



Rafforzare la sicurezza IAM Roles Anywhere utilizzando controlli di accesso basati su certificati

# AWS Guida prescrittiva



# AWS Guida prescrittiva: Rafforzare la sicurezza IAM Roles Anywhere utilizzando controlli di accesso basati su certificati

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

I marchi e l'immagine commerciale di Amazon non possono essere utilizzati in relazione a prodotti o servizi che non siano di Amazon, in una qualsiasi modalità che possa causare confusione tra i clienti o in una qualsiasi modalità che denigri o discrediti Amazon. Tutti gli altri marchi non di proprietà di Amazon sono di proprietà dei rispettivi proprietari, che possono o meno essere affiliati, collegati o sponsorizzati da Amazon.

# Table of Contents

|                                                                                                 |    |
|-------------------------------------------------------------------------------------------------|----|
| Introduzione .....                                                                              | 1  |
| Destinatari principali .....                                                                    | 3  |
| Obiettivi .....                                                                                 | 3  |
| Concetti chiave .....                                                                           | 4  |
| Privilegio minimo .....                                                                         | 4  |
| Autenticazione basata su certificati .....                                                      | 5  |
| Ancoraggi di fiducia e modelli di fiducia .....                                                 | 5  |
| Credenziali di sicurezza temporanee .....                                                       | 6  |
| Autorizzazioni a doppio livello in IAM .....                                                    | 6  |
| AWS Aiutante per le credenziali .....                                                           | 7  |
| Architecture .....                                                                              | 8  |
| Opzione 1: Assumi qualsiasi ruolo .....                                                         | 11 |
| Opzione 2: Assumi un ruolo specifico .....                                                      | 13 |
| Domande frequenti .....                                                                         | 17 |
| Cosa sono gli attributi dei certificati e perché sono importanti? IAM Roles Anywhere .....      | 17 |
| Come funzionano le credenziali temporanee? IAM Roles Anywhere .....                             | 17 |
| Quali sono i vantaggi dell'utilizzo? IAM Roles Anywhere .....                                   | 17 |
| Come si IAM Roles Anywhere integra con l'infrastruttura di certificati esistente? .....         | 18 |
| Quali sono le migliori pratiche per implementare il privilegio minimo? IAM Roles Anywhere ..... | 18 |
| Risorse e passaggi successivi .....                                                             | 19 |
| Risorse .....                                                                                   | 19 |
| AWS Autorità di certificazione privata risorse .....                                            | 19 |
| IAM Roles Anywhere e risorse IAM .....                                                          | 19 |
| Appendice: Politiche di esempio .....                                                           | 21 |
| Applicazione 1 .....                                                                            | 21 |
| Applicazione 2 .....                                                                            | 22 |
| Cronologia dei documenti .....                                                                  | 25 |
| Glossario .....                                                                                 | 26 |
| # .....                                                                                         | 26 |
| A .....                                                                                         | 27 |
| B .....                                                                                         | 30 |
| C .....                                                                                         | 32 |
| D .....                                                                                         | 35 |
| E .....                                                                                         | 39 |

|         |       |
|---------|-------|
| F ..... | 41    |
| G ..... | 43    |
| H ..... | 44    |
| I ..... | 46    |
| L ..... | 48    |
| M ..... | 49    |
| O ..... | 54    |
| P ..... | 56    |
| Q ..... | 59    |
| R ..... | 60    |
| S ..... | 63    |
| T ..... | 67    |
| U ..... | 68    |
| V ..... | 69    |
| W ..... | 69    |
| Z ..... | 71    |
| .....   | lxxii |

# Rafforzare la sicurezza IAM Roles Anywhere utilizzando controlli di accesso basati su certificati

Alberto Sagrado Amador, Amazon Web Services

Luglio 2025 (cronologia del documento)

Man mano che le organizzazioni espandono la propria presenza sul cloud e adottano l'automazione, è sempre più importante gestire l'accesso sicuro per le identità non umane, come applicazioni, server e contenitori. Gli approcci tradizionali utilizzano credenziali a lungo termine o segreti codificati, ma questi approcci possono creare rischi per la sicurezza e costi operativi. [AWS Identity and Access Management Roles Anywhere](#) affronta queste sfide consentendo ai carichi di lavoro esterni all'UE di accedere Cloud AWS alle AWS risorse in modo sicuro tramite certificati [X.509](#) (Wikipedia) anziché credenziali a lungo termine.

Organizations di solito si scontra con la proliferazione delle chiavi di accesso, la complessa rotazione delle credenziali e la limitata capacità di applicare controlli di accesso granulari. I moderni framework di sicurezza enfatizzano [i principi Zero Trust](#), just-in-time l'accesso e il principio del privilegio minimo, tutti elementi che possono essere raggiunti attraverso una corretta implementazione dell'autenticazione basata su certificati.

