. A causa della sua urgenza, un hotfix viene in genere creato al di fuori del tipico DevOps flusso di lavoro di rilascio.

periodo di hypercare

Subito dopo la conversione, il periodo di tempo in cui un team di migrazione gestisce e monitora le applicazioni migrate nel cloud per risolvere eventuali problemi. In genere, questo periodo dura da 1 a 4 giorni. Al termine del periodo di hypercare, il team addetto alla migrazione in genere trasferisce la responsabilità delle applicazioni al team addetto alle operazioni cloud.

## I

IaC

Vedi l'infrastruttura come codice.

Policy basata su identità

Una policy associata a uno o più principi IAM che definisce le relative autorizzazioni all'interno dell' Cloud AWS ambiente.

applicazione inattiva

Un'applicazione che prevede un uso di CPU e memoria medio compreso tra il 5% e il 20% in un periodo di 90 giorni. In un progetto di migrazione, è normale ritirare queste applicazioni o mantenerle on-premise.

IIoT

Vedi Industrial Internet of Things.

infrastruttura immutabile

Un modello che implementa una nuova infrastruttura per i carichi di lavoro di produzione anziché aggiornare, applicare patch o modificare l'infrastruttura esistente. Le infrastrutture immutabili sono intrinsecamente più coerenti, affidabili e prevedibili delle infrastrutture mutabili. Per ulteriori informazioni, consulta la best practice Deploy using immutable infrastructure nel Framework. AWS Well-Architected

VPC in ingresso (ingress)

In un'architettura AWS multi-account, un VPC che accetta, ispeziona e indirizza le connessioni di rete dall'esterno di un'applicazione. Nel documento Architettura di riferimento per la sicurezza di

AWS si consiglia di configurare l'account di rete con VPC in entrata, in uscita e di ispezione per proteggere l'interfaccia bidirezionale tra l'applicazione e Internet in generale.

migrazione incrementale

Una strategia di conversione in cui si esegue la migrazione dell'applicazione in piccole parti anziché eseguire una conversione singola e completa. Ad esempio, inizialmente potresti spostare solo alcuni microservizi o utenti nel nuovo sistema. Dopo aver verificato che tutto funzioni correttamente, puoi spostare in modo incrementale microservizi o utenti aggiuntivi fino alla disattivazione del sistema legacy. Questa strategia riduce i rischi associati alle migrazioni di grandi dimensioni.

Industria 4.0

Un termine introdotto da Klaus Schwab nel 2016 per riferirsi alla modernizzazione dei processi di produzione attraverso progressi in termini di connettività, dati in tempo reale, automazione, analisi e. AI/ML

infrastruttura

Tutte le risorse e gli asset contenuti nell'ambiente di un'applicazione.

infrastruttura come codice (IaC)

Il processo di provisioning e gestione dell'infrastruttura di un'applicazione tramite un insieme di file di configurazione. Il processo IaC è progettato per aiutarti a centralizzare la gestione dell'infrastruttura, a standardizzare le risorse e a dimensionare rapidamente, in modo che i nuovi ambienti siano ripetibili, affidabili e coerenti.

Internet delle cose industriale (IIoT)

L'uso di sensori e dispositivi connessi a Internet nei settori industriali, come quello manifatturiero, energetico, automobilistico, sanitario, delle scienze della vita e dell'agricoltura. Per ulteriori informazioni, consulta Creazione di una strategia di trasformazione digitale dell'Internet delle cose industriale (IIoT).

VPC di ispezione

In un'architettura AWS multi-account, un VPC centralizzato che gestisce le ispezioni del traffico di rete tra VPC (uguali o diversi Regioni AWS), Internet e reti locali. Nel documento Architettura di riferimento per la sicurezza di AWS si consiglia di configurare l'account di rete con VPC in entrata, in uscita e di ispezione per proteggere l'interfaccia bidirezionale tra l'applicazione e Internet in generale.

Internet of Things (IoT)

La rete di oggetti fisici connessi con sensori o processori incorporati che comunicano con altri dispositivi e sistemi tramite Internet o una rete di comunicazione locale. Per ulteriori informazioni, consulta Cos'è l'IoT?

interpretabilità

Una caratteristica di un modello di machine learning che descrive il grado in cui un essere umano è in grado di comprendere in che modo le previsioni del modello dipendono dai suoi input. Per ulteriori informazioni, consulta Interpretabilità del modello di machine learning con. AWS

IoT

Vedi Internet of Things.

libreria di informazioni IT (ITIL)

Una serie di best practice per offrire servizi IT e allinearli ai requisiti aziendali. ITIL fornisce le basi per ITSM.

gestione dei servizi IT (ITSM)

Attività associate alla progettazione, implementazione, gestione e supporto dei servizi IT per un'organizzazione. Per informazioni sull'integrazione delle operazioni cloud con gli strumenti ITSM, consulta la guida all'integrazione delle operazioni.

ITIL

Vedi la libreria di informazioni IT.

ITSM

Vedi Gestione dei servizi IT.

# L

controllo degli accessi basato su etichette (LBAC)

Un'implementazione del controllo di accesso obbligatorio (MAC) in cui agli utenti e ai dati stessi viene assegnato esplicitamente un valore di etichetta di sicurezza. L'intersezione tra l'etichetta di sicurezza utente e l'etichetta di sicurezza dei dati determina quali righe e colonne possono essere visualizzate dall'utente.

zona di destinazione

Una landing zone è un AWS ambiente multi-account ben progettato, scalabile e sicuro. Questo è un punto di partenza dal quale le organizzazioni possono avviare e distribuire rapidamente carichi di lavoro e applicazioni con fiducia nel loro ambiente di sicurezza e infrastruttura. Per ulteriori informazioni sulle zone di destinazione, consulta la sezione Configurazione di un ambiente AWS multi-account sicuro e scalabile.

modello linguistico di grandi dimensioni (LLM)

Un modello di intelligenza artificiale di deep learning preaddestrato su una grande quantità di dati. Un LLM può svolgere più attività, come rispondere a domande, riepilogare documenti, tradurre testo in altre lingue e completare frasi. Per ulteriori informazioni, consulta Cosa sono gli LLM.

migrazione su larga scala

Una migrazione di 300 o più server.

BIANCO

Vedi controllo degli accessi basato su etichette.

Privilegio minimo

La best practice di sicurezza per la concessione delle autorizzazioni minime richieste per eseguire un'attività. Per ulteriori informazioni, consulta Applicazione delle autorizzazioni del privilegio minimo nella documentazione di IAM.

eseguire il rehosting (lift and shift)

Vedi 7 R.

sistema little-endian

Un sistema che memorizza per primo il byte meno importante. Vedi anche endianità.

LLM

Vedi modello linguistico di grandi dimensioni.

ambienti inferiori

Vedi ambiente.

# M

machine learning (ML)

Un tipo di intelligenza artificiale che utilizza algoritmi e tecniche per il riconoscimento e l'apprendimento di schemi. Il machine learning analizza e apprende dai dati registrati, come i dati dell'Internet delle cose (IoT), per generare un modello statistico basato su modelli. Per ulteriori informazioni, consulta la sezione Machine learning.

ramo principale

Vedi filiale.

malware

Software progettato per compromettere la sicurezza o la privacy del computer. Il malware potrebbe interrompere i sistemi informatici, divulgare informazioni sensibili o ottenere accessi non autorizzati. Esempi di malware includono virus, worm, ransomware, trojan horse, spyware e keylogger.

servizi gestiti

Servizi AWS per cui AWS gestisce il livello di infrastruttura, il sistema operativo e le piattaforme e si accede agli endpoint per archiviare e recuperare i dati. Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3) e Amazon DynamoDB sono esempi di servizi gestiti. Questi sono noti anche come servizi astratti.

sistema di esecuzione della produzione (MES)

Un sistema software per tracciare, monitorare, documentare e controllare i processi di produzione che convertono le materie prime in prodotti finiti in officina.

MAP

Vedi Migration Acceleration Program.

MCP

Vedi Model Context Protocol.

Model Context Protocol (MCP)

Un protocollo stateless per la comunicazione tra agenti e strumenti.

Server MCP

Un servizio che espone uno o più strumenti tramite il Model Context Protocol.

meccanismo

Un processo completo in cui si crea uno strumento, si promuove l'adozione dello strumento e quindi si esaminano i risultati per apportare le modifiche. Un meccanismo è un ciclo che si rafforza e si migliora man mano che funziona. Per ulteriori informazioni, vedete Creazione di meccanismi nel AWS Well-Architected Framework.

account membro

Tutti gli account Account AWS diversi dall'account di gestione che fanno parte di un'organizzazione in AWS Organizations. Un account può essere membro di una sola organizzazione alla volta.

MEH

Vedi sistema di esecuzione della produzione.

Message Queuing Telemetry Transport (MQTT)

Un protocollo di comunicazione da macchina a macchina (M2M) leggero, basato sul publish/subscribemodello, per dispositivi IoT con risorse limitate.

microservizio

Un piccolo servizio indipendente che comunica tramite API ben definite ed è in genere di proprietà di piccoli team autonomi. Ad esempio, un sistema assicurativo potrebbe includere microservizi che si riferiscono a funzionalità aziendali, come vendite o marketing, o sottodomini, come acquisti, reclami o analisi. I vantaggi dei microservizi includono agilità, dimensionamento flessibile, facilità di implementazione, codice riutilizzabile e resilienza. Per ulteriori informazioni, consulta Integrazione dei microservizi utilizzando servizi serverless. AWS

architettura di microservizi

Un approccio alla creazione di un'applicazione con componenti indipendenti che eseguono ogni processo applicativo come microservizio. Questi microservizi comunicano tramite un'interfaccia ben definita utilizzando API leggere. Ogni microservizio in questa architettura può essere aggiornato, distribuito e dimensionato per soddisfare la richiesta di funzioni specifiche di un'applicazione. Per ulteriori informazioni, vedere Implementazione dei microservizi su. AWS

Programma di accelerazione della migrazione (MAP)

Un AWS programma che fornisce consulenza, supporto, formazione e servizi per aiutare le organizzazioni a costruire una solida base operativa per il passaggio al cloud e per contribuire a compensare il costo iniziale delle migrazioni. MAP include una metodologia di migrazione per

eseguire le migrazioni precedenti in modo metodico e un set di strumenti per automatizzare e accelerare gli scenari di migrazione comuni.

migrazione su larga scala

Il processo di trasferimento della maggior parte del portfolio di applicazioni sul cloud avviene a ondate, con più applicazioni trasferite a una velocità maggiore in ogni ondata. Questa fase utilizza le migliori pratiche e le lezioni apprese nelle fasi precedenti per implementare una fabbrica di migrazione di team, strumenti e processi per semplificare la migrazione dei carichi di lavoro attraverso l'automazione e la distribuzione agile. Questa è la terza fase della strategia di migrazione AWS.