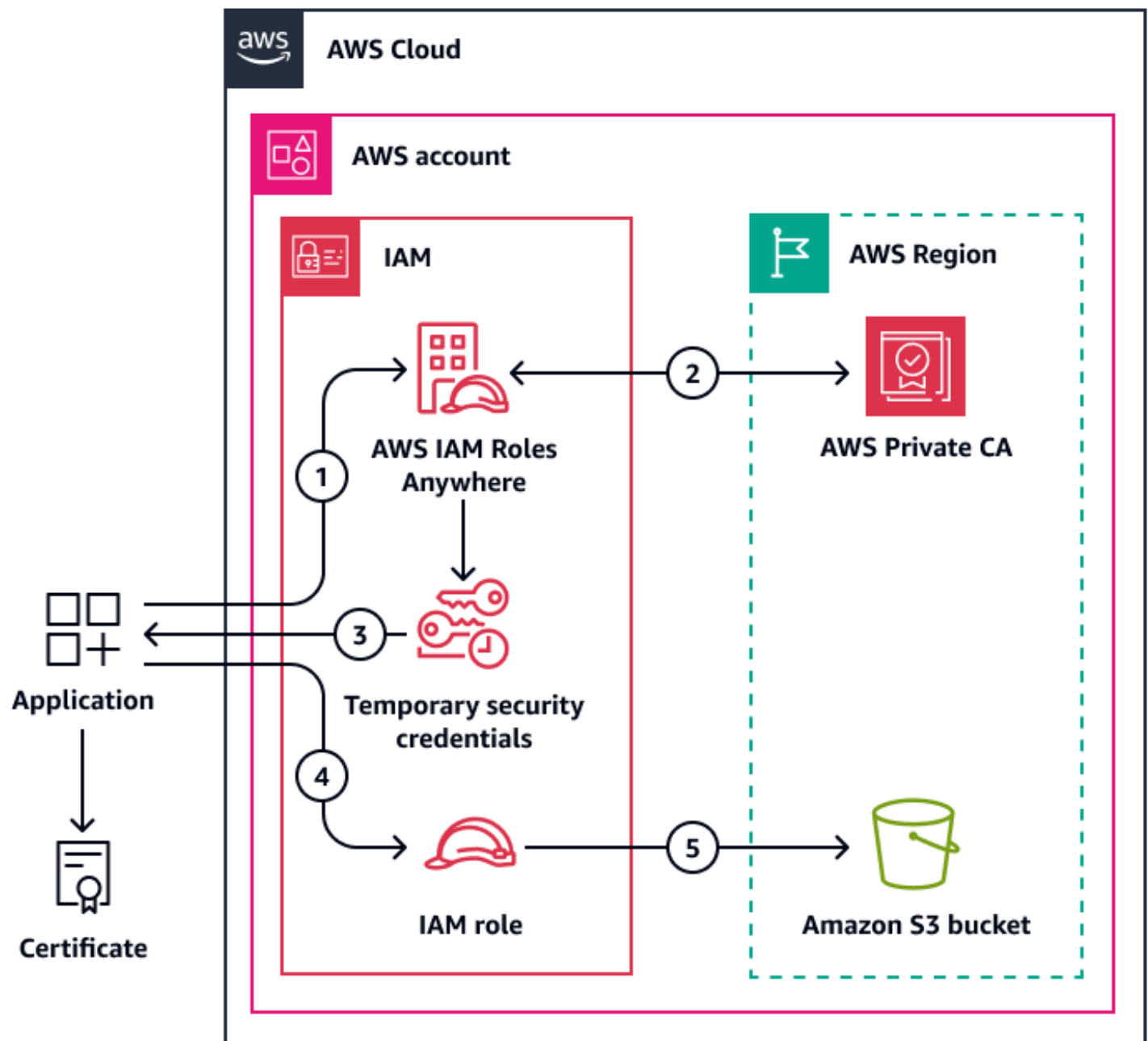
[Questa guida dimostra come migliorare la sicurezza gestendo efficacemente gli attributi dei certificati e le relazioni IAM Roles Anywhere di fiducia tra i ruoli \(IAM\).](#) [AWS Identity and Access Management](#)

Utilizza un esempio pratico di architettura per dimostrare come implementare controlli di accesso granulari e applicare il principio del privilegio minimo nelle sessioni. IAM Roles Anywhere

[L'architettura utilizza and \(\). IAM Roles Anywhere](#) [AWS Autorità di certificazione privata](#) [AWS Private CA](#) AWS Private CA funge da ancoraggio di fiducia e [AWS Certificate Manager \(ACM\)](#) gestisce i certificati. Questa base riflette le configurazioni di sicurezza del mondo reale e le loro implicazioni.

Senza configurazioni di policy adeguate per i ruoli IAM, qualsiasi certificato emesso da AWS Private CA potrebbe essere potenzialmente utilizzato per assumere ruoli. Ciò può creare significative vulnerabilità di sicurezza, tra cui assunzione di ruoli non autorizzati, violazioni dei dati e compromissione delle credenziali. Questa guida mostra come contribuire a mitigare questi rischi attraverso una corretta configurazione delle politiche e la gestione degli attributi dei certificati.

Il diagramma seguente mostra il flusso di lavoro con cui un'applicazione può richiedere l'accesso IAM Roles Anywhere e quindi eseguire le azioni consentite sulla destinazione. Account AWS



Il diagramma mostra il flusso di lavoro seguente:

1. L'applicazione richiede credenziali di sicurezza temporanee IAM Roles Anywhere e fornisce il relativo certificato per l'autenticazione.
2. IAM Roles Anywhere utilizza una relazione di fiducia con cui autenticare l'applicazione. AWS Private CA
3. IAM Roles Anywhere genera un file JSON che contiene le credenziali di sicurezza temporanee e lo restituisce all'applicazione.

#### 4. Utilizzando le credenziali di sicurezza temporanee, l'applicazione assume un ruolo IAM in. Account AWS

L'applicazione esegue le azioni consentite dalle policy associate al ruolo IAM e all'account. Ad esempio, potrebbe accedere a un bucket Amazon Simple Storage Service (Amazon S3).