fabbrica di migrazione

Cross-functional team che semplificano la migrazione dei carichi di lavoro attraverso approcci automatizzati e agili. I team di Migration Factory includono in genere operazioni, analisti e proprietari aziendali, ingegneri addetti alla migrazione, sviluppatori e DevOps professionisti che lavorano nell'ambito degli sprint. Tra il 20% e il 50% di un portfolio di applicazioni aziendali è costituito da schemi ripetuti che possono essere ottimizzati con un approccio di fabbrica. Per ulteriori informazioni, consulta la discussione sulle fabbriche di migrazione e la Guida alla fabbrica di migrazione al cloud in questo set di contenuti.

metadati di migrazione

Le informazioni sull'applicazione e sul server necessarie per completare la migrazione. Ogni modello di migrazione richiede un set diverso di metadati di migrazione. Esempi di metadati di migrazione includono la sottorete, il gruppo di sicurezza e l'account di destinazione. AWS

modello di migrazione

Un'attività di migrazione ripetibile che descrive in dettaglio la strategia di migrazione, la destinazione della migrazione e l'applicazione o il servizio di migrazione utilizzati. Esempio: riorganizza la migrazione su Amazon EC2 AWS con Application Migration Service.

Valutazione del portfolio di migrazione (MPA)

Uno strumento online che fornisce informazioni per la convalida del business case per la migrazione a. Cloud AWS MPA offre una valutazione dettagliata del portfolio (dimensionamento corretto dei server, prezzi, confronto del TCO, analisi dei costi di migrazione) e pianificazione della migrazione (analisi e raccolta dei dati delle applicazioni, raggruppamento delle applicazioni, prioritizzazione delle migrazioni e pianificazione delle ondate). Lo strumento MPA (richiede l'accesso) è disponibile gratuitamente per tutti i AWS consulenti e i consulenti dei partner APN.

valutazione della preparazione alla migrazione (MRA)

Il processo di acquisizione di informazioni sullo stato di preparazione al cloud di un'organizzazione, l'identificazione dei punti di forza e di debolezza e la creazione di un piano d'azione per colmare le lacune identificate, utilizzando il CAF. AWS Per ulteriori informazioni, consulta la guida di preparazione alla migrazione. MRA è la prima fase della strategia di migrazione AWS.

strategia di migrazione

L'approccio utilizzato per migrare un carico di lavoro verso. Cloud AWS Per ulteriori informazioni, consulta la voce 7 R in questo glossario e consulta Mobilita la tua organizzazione per accelerare le migrazioni su larga scala.

ML

Vedi machine learning.

modernizzazione

Trasformazione di un'applicazione obsoleta (legacy o monolitica) e della relativa infrastruttura in un sistema agile, elastico e altamente disponibile nel cloud per ridurre i costi, aumentare l'efficienza e sfruttare le innovazioni. Per ulteriori informazioni, vedere Strategia per la modernizzazione delle applicazioni in. Cloud AWS

valutazione della preparazione alla modernizzazione

Una valutazione che aiuta a determinare la preparazione alla modernizzazione delle applicazioni di un'organizzazione, identifica vantaggi, rischi e dipendenze e determina in che misura l'organizzazione può supportare lo stato futuro di tali applicazioni. Il risultato della valutazione è uno schema dell'architettura di destinazione, una tabella di marcia che descrive in dettaglio le fasi di sviluppo e le tappe fondamentali del processo di modernizzazione e un piano d'azione per colmare le lacune identificate. Per ulteriori informazioni, vedere Valutazione della preparazione alla modernizzazione per le applicazioni in. Cloud AWS

applicazioni monolitiche (monoliti)

Applicazioni eseguite come un unico servizio con processi strettamente collegati. Le applicazioni monolitiche presentano diversi inconvenienti. Se una funzionalità dell'applicazione registra un picco di domanda, l'intera architettura deve essere dimensionata. L'aggiunta o il miglioramento delle funzionalità di un'applicazione monolitica diventa inoltre più complessa man mano che la base di codice cresce. Per risolvere questi problemi, puoi utilizzare un'architettura di microservizi. Per ulteriori informazioni, consulta la sezione Scomposizione dei monoliti in microservizi.

MAPPA

Vedi Migration Portfolio Assessment.

MQTT

Vedi Message Queuing Telemetry Transport.

classificazione multiclasse

Un processo che aiuta a generare previsioni per più classi (prevedendo uno o più di due risultati). Ad esempio, un modello di machine learning potrebbe chiedere "Questo prodotto è un libro, un'auto o un telefono?" oppure "Quale categoria di prodotti è più interessante per questo cliente?"

infrastruttura mutabile

Un modello che aggiorna e modifica l'infrastruttura esistente per i carichi di lavoro di produzione. Per migliorare la coerenza, l'affidabilità e la prevedibilità, il AWS Well-Architected Framework consiglia l'uso di un'infrastruttura immutabile come best practice.

# O

OAC

Vedi Origin Access Control.

QUERCIA

Vedi Origin Access Identity.

OCM

Vedi gestione delle modifiche organizzative.

migrazione offline

Un metodo di migrazione in cui il carico di lavoro di origine viene eliminato durante il processo di migrazione. Questo metodo prevede tempi di inattività prolungati e viene in genere utilizzato per carichi di lavoro piccoli e non critici.

OI

Vedi l'integrazione delle operazioni.

OLA

Vedi accordo a livello operativo.

migrazione online

Un metodo di migrazione in cui il carico di lavoro di origine viene copiato sul sistema di destinazione senza essere messo offline. Le applicazioni connesse al carico di lavoro possono continuare a funzionare durante la migrazione. Questo metodo comporta tempi di inattività pari a zero o comunque minimi e viene in genere utilizzato per carichi di lavoro di produzione critici.

OPC-UA

Vedi Open Process Communications - Unified Architecture.