## Destinatari principali

Questa guida è destinata agli architetti del cloud, agli ingegneri della sicurezza e agli DevOps ingegneri che implementano i controlli di accesso per ambienti cloud ibridi o automatizzano la gestione delle autorizzazioni per le identità non umane. Questa guida può anche aiutarti a rispettare le normative o a soddisfare le migliori pratiche di sicurezza. Per comprendere i concetti e i consigli contenuti in questa guida, è necessario conoscere quanto segue:

- Nozioni di base su IAM
- Infrastruttura a chiave pubblica (PKI) e gestione dei certificati X.509
- Principi di sicurezza Zero Trust e accesso con privilegi minimi
- Servizi AWS per l'autenticazione basata su certificati, ad esempio e IAM Roles Anywhere AWS Private CA

## Obiettivi

L'utilizzo IAM Roles Anywhere di certificati X.509 per l'autenticazione può fornire i seguenti risultati aziendali chiave:

- Sicurezza avanzata: elimina i rischi associati all'uso di credenziali a lungo termine
- Sovraccarico operativo ridotto: automatizza la gestione e la rotazione delle credenziali
- Migliore conformità: fornisce audit trail dettagliati e applica l'accesso con privilegi minimi
- Gestione scalabile: centralizza il controllo degli accessi in ambienti ibridi
- Efficienza in termini di costi: riduce i costi associati agli sforzi di risposta agli incidenti di sicurezza e alla complessità della gestione

# Concetti chiave per l'utilizzo dei controlli di accesso basati su certificati in AWS

I controlli di accesso basati su certificati richiedono la comprensione di diversi concetti di autenticazione e autorizzazione interdipendenti. AWS Ad esempio, il principio del privilegio minimo determina l'ambito delle autorizzazioni concesse tramite l'autenticazione basata su certificati, che influisce direttamente sul ruolo (IAM) e sulla progettazione delle politiche. AWS Identity and Access Management L'autenticazione basata su certificati di per sé si basa sulla convalida dei certificati X.509 rispetto ai trust anchor configurati, che definiscono la catena di fiducia crittografica per la verifica dei certificati. Le credenziali di sicurezza temporanee generate attraverso questo processo hanno caratteristiche specifiche del ciclo di vita che influiscono sulla gestione delle sessioni e sulle strategie di rotazione delle credenziali. Inoltre, AWS Identity and Access Management Roles Anywhere implementa un modello di autorizzazione a doppio livello in cui sia le policy dei ruoli IAM che le configurazioni dei profili devono autorizzare l'accesso. Senza comprendere come interagiscono questi concetti, le implementazioni possono causare errori di autenticazione, accessi con privilegi eccessivi o lacune di sicurezza nella catena di convalida dei certificati. Questi concetti costituiscono la base tecnica necessaria per configurare correttamente le relazioni di fiducia, i limiti di autorizzazione e i cicli di vita delle credenziali nei sistemi di controllo degli accessi basati su certificati.

AWS

Questa sezione contiene i seguenti argomenti:

- [Privilegio minimo](#)
- [Autenticazione basata su certificati](#)
- [Ancoraggi di fiducia e modelli di fiducia](#)
- [Credenziali di sicurezza temporanee](#)
- [Autorizzazioni a doppio livello in IAM](#)
- [AWS Aiutante per le credenziali](#)

## Privilegio minimo

Il principio del privilegio minimo è un concetto di sicurezza che consiglia di concedere il livello minimo di accesso (o autorizzazioni) necessario agli utenti, ai programmi o ai sistemi per svolgere le proprie attività. La filosofia guida è semplice: minore è il numero di autorizzazioni di cui dispone un'entità, minore è il rischio di danni dolosi o accidentali.



Nel contesto di AWS, questo principio è particolarmente rilevante. AWS fornisce un'ampia gamma di risorse e servizi, dalle macchine virtuali alle risorse di archiviazione. Durante la creazione e la gestione AWS dell'infrastruttura, l'applicazione del principio del privilegio minimo assicura che ogni entità (un utente, un servizio o un'applicazione) disponga solo delle autorizzazioni necessarie per funzionare correttamente e nient'altro.

L'implementazione del privilegio minimo in AWS offre i seguenti vantaggi:

- **Sicurezza:** limitando l'accesso, riduci il potenziale impatto di una violazione della sicurezza. Se un utente o un servizio dispone di autorizzazioni minime, la portata del danno si riduce notevolmente.
- **Conformità:** molti quadri normativi richiedono controlli di accesso rigorosi. Il rispetto del principio del privilegio minimo aiuta a soddisfare questi requisiti di conformità.
- **Semplicità operativa:** la gestione delle autorizzazioni può diventare complessa. L'applicazione del privilegio minimo può mantenere le configurazioni il più semplici e gestibili possibile.

## Autenticazione basata su certificati

L'autenticazione basata su certificati utilizza certificati digitali per verificare l'identità di un dispositivo, servizio o applicazione. I certificati X.509 contengono attributi che identificano l'entità e sono firmati da un'autorità di certificazione attendibile. Questo metodo di autenticazione elimina la necessità di credenziali statiche e fornisce un modo crittograficamente sicuro per stabilire la fiducia.

Mentre l'autenticazione basata sull'identità si basa su credenziali direttamente associate a un [ruolo](#) o [utente](#) IAM, l'autenticazione basata sui certificati utilizza i certificati X.509 per stabilire l'identità. L'autenticazione basata su certificati offre vantaggi negli ambienti ibridi in quanto offre un livello di sicurezza più elevato, una rotazione automatizzata delle credenziali e la capacità di codificare gli attributi che possono essere utilizzati per un controllo granulare degli accessi.

## Ancoraggi di fiducia e modelli di fiducia

È possibile stabilire un rapporto di fiducia tra l'autorità di certificazione (CA) IAM Roles Anywhere e l'autorità di certificazione (CA) creando un ancoraggio di fiducia. Un trust anchor è un riferimento a una fonte CA esterna [AWS Private CA](#) o a una fonte CA esterna. I carichi di lavoro esterni vengono AWS autenticati con il trust anchor utilizzando certificati emessi dalla CA affidabile in cambio di credenziali temporanee. AWS Possono esserci più trust anchor in uno. Account AWS Per ulteriori informazioni, consulta il [modello IAM Roles Anywhere di fiducia](#). Il modello di fiducia definisce il modo

in cui i certificati vengono convalidati e quali attributi del certificato sono necessari per una corretta autenticazione.