Comunicazioni a processo aperto - Architettura unificata () OPC-UA

Un protocollo di comunicazione da macchina a macchina (M2M) per l'automazione industriale. OPC-UA fornisce uno standard di interoperabilità con schemi di crittografia, autenticazione e autorizzazione dei dati.

accordo a livello operativo (OLA)

Un accordo che chiarisce quali sono gli impegni reciproci tra i gruppi IT funzionali, a supporto di un accordo sul livello di servizio (SLA).

revisione della prontezza operativa (ORR)

Un elenco di domande e best practice associate che aiutano a comprendere, valutare, prevenire o ridurre la portata degli incidenti e dei possibili guasti. Per ulteriori informazioni, vedere Operational Readiness Reviews (ORR) nel Framework. AWS Well-Architected

tecnologia operativa (OT)

Sistemi hardware e software che interagiscono con l'ambiente fisico per controllare operazioni, apparecchiature e infrastrutture industriali. Nella produzione, l'integrazione di sistemi OT e di tecnologia dell'informazione (IT) è un obiettivo chiave per le trasformazioni dell'Industria 4.0.

integrazione delle operazioni (OI)

Il processo di modernizzazione delle operazioni nel cloud, che prevede la pianificazione, l'automazione e l'integrazione della disponibilità. Per ulteriori informazioni, consulta la guida all'integrazione delle operazioni.

trail organizzativo

Un percorso creato da noi AWS CloudTrail che registra tutti gli eventi di un'organizzazione per tutti Account AWS . AWS Organizations Questo percorso viene creato in ogni Account AWS che

fa parte dell'organizzazione e tiene traccia dell'attività in ogni account. Per ulteriori informazioni, consulta Creazione di un percorso per un'organizzazione nella CloudTrail documentazione.

gestione del cambiamento organizzativo (OCM)

Un framework per la gestione di trasformazioni aziendali importanti e che comportano l'interruzione delle attività dal punto di vista delle persone, della cultura e della leadership. OCM aiuta le organizzazioni a prepararsi e passare a nuovi sistemi e strategie accelerando l'adozione del cambiamento, affrontando i problemi di transizione e promuovendo cambiamenti culturali e organizzativi. Nella strategia di AWS migrazione, questo framework si chiama accelerazione delle persone, a causa della velocità di cambiamento richiesta nei progetti di adozione del cloud. Per ulteriori informazioni, consultare la Guida OCM.

controllo dell'accesso all'origine (OAC)

In CloudFront, un'opzione avanzata per limitare l'accesso per proteggere i contenuti di Amazon Simple Storage Service (Amazon S3). OAC supporta in tutto tutti i bucket S3 Regioni AWS, la crittografia lato server con AWS KMS (SSE-KMS) e le richieste dinamiche PUT e dirette al bucket S3. DELETE

identità di accesso origine (OAI)

Nel CloudFront, un'opzione per limitare l'accesso per proteggere i tuoi contenuti Amazon S3. Quando usi OAI, CloudFront crea un principale con cui Amazon S3 può autenticarsi. I principali autenticati possono accedere ai contenuti in un bucket S3 solo tramite una distribuzione specifica. CloudFront Vedi anche OAC, che fornisce un controllo degli accessi più granulare e avanzato.

ORR

Vedi la revisione della prontezza operativa.

- NON

Vedi la tecnologia operativa.

VPC in uscita (egress)

In un'architettura AWS multi-account, un VPC che gestisce le connessioni di rete avviate dall'interno di un'applicazione. Nel documento Architettura di riferimento per la sicurezza di AWS si consiglia di configurare l'account di rete con VPC in entrata, in uscita e di ispezione per proteggere l'interfaccia bidirezionale tra l'applicazione e Internet in generale.

# P

limite delle autorizzazioni

Una policy di gestione IAM collegata ai principali IAM per impostare le autorizzazioni massime che l'utente o il ruolo possono avere. Per ulteriori informazioni, consulta Limiti delle autorizzazioni nella documentazione di IAM.

informazioni di identificazione personale (PII)

Informazioni che, se visualizzate direttamente o abbinate ad altri dati correlati, possono essere utilizzate per dedurre ragionevolmente l'identità di un individuo. Esempi di informazioni personali includono nomi, indirizzi e informazioni di contatto.

Informazioni che consentono l'identificazione personale degli utenti

Visualizza le informazioni di identificazione personale.

playbook

Una serie di passaggi predefiniti che raccolgono il lavoro associato alle migrazioni, come l'erogazione delle funzioni operative principali nel cloud. Un playbook può assumere la forma di script, runbook automatici o un riepilogo dei processi o dei passaggi necessari per gestire un ambiente modernizzato.

PLC

Vedi controllore logico programmabile.

PLM

Vedi la gestione del ciclo di vita del prodotto.

policy

Un oggetto in grado di definire le autorizzazioni (vedi politica basata sull'identità), specificare le condizioni di accesso (vedi politicabasata sulle risorse) o definire le autorizzazioni massime per tutti gli account di un'organizzazione in (vedi politica di controllo dei servizi). AWS Organizations

persistenza poliglotta

Scelta indipendente della tecnologia di archiviazione di dati di un microservizio in base ai modelli di accesso ai dati e ad altri requisiti. Se i microservizi utilizzano la stessa tecnologia di archiviazione di dati, possono incontrare problemi di implementazione o registrare prestazioni scadenti. I microservizi vengono implementati più facilmente e ottengono prestazioni e scalabilità migliori se utilizzano l'archivio dati più adatto alle loro esigenze.

valutazione del portfolio

Un processo di scoperta, analisi e definizione delle priorità del portfolio di applicazioni per pianificare la migrazione. Per ulteriori informazioni, consulta la pagina Valutazione della preparazione alla migrazione.

predicate

Una condizione di interrogazione che restituisce o, in genere, si trova in una clausola`WHERE`. `true` `false`

predicato pushdown

Una tecnica di ottimizzazione delle query del database che filtra i dati della query prima del trasferimento. Ciò riduce la quantità di dati che devono essere recuperati ed elaborati dal database relazionale e migliora le prestazioni delle query.

controllo preventivo

Un controllo di sicurezza progettato per impedire il verificarsi di un evento. Questi controlli sono la prima linea di difesa per impedire accessi non autorizzati o modifiche indesiderate alla rete. Per ulteriori informazioni, consulta Controlli preventivi in Implementazione dei controlli di sicurezza in AWS.

principale

Un'entità in AWS grado di eseguire azioni e accedere alle risorse. Questa entità è in genere un utente root per un Account AWS ruolo IAM o un utente. Per ulteriori informazioni, consulta Principali in Termini e concetti dei ruoli nella documentazione di IAM.

privacy fin dalla progettazione

Un approccio ingegneristico dei sistemi che tiene conto della privacy durante l'intero processo di sviluppo.

zone ospitate private

Un container che contiene informazioni su come si desidera che Amazon Route 53 risponda alle query DNS per un dominio e i relativi sottodomini all'interno di uno o più VPC. Per ulteriori informazioni, consulta Utilizzo delle zone ospitate private nella documentazione di Route 53.

controllo proattivo

Un controllo di sicurezza progettato per impedire l'implementazione di risorse non conformi. Questi controlli analizzano le risorse prima del loro provisioning. Se la risorsa non è conforme al

controllo, non viene fornita. Per ulteriori informazioni, consulta la guida di riferimento sui controlli nella AWS Control Tower documentazione e consulta Controlli proattivi in Implementazione dei controlli di sicurezza su. AWS

gestione del ciclo di vita del prodotto (PLM)

La gestione dei dati e dei processi di un prodotto durante l'intero ciclo di vita, dalla progettazione, sviluppo e lancio, attraverso la crescita e la maturità, fino al declino e alla rimozione.

Ambiente di produzione

Vedi ambiente.

controllore logico programmabile (PLC)

Nella produzione, un computer altamente affidabile e adattabile che monitora le macchine e automatizza i processi di produzione.

concatenamento rapido

Utilizzo dell'output di un prompt LLM come input per il prompt successivo per generare risposte migliori. Questa tecnica viene utilizzata per suddividere un'attività complessa in sottoattività o per perfezionare o espandere iterativamente una risposta preliminare. Aiuta a migliorare l'accuratezza e la pertinenza delle risposte di un modello e consente risultati più granulari e personalizzati.

pseudonimizzazione

Il processo di sostituzione degli identificatori personali in un set di dati con valori segnaposto. La pseudonimizzazione può aiutare a proteggere la privacy personale. I dati pseudonimizzati sono ancora considerati dati personali.

publish/subscribe (pub/sub)

Un modello che consente comunicazioni asincrone tra microservizi per migliorare la scalabilità e la reattività. Ad esempio, in un MES basato su microservizi, un microservizio può pubblicare messaggi di eventi su un canale a cui altri microservizi possono abbonarsi. Il sistema può aggiungere nuovi microservizi senza modificare il servizio di pubblicazione.

# Q

Piano di query

Una serie di passaggi, come le istruzioni, utilizzati per accedere ai dati in un sistema di database relazionale SQL.

regressione del piano di query

Quando un ottimizzatore del servizio di database sceglie un piano non ottimale rispetto a prima di una determinata modifica all'ambiente di database. Questo può essere causato da modifiche a statistiche, vincoli, impostazioni dell'ambiente, associazioni dei parametri di query e aggiornamenti al motore di database.

# R

Matrice RACI

Vedi responsabile, responsabile, consultato, informato (RACI).

RAG

Vedi Retrieval Augmented Generation.

ransomware

Un software dannoso progettato per bloccare l'accesso a un sistema informatico o ai dati fino a quando non viene effettuato un pagamento.

Matrice RASCI

Vedi responsabile, responsabile, consultato, informato (RACI).

RCAC

Vedi controllo dell'accesso a righe e colonne.

replica di lettura

Una copia di un database utilizzata per scopi di sola lettura. È possibile indirizzare le query alla replica di lettura per ridurre il carico sul database principale.

riprogettare

Vedi 7 Rs.

obiettivo del punto di ripristino (RPO)

Il periodo di tempo massimo accettabile dall'ultimo punto di ripristino dei dati. Questo determina ciò che si considera una perdita di dati accettabile tra l'ultimo punto di ripristino e l'interruzione del servizio.

obiettivo del tempo di ripristino (RTO)

Il ritardo massimo accettabile tra l'interruzione del servizio e il ripristino del servizio.

rifattorizzare

Vedi 7 R.