## Credenziali di sicurezza temporanee

Le credenziali di sicurezza temporanee forniscono un accesso limitato nel tempo alle AWS risorse, che in genere durano da pochi minuti a diverse ore. A differenza delle chiavi di accesso a lungo termine, queste credenziali scadono automaticamente. Ciò riduce significativamente il rischio di compromissione delle credenziali e semplifica la gestione degli accessi tra sistemi distribuiti. Per ulteriori informazioni sulle credenziali temporanee, consulta la sezione [Richiedere ai carichi di lavoro di utilizzare credenziali temporanee con ruoli IAM per accedere alle AWS](#) best practice nella documentazione IAM.

## Autorizzazioni a doppio livello in IAM

IAM Roles Anywhere implementa un modello di autorizzazione a doppio livello attraverso la combinazione di ruoli e profili IAM. In un profilo, puoi definire policy di sessione IAM che limitano le autorizzazioni create per una sessione. Un profilo può avere molti ruoli IAM ma solo una policy di sessione. Il modello di autorizzazione a doppio livello offre una maggiore sicurezza richiedendo che le autorizzazioni siano esplicitamente consentite su entrambi i livelli prima di concedere l'accesso. Di seguito sono riportati i due livelli:

- Il livello IAM roles definisce quanto segue:
  - Politiche di fiducia che determinano quale entità può assumere il ruolo
  - Politiche di autorizzazione che specificano a quali AWS risorse il ruolo può accedere e quali azioni può eseguire
  - Elementi condizionali che possono limitare ulteriormente l'accesso in base a criteri specifici
- Il livello IAM Roles Anywhere dei profili esegue le seguenti operazioni:
  - Definisce quali ruoli IAM possono essere assunti tramite IAM Roles Anywhere
  - Fornisce controlli aggiuntivi per l'assunzione dei ruoli
  - Funge da filtro di autorizzazione, anche se il ruolo IAM stesso consente un accesso più ampio

Ad esempio, se un ruolo IAM consente l'accesso ad Amazon Simple Storage Service (Amazon S3) e Amazon DynamoDB ma il profilo consente solo l'accesso ad Amazon S3, l'applicazione può accedere

solo alle risorse Amazon S3. Questo approccio a due livelli applica il principio del privilegio minimo richiedendo un'autorizzazione esplicita in entrambi i livelli.

## AWS Aiutante per le credenziali

Utilizzando [Credential Helper](#) (GitHub) for IAM Roles Anywhere, definisci tramite AWS Command Line Interface (AWS CLI) quale ancoraggio, profilo e ruolo di trust desideri utilizzare per consentire all'applicazione di accedere alle risorse. AWS Di seguito è riportato un esempio di chiamata che utilizza lo strumento AWS Credential Helper:

```
./aws_signing_helper credential-process  
  --certificate <Path to certificate>  
  --private-key <Path to private key>  
  --trust-anchor-arn <Trust anchor ARN>  
  --profile-arn <Profile 1 ARN>  
  --role-arn <Role 1 ARN>
```

Questo strumento è compatibile con la `credential_process` funzionalità disponibile in tutta la lingua. SDKs Se utilizzate con un AWS SDK, queste credenziali si aggiornano automaticamente prima della scadenza, senza richiedere alcuna implementazione aggiuntiva per il rinnovo delle credenziali. Credential Helper gestisce il processo di creazione di una firma con il certificato e di chiamata all'endpoint per ottenere le credenziali di sessione. Quindi, restituisce le credenziali di sicurezza temporanee al processo di chiamata in un formato JSON standard.

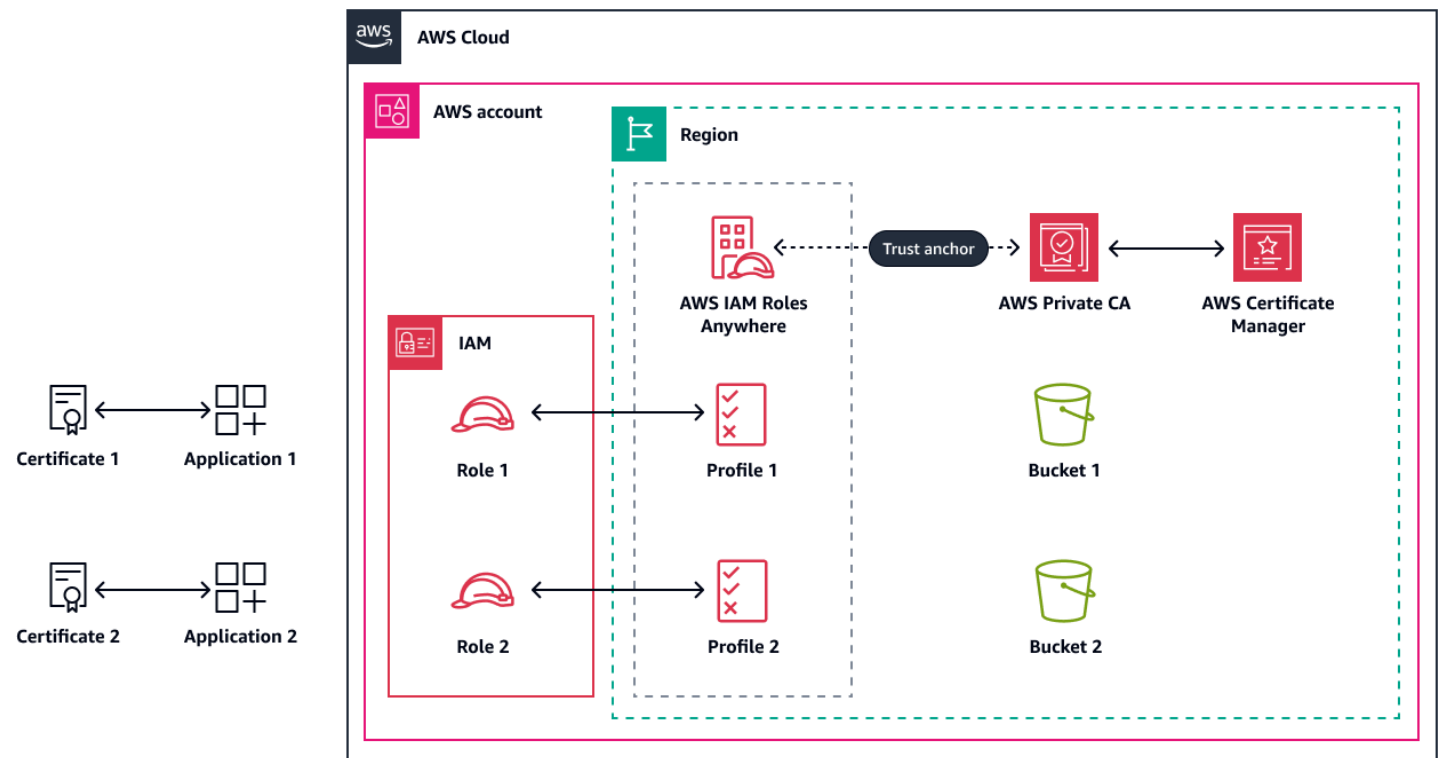
Per ulteriori informazioni, consulta [Ottenere credenziali di sicurezza temporanee](#) da IAM Roles Anywhere