Region

Una raccolta di AWS risorse in un'area geografica. Ciascuna Regione AWS è isolata e indipendente dalle altre per fornire tolleranza agli errori, stabilità e resilienza. Per ulteriori informazioni, consulta Specificare cosa può usare Regioni AWS il tuo account.

regressione

Una tecnica di ML che prevede un valore numerico. Ad esempio, per risolvere il problema "A che prezzo verrà venduta questa casa?" un modello di ML potrebbe utilizzare un modello di regressione lineare per prevedere il prezzo di vendita di una casa sulla base di dati noti sulla casa (ad esempio, la metratura).

riospitare

Vedi 7 R.

rilascio

In un processo di implementazione, l'atto di promuovere modifiche a un ambiente di produzione.

trasferisco

Vedi 7 Rs.

ripiattaforma

Vedi 7 Rs.

riacquisto

Vedi 7 Rs.

resilienza

La capacità di un'applicazione di resistere o ripristinare le interruzioni. L'elevata disponibilità e il disaster recovery sono considerazioni comuni quando si pianifica la resilienza in. Cloud AWSPer ulteriori informazioni, vedere Cloud AWS Resilience.

policy basata su risorse

Una policy associata a una risorsa, ad esempio un bucket Amazon S3, un endpoint o una chiave di crittografia. Questo tipo di policy specifica a quali principali è consentito l'accesso, le azioni supportate e qualsiasi altra condizione che deve essere soddisfatta.

matrice di assegnazione di responsabilità (RACI)

Una matrice che definisce i ruoli e le responsabilità di tutte le parti coinvolte nelle attività di migrazione e nelle operazioni cloud. Il nome della matrice deriva dai tipi di responsabilità definiti nella matrice: responsabile (R), responsabile (A), consultato (C) e informato (I). Il tipo di supporto (S) è facoltativo. Se includi il supporto, la matrice viene chiamata matrice RASCI e, se la escludi, viene chiamata matrice RACI.

controllo reattivo

Un controllo di sicurezza progettato per favorire la correzione di eventi avversi o deviazioni dalla baseline di sicurezza. Per ulteriori informazioni, consulta Controlli reattivi in Implementazione dei controlli di sicurezza in AWS.

retain

Vedi 7 R.

andare in pensione

Vedi 7 Rs.

Retrieval Augmented Generation (RAG)

Una tecnologia di intelligenza artificiale generativa in cui un LLM fa riferimento a una fonte di dati autorevole esterna alle sue fonti di dati di formazione prima di generare una risposta. Ad esempio, un modello RAG potrebbe eseguire una ricerca semantica nella knowledge base o nei dati personalizzati di un'organizzazione. Per ulteriori informazioni, consulta Cos'è il RAG.

rotazione

Processo di aggiornamento periodico di un segreto per rendere più difficile l'accesso alle credenziali da parte di un utente malintenzionato.

controllo dell'accesso a righe e colonne (RCAC)

L'uso di espressioni SQL di base e flessibili con regole di accesso definite. RCAC è costituito da autorizzazioni di riga e maschere di colonna.

RPO

Vedi obiettivo del punto di ripristino.

VERSO

Vedi obiettivo del tempo di ripristino.

runbook

Un insieme di procedure manuali o automatizzate necessarie per eseguire un'attività specifica. In genere sono progettati per semplificare operazioni o procedure ripetitive con tassi di errore elevati.

# S

SAML 2.0

Uno standard aperto utilizzato da molti provider di identità (IdPs). Questa funzionalità abilita il single sign-on (SSO) federato, in modo che gli utenti possano accedere Console di gestione AWS o chiamare le operazioni AWS API senza che tu debba creare un utente in IAM per tutti i membri dell'organizzazione. Per ulteriori informazioni sulla federazione basata su SAML 2.0, consulta Informazioni sulla federazione basata su SAML 2.0 nella documentazione di IAM.

SCADA

Vedi controllo di supervisione e acquisizione dati.

SCP

Vedi la politica di controllo del servizio.

Secret

In Gestione dei segreti AWS, informazioni riservate o riservate, come una password o le credenziali utente, archiviate in forma crittografata. È costituito dal valore segreto e dai relativi metadati. Il valore segreto può essere binario, una stringa singola o più stringhe. Per ulteriori informazioni, consulta Cosa c'è in un segreto di Secrets Manager? nella documentazione di Secrets Manager.

sicurezza fin dalla progettazione

Un approccio di ingegneria dei sistemi che tiene conto della sicurezza durante l'intero processo di sviluppo.

controllo di sicurezza

Un guardrail tecnico o amministrativo che impedisce, rileva o riduce la capacità di un autore di minacce di sfruttare una vulnerabilità di sicurezza. Esistono quattro tipi principali di controlli di sicurezza: preventivi, investigativi, reattivi e proattivi.

rafforzamento della sicurezza

Il processo di riduzione della superficie di attacco per renderla più resistente agli attacchi. Può includere azioni come la rimozione di risorse che non sono più necessarie, l'implementazione di best practice di sicurezza che prevedono la concessione del privilegio minimo o la disattivazione di funzionalità non necessarie nei file di configurazione.

sistema di gestione delle informazioni e degli eventi di sicurezza (SIEM)

Strumenti e servizi che combinano sistemi di gestione delle informazioni di sicurezza (SIM) e sistemi di gestione degli eventi di sicurezza (SEM). Un sistema SIEM raccoglie, monitora e analizza i dati da server, reti, dispositivi e altre fonti per rilevare minacce e violazioni della sicurezza e generare avvisi.

automazione della risposta alla sicurezza

Un'azione predefinita e programmata progettata per rispondere o porre rimedio automaticamente a un evento di sicurezza. Queste automazioni fungono da controlli di sicurezza investigativi o reattivi che aiutano a implementare le migliori pratiche di sicurezza. AWS Esempi di azioni di risposta automatizzate includono la modifica di un gruppo di sicurezza VPC, l'applicazione di patch a un'istanza Amazon EC2 o la rotazione delle credenziali.