# Architettura per i controlli di accesso basati su certificati in AWS

Puoi utilizzarlo AWS Identity and Access Management Roles Anywhere per ottenere credenziali di sicurezza temporanee in AWS Identity and Access Management (IAM) per carichi di lavoro come server, contenitori e applicazioni eseguiti all'esterno di AWS. I tuoi carichi di lavoro possono utilizzare le stesse [politiche IAM](#) e gli stessi [ruoli IAM](#) che utilizzi per accedere alle risorse. AWS IAM Roles Anywhere elimina la necessità di gestire le credenziali a lungo termine per i carichi di lavoro che operano al di fuori di Cloud AWS.

Per essere utilizzati IAM Roles Anywhere, i carichi di lavoro devono utilizzare certificati X.509 emessi dall'autorità di certificazione (CA) dell'autorità di [certificazione](#) (CA). La CA viene registrata IAM Roles Anywhere come punto di riferimento di fiducia per stabilire un rapporto di fiducia tra l'infrastruttura a chiave pubblica e IAM Roles Anywhere. In questa guida, utilizzi [AWS Autorità di certificazione privata \(AWS Private CA\)](#) come CA e poi stabilisci un rapporto di fiducia con IAM Roles Anywhere. Nel contesto di IAM Roles Anywhere, AWS Private CA funge da fonte affidabile per l'emissione di certificati con attributi specifici che possono essere utilizzati per controllare l'accesso alle AWS risorse attraverso politiche granulari.

Questa guida fornisce due diverse opzioni per configurare l'accesso basato su certificati alle risorse presenti nelle aree di destinazione e AWS Account AWS Regione AWS. Il diagramma seguente mostra le risorse comuni tra le due opzioni. AWS Private CA è configurato nello stesso account e nella stessa regione in cui IAM Roles Anywhere è distribuito. Esiste un ancoraggio di fiducia tra IAM Roles Anywhere e AWS Private CA. Per impostazione predefinita, tutti i certificati AWS Private CA generati possono essere utilizzati durante il processo di firma e sono archiviati all'interno di AWS Certificate Manager (ACM). Ai fini di questa guida, le applicazioni accedono a uno o più bucket Amazon Simple Storage Service (Amazon S3) nel Account AWS.



L'architettura deve avere le seguenti caratteristiche:

- **Certificati:** puoi utilizzare ACM per generare certificati. Poiché ACM è un servizio regionale, deve essere distribuito nello stesso modo di. Regione AWS AWS Private CA A causa delle limitazioni tra account, ti consigliamo di distribuire ACM nello stesso account di. AWS Private CA Per ulteriori informazioni, consulta [Condizioni per l'utilizzo AWS Private CA per firmare i certificati privati ACM](#) nella documentazione ACM.
- **Un'autorità di certificazione:** è possibile utilizzare AWS Private CA o utilizzare una CA esterna. Poiché AWS Private CA si tratta di un servizio regionale, deve essere distribuito nello stesso modo Regione AWS in cui ACM e i certificati.
- **Ruoli IAM:** associa le policy e le autorizzazioni IAM ai ruoli IAM, in base ai requisiti aziendali o ai casi d'uso dell'organizzazione. Per ulteriori informazioni, consulta la [creazione di ruoli IAM](#) nella documentazione IAM.
- **IAM Roles Anywhere profili:** configura i profili per specificare quali ruoli IAM Roles Anywhere assume e cosa possono fare i carichi di lavoro con le credenziali temporanee. Nel profilo, definisci le policy di sessione IAM per limitare le autorizzazioni create per una sessione. Per ulteriori informazioni, consulta [Configurare i ruoli](#) nella IAM Roles Anywhere documentazione.
- **Strumento di supporto alle credenziali:** utilizza lo strumento di supporto alle credenziali che IAM Roles Anywhere fornisce per ottenere credenziali di sicurezza temporanee. Per ulteriori

informazioni, consulta [Ottenere credenziali di sicurezza temporanee](#) dalla documentazione. IAM Roles Anywhere IAM Roles Anywhere

Per delegare l'autorizzazione all'accesso a una risorsa tramite IAM Roles Anywhere, crei un ruolo IAM con una politica di autorizzazione e una politica di fiducia. Una politica di autorizzazioni concede all'entità che assume le autorizzazioni necessarie per eseguire le attività previste sulla risorsa. Una [politica di fiducia](#) specifica quali membri dell'account fidati sono autorizzati ad assumere il ruolo. In questa guida, le politiche di autorizzazione definiscono a quali bucket Amazon S3 l'entità può accedere e le politiche di fiducia definiscono quale applicazione può assumere il ruolo.