Crittografia lato server

Crittografia dei dati a destinazione, da parte di chi li riceve. Servizio AWS

Policy di controllo dei servizi (SCP)

Una policy che fornisce il controllo centralizzato sulle autorizzazioni per tutti gli account di un'organizzazione in AWS Organizations. Le SCP definiscono i guardrail o fissano i limiti alle azioni che un amministratore può delegare a utenti o ruoli. Puoi utilizzare le SCP come elenchi consentiti o elenchi di rifiuto, per specificare quali servizi o azioni sono consentiti o proibiti. Per ulteriori informazioni, consulta le politiche di controllo del servizio nella AWS Organizations documentazione.

endpoint del servizio

L'URL del punto di ingresso per un Servizio AWS. Puoi utilizzare l'endpoint per connetterti a livello di programmazione al servizio di destinazione. Per ulteriori informazioni, consulta Endpoint del Servizio AWS nei Riferimenti generali di AWS.

accordo sul livello di servizio (SLA)

Un accordo che chiarisce ciò che un team IT promette di offrire ai propri clienti, ad esempio l'operatività e le prestazioni del servizio.

indicatore del livello di servizio (SLI)

Misurazione di un aspetto prestazionale di un servizio, ad esempio il tasso di errore, la disponibilità o la velocità effettiva.

obiettivo a livello di servizio (SLO)

Una metrica target che rappresenta lo stato di un servizio, misurato da un indicatore del livello di servizio.

Modello di responsabilità condivisa

Un modello che descrive la responsabilità condivisa AWS per la sicurezza e la conformità del cloud. AWS è responsabile della sicurezza del cloud, mentre tu sei responsabile della sicurezza nel cloud. Per ulteriori informazioni, consulta Modello di responsabilità condivisa.

Shadow AI

Applicazioni di intelligenza artificiale non autorizzate create o utilizzate al di fuori dei canali regolamentati all'interno di un'organizzazione.

SIEM

Vedi il sistema di gestione delle informazioni e degli eventi sulla sicurezza.

punto di errore singolo (SPOF)

Un guasto in un singolo componente critico di un'applicazione che può disturbare il sistema.

SLAM

Vedi il contratto sul livello di servizio.

SLI

Vedi l'indicatore del livello di servizio.

LENTA

Vedi obiettivo del livello di servizio.

modello split-and-seed

Un modello per dimensionare e accelerare i progetti di modernizzazione. Man mano che vengono definite nuove funzionalità e versioni dei prodotti, il team principale si divide per creare nuovi team di prodotto. Questo aiuta a dimensionare le capacità e i servizi dell'organizzazione, migliora la produttività degli sviluppatori e supporta una rapida innovazione. Per ulteriori informazioni, vedere Approccio graduale alla modernizzazione delle applicazioni in. Cloud AWS

SPOF

Vedi punto di errore singolo.

schema a stella

Una struttura organizzativa di database che utilizza un'unica tabella dei fatti di grandi dimensioni per archiviare i dati transazionali o misurati e utilizza una o più tabelle dimensionali più piccole per memorizzare gli attributi dei dati. Questa struttura è progettata per l'uso in un data warehouse o per scopi di business intelligence.

modello del fico strangolatore

Un approccio alla modernizzazione dei sistemi monolitici mediante la riscrittura e la sostituzione incrementali delle funzionalità del sistema fino alla disattivazione del sistema legacy. Questo modello utilizza l'analogia di una pianta di fico che cresce fino a diventare un albero robusto e alla fine annienta e sostituisce il suo ospite. Il modello è stato introdotto da Martin Fowler come metodo per gestire il rischio durante la riscrittura di sistemi monolitici. Per un esempio di come applicare questo modello, consulta Modernizzare i servizi Web Microsoft ASP.NET (ASMX) legacy in modo incrementale utilizzando contenitori e Amazon API Gateway.

sottorete

Un intervallo di indirizzi IP nel VPC. Una sottorete deve risiedere in una singola zona di disponibilità.

controllo di supervisione e acquisizione dati (SCADA)

Nella produzione, un sistema che utilizza hardware e software per monitorare gli asset fisici e le operazioni di produzione.

crittografia simmetrica

Un algoritmo di crittografia che utilizza la stessa chiave per crittografare e decrittografare i dati.

test sintetici

Test di un sistema in modo da simulare le interazioni degli utenti per rilevare potenziali problemi o monitorare le prestazioni. Puoi usare Amazon CloudWatch Synthetics per creare questi test.

prompt di sistema

Una tecnica per fornire contesto, istruzioni o linee guida a un LLM per indirizzarne il comportamento. I prompt di sistema aiutano a impostare il contesto e stabilire regole per le interazioni con gli utenti.

# T

tag

Key-value coppie che fungono da metadati per l'organizzazione delle risorse. AWS Con i tag è possibile a gestire, identificare, organizzare, cercare e filtrare le risorse. Per ulteriori informazioni, consulta Tagging delle risorse AWS.

variabile di destinazione

Il valore che stai cercando di prevedere nel machine learning supervisionato. Questo è indicato anche come variabile di risultato. Ad esempio, in un ambiente di produzione la variabile di destinazione potrebbe essere un difetto del prodotto.

elenco di attività

Uno strumento che viene utilizzato per tenere traccia dei progressi tramite un runbook. Un elenco di attività contiene una panoramica del runbook e un elenco di attività generali da completare. Per ogni attività generale, include la quantità stimata di tempo richiesta, il proprietario e lo stato di avanzamento.

ambiente di test

Vedi ambiente.

training

Fornire dati da cui trarre ispirazione dal modello di machine learning. I dati di training devono contenere la risposta corretta. L'algoritmo di apprendimento trova nei dati di addestramento i pattern che mappano gli attributi dei dati di input al target (la risposta che si desidera prevedere). Produce un modello di ML che acquisisce questi modelli. Puoi quindi utilizzare il modello di ML per creare previsioni su nuovi dati di cui non si conosce il target.

strumento

Una funzione o API che un agente può richiamare per eseguire operazioni in sistemi esterni.