Questa guida illustra i seguenti scenari per illustrare le opzioni di configurazione per le policy di fiducia dei ruoli IAM:

- [Opzione 1: le applicazioni possono assumere qualsiasi ruolo collegato a un IAM Roles Anywhere profilo](#)— Uno o più certificati sono stati forniti in ACM da AWS Private CA e condivisi con le applicazioni che richiedono l'accesso alle risorse. AWS Queste applicazioni possono assumere qualsiasi ruolo collegato a un IAM Roles Anywhere profilo. Questo perché la politica di attendibilità non limita l'applicazione che può assumerlo.
- [Opzione 2: le applicazioni possono assumere solo il ruolo consentito dalla politica di fiducia](#)— Due certificati sono stati forniti in ACM da AWS Private CA e condivisi con le applicazioni che richiedono l'accesso alle AWS risorse. A causa dei controlli di accesso basati sui certificati nelle politiche di attendibilità, l'Applicazione 1 può assumere solo il Ruolo 1 e l'Applicazione 2 può assumere solo il Ruolo 2.

#### Prerequisiti

Per configurare queste opzioni, è necessario completare quanto segue:

- Un'applicazione esterna che richiede l'accesso alle risorse di your Account AWS and target Regione AWS.
- L'autorità di certificazione è configurata nella stessa regione di IAM Roles Anywhere. Per istruzioni sulla configurazione AWS Autorità di certificazione privata, consulta [Guida introduttiva IAM Roles Anywhere](#).
- Hai rilasciato un certificato per la domanda. Per ulteriori informazioni e istruzioni, consulta [AWS Certificate Manager i certificati](#).

## Opzione 1: le applicazioni possono assumere qualsiasi ruolo collegato a un IAM Roles Anywhere profilo

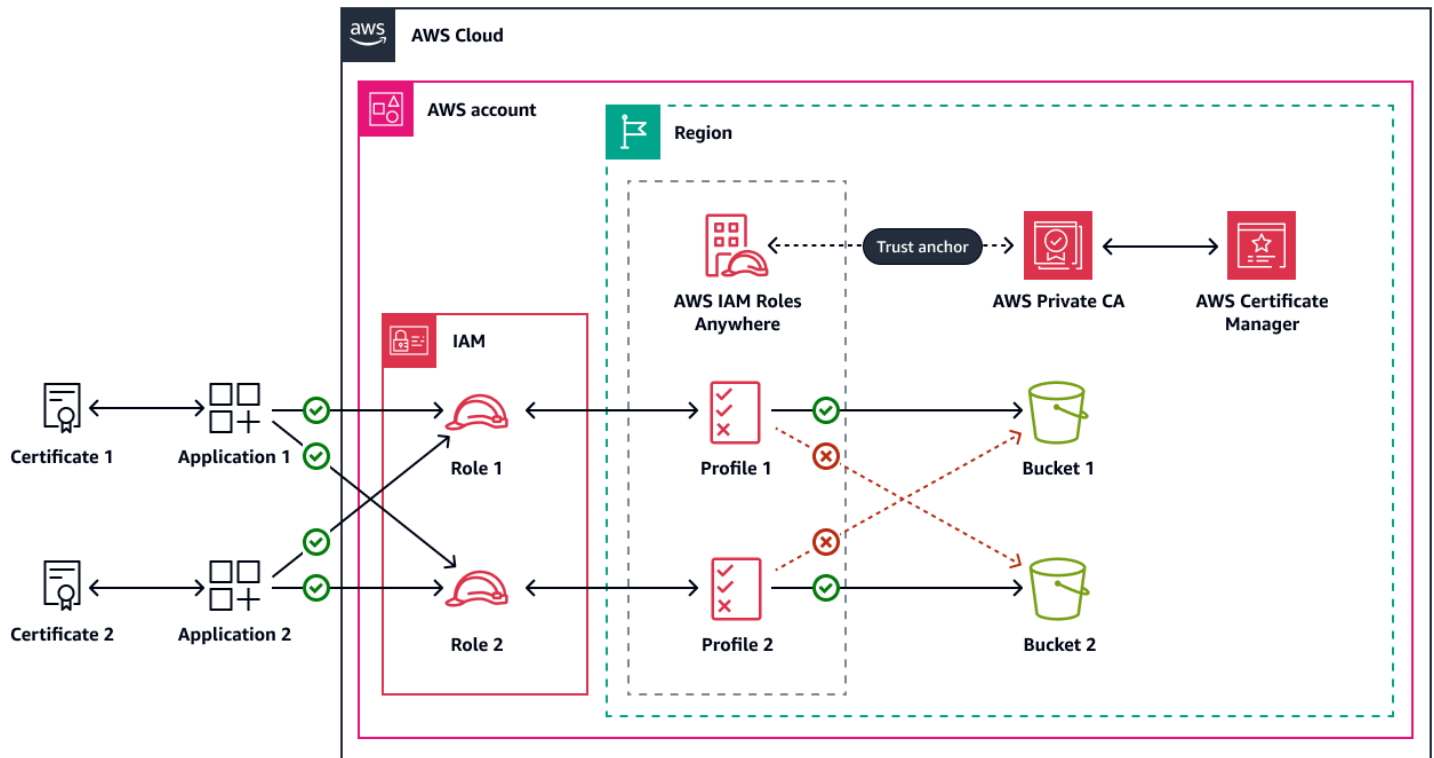
In questo scenario, due certificati sono stati forniti in AWS Certificate Manager (ACM) dall' AWS Autorità di certificazione privata istanza e condivisi con le applicazioni che richiedono l'accesso alle AWS risorse. Queste applicazioni possono assumere qualsiasi ruolo collegato a un IAM Roles Anywhere profilo. Questo perché la politica di attendibilità non limita l'applicazione che può assumerlo.

### Note

In questo scenario, non è necessario che le applicazioni dispongano di certificati separati. Potrebbero condividere un unico certificato.

Quando un'applicazione assume un ruolo, le autorizzazioni sono la convergenza di ciò che è esplicitamente consentito sia nel ruolo IAM che nel profilo. IAM Roles Anywhere Utilizzando questo approccio, puoi limitare le autorizzazioni di sessione tramite IAM Roles Anywhere i profili, indipendentemente dalle altre autorizzazioni consentite nel ruolo IAM.

L'immagine seguente mostra l'accesso di ogni applicazione. Alle applicazioni viene negato l'accesso ad alcune AWS risorse perché non viene loro concesso esplicitamente l'accesso sia nel ruolo IAM che nel IAM Roles Anywhere profilo. Se la chiamata Credential Helper include Amazon Resource Name (ARN) per il ruolo 1, all'applicazione vengono concesse credenziali di sicurezza temporanee per accedere a Bucket 1 tramite Role 1. Se la chiamata Credential Helper include l'ARN per il ruolo 2, all'applicazione vengono concesse credenziali di sicurezza temporanee per accedere a Bucket 2 tramite il ruolo 2.



Le politiche di attendibilità del ruolo 1 e del ruolo 2 sono configurate IAM Roles Anywhere per consentire di assumere il ruolo, impostare l'identità di origine e contrassegnare le sessioni. Di seguito è riportato un esempio di politica di attendibilità che consente alle applicazioni di assumere qualsiasi ruolo collegato a un IAM Roles Anywhere profilo:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "rolesanywhere.amazonaws.com"
      },
      "Action": [
        "sts:AssumeRole",
        "sts:SetSourceIdentity",
        "sts:TagSession"
      ],
      "Condition": {
        "StringEquals": {
          "sts:SourceIdentity": [
```



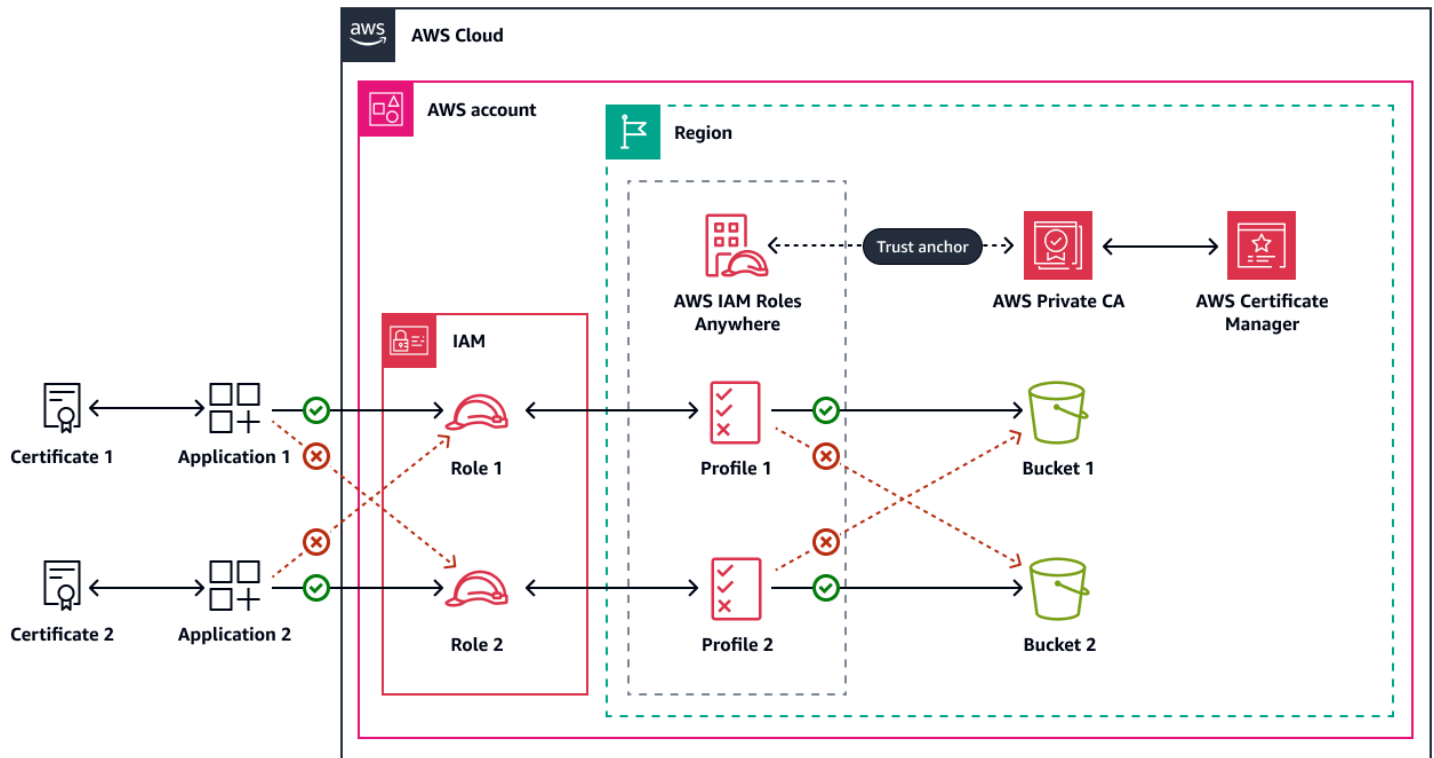
```
        "${sourceIdentityPrefix}${sourceIdentityValue}"
      ]
    }
  }
}
]
```

Per ulteriori informazioni sulle politiche di attendibilità dei ruoli e su come modificare questo esempio, consulta la [politica di attendibilità](#) nella IAM Roles Anywhere documentazione.

Esempi di criteri di ruolo e profilo per l'Applicazione 1 e l'Applicazione 2 sono inclusi nella sezione [Appendice: Esempi di politiche di profilo e ruolo](#) di questa guida.

## Opzione 2: le applicazioni possono assumere solo il ruolo consentito dalla politica di fiducia

In questo scenario, due certificati sono stati forniti in AWS Certificate Manager (ACM) AWS Autorità di certificazione privata e condivisi con le applicazioni che richiedono l'accesso alle risorse. AWS L'applicazione 1 può assumere solo il ruolo 1 e l'applicazione 2 può assumere solo il ruolo 2. Nella politica di attendibilità dei ruoli, si configurano i campi relativi all'oggetto del certificato come condizioni. Queste condizioni consentono all'applicazione di assumere solo un ruolo specifico. Grazie alle autorizzazioni del ruolo, solo l'Applicazione 1 può accedere al Bucket 1 e solo l'Applicazione 2 può accedere al Bucket 2. L'immagine seguente mostra l'accesso di ogni applicazione.



In questa opzione, si configurano le politiche di attendibilità in modo che vengano consentite `AssumeRole` solo quando vengono soddisfatti attributi specifici del certificato. La policy di fiducia dei ruoli di esempio mostra come configurare la `Condition` sezione per richiedere un nome comune del certificato specifico (CN), che è diverso per il ruolo 1 e il ruolo 2. Ogni applicazione può assumere un ruolo specifico perché IAM Roles Anywhere ha una relazione di trust ancoraggio con. AWS Private CA. Questo approccio aiuta a prevenire l'accesso non autorizzato a ruoli e dati, poiché l'applicazione non può assumere alcun ruolo collegato al profilo di destinazione. Ad esempio, è possibile separare i dati aziendali in diversi bucket, configurare i ruoli per consentire l'accesso a uno solo di questi bucket e quindi utilizzare i controlli di accesso basati sui certificati nella politica di fiducia per definire il ruolo che l'applicazione può assumere.

Il seguente esempio di politica di fiducia per il ruolo 1 presenta una condizione che consente l'assunzione del ruolo solo se il nome del certificato è `application-1.com` e se il trust anchor Amazon Resource Name (ARN) corrisponde:

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