Transit Gateway

Un hub di transito di rete che è possibile utilizzare per collegare i VPC e le reti on-premise. Per ulteriori informazioni, consulta Cos'è un gateway di transito nella AWS Transit Gateway documentazione.

flusso di lavoro basato su trunk

Un approccio in cui gli sviluppatori creano e testano le funzionalità localmente in un ramo di funzionalità e quindi uniscono tali modifiche al ramo principale. Il ramo principale viene quindi integrato negli ambienti di sviluppo, preproduzione e produzione, in sequenza.

Accesso attendibile

Concessione delle autorizzazioni a un servizio specificato dall'utente per eseguire attività all'interno dell'organizzazione AWS Organizations e nei suoi account per conto dell'utente. Il servizio attendibile crea un ruolo collegato al servizio in ogni account, quando tale ruolo è necessario, per eseguire attività di gestione per conto dell'utente. Per ulteriori informazioni, consulta Utilizzo AWS Organizations con altri AWS servizi nella AWS Organizations documentazione.

regolazione

Modificare alcuni aspetti del processo di training per migliorare la precisione del modello di ML. Ad esempio, puoi addestrare il modello di ML generando un set di etichette, aggiungendo etichette e quindi ripetendo questi passaggi più volte con impostazioni diverse per ottimizzare il modello.

team da due pizze

Una piccola DevOps squadra che puoi sfamare con due pizze. Un team composto da due persone garantisce la migliore opportunità possibile di collaborazione nello sviluppo del software.

# U

incertezza

Un concetto che si riferisce a informazioni imprecise, incomplete o sconosciute che possono minare l'affidabilità dei modelli di machine learning predittivi. Esistono due tipi di incertezza:

l'incertezza epistemica, che è causata da dati limitati e incompleti, mentre l'incertezza aleatoria è causata dal rumore e dalla casualità insiti nei dati.

compiti indifferenziati

Conosciuto anche come sollevamento di carichi pesanti, è un lavoro necessario per creare e far funzionare un'applicazione, ma che non apporta valore diretto all'utente finale né offre vantaggi competitivi. Esempi di attività indifferenziate includono l'approvvigionamento, la manutenzione e la pianificazione della capacità.

ambienti superiori

Vedi ambiente.

# V

vacuum

Un'operazione di manutenzione del database che prevede la pulizia dopo aggiornamenti incrementali per recuperare lo spazio di archiviazione e migliorare le prestazioni.

controllo delle versioni

Processi e strumenti che tengono traccia delle modifiche, ad esempio le modifiche al codice di origine in un repository.

Peering VPC

Una connessione tra due VPC che consente di instradare il traffico tramite indirizzi IP privati. Per ulteriori informazioni, consulta Che cos'è il peering VPC? nella documentazione di Amazon VPC.

vulnerabilità

Un difetto software o hardware che compromette la sicurezza del sistema.

# W

cache calda

Una cache del buffer che contiene dati correnti e pertinenti a cui si accede frequentemente. L'istanza di database può leggere dalla cache del buffer, il che richiede meno tempo rispetto alla lettura dalla memoria dal disco principale.

dati caldi

Dati a cui si accede raramente. Quando si eseguono interrogazioni di questo tipo di dati, in genere sono accettabili interrogazioni moderatamente lente.

funzione finestra

Una funzione SQL che esegue un calcolo su un gruppo di righe che si riferiscono in qualche modo al record corrente. Le funzioni della finestra sono utili per l'elaborazione di attività, come il calcolo di una media mobile o l'accesso al valore delle righe in base alla posizione relativa della riga corrente.

Carico di lavoro

Una raccolta di risorse e codice che fornisce valore aziendale, ad esempio un'applicazione rivolta ai clienti o un processo back-end.

flusso di lavoro

Gruppi funzionali in un progetto di migrazione responsabili di una serie specifica di attività. Ogni flusso di lavoro è indipendente ma supporta gli altri flussi di lavoro del progetto. Ad esempio, il flusso di lavoro del portfolio è responsabile della definizione delle priorità delle applicazioni, della pianificazione delle ondate e della raccolta dei metadati di migrazione. Il flusso di lavoro del portfolio fornisce queste risorse al flusso di lavoro di migrazione, che quindi migra i server e le applicazioni.

VERME

Vedi scrivere una volta, leggere molti.

WQF

Vedi AWS Workload Qualification Framework.

scrivi una volta, leggi molte (WORM)

Un modello di storage che scrive i dati una sola volta e ne impedisce l'eliminazione o la modifica. Gli utenti autorizzati possono leggere i dati tutte le volte che è necessario, ma non possono modificarli. Questa infrastruttura di archiviazione dei dati è considerata immutabile.

# Z

exploit zero-day

Un attacco, in genere malware, che sfrutta una vulnerabilità zero-day.

vulnerabilità zero-day

Un difetto o una vulnerabilità assoluta in un sistema di produzione. Gli autori delle minacce possono utilizzare questo tipo di vulnerabilità per attaccare il sistema. Gli sviluppatori vengono spesso a conoscenza della vulnerabilità causata dall'attacco.

prompt zero-shot

Fornire a un LLM le istruzioni per eseguire un'attività ma non esempi (immagini) che possano aiutarla. Il LLM deve utilizzare le sue conoscenze pre-addestrate per gestire l'attività. L'efficacia del prompt zero-shot dipende dalla complessità dell'attività e dalla qualità del prompt. Vedi anche few-shot prompting.

applicazione zombie

Un'applicazione che prevede un utilizzo CPU e memoria inferiore al 5%. In un progetto di migrazione, è normale ritirare queste applicazioni.

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.