```

    "Principal": {
      "Service": "rolesanywhere.amazonaws.com"
    },
    "Action": [
      "sts:AssumeRole",
      "sts:SetSourceIdentity",
      "sts:TagSession"
    ],
    "Condition": {
      "StringEquals": {
        "aws:PrincipalTag/x509Subject/CN": "application-1.com"
      },
      "ArnEquals": {
        "aws:SourceArn": [
          "arn:aws:rolesanywhere:<region>:<account-ID>:trust-anchor/<TA_ID>"
        ]
      }
    }
  }
}

```

Il seguente esempio di politica di attendibilità per Role 2 presenta una condizione che consente l'assunzione del ruolo solo se il nome del certificato è `application-2.com` e se l'ARN del trust anchor corrisponde:

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "rolesanywhere.amazonaws.com"
      },
      "Action": [
        "sts:AssumeRole",
        "sts:SetSourceIdentity",
        "sts:TagSession"
      ],
      "Condition": {
        "StringEquals": {

```

```
        "aws:PrincipalTag/x509Subject/CN": "application-2.com"
      },
      "ArnEquals": {
        "aws:SourceArn": [
          "arn:aws:rolesanywhere:<region>:<account-ID>:trust-anchor/
<TA_ID>"
        ]
      }
    }
  ]
}
```

Per ulteriori informazioni sulle politiche di fiducia dei ruoli e su come modificare questi esempi, consulta la [politica di fiducia nella documentazione](#). IAM Roles Anywhere

Esempi di politiche relative a ruoli e profili per l'Applicazione 1 e l'Applicazione 2 sono inclusi nella sezione [Appendice: Esempi di politiche di profilo e ruolo](#) di questa guida.

# Domande frequenti sui controlli di accesso basati su certificati su AWS

## Cosa sono gli attributi dei certificati e perché sono importanti? IAM Roles Anywhere

Gli attributi dei certificati sono campi all'interno dei certificati X.509 che contengono informazioni sul titolare del certificato, ad esempio il nome comune, l'organizzazione o le estensioni personalizzate. Inoltre AWS Identity and Access Management Roles Anywhere, questi attributi possono essere utilizzati nelle politiche di fiducia dei ruoli per implementare un controllo granulare degli accessi. Ciò consente di prendere decisioni di accesso in base alle caratteristiche del certificato piuttosto che alla sua validità.

## Come funzionano le credenziali temporanee? IAM Roles Anywhere

Quando un carico di lavoro si autentica utilizzando un certificato, IAM Roles Anywhere fornisce credenziali di sicurezza temporanee che in genere durano da 15 minuti a 12 ore. Quando queste credenziali scadono, devono essere aggiornate. Ciò riduce il rischio di compromissione delle credenziali. La natura temporanea di queste credenziali è una funzionalità di sicurezza fondamentale che aiuta a mantenere il principio del privilegio minimo.

## Quali sono i vantaggi dell'utilizzo? IAM Roles Anywhere

Rispetto all'utilizzo di chiavi di accesso a lungo termine, IAM Roles Anywhere offre diversi vantaggi:

- Non è necessario gestire o ruotare le chiavi di accesso
- Autenticazione basata su certificati con convalida integrata
- Scadenza e rinnovo automatici delle credenziali
- Controllo granulare degli accessi tramite gli attributi del certificato
- Funzionalità di controllo migliorate grazie al tracciamento dei certificati
- Riduzione del rischio di esposizione delle credenziali

## Come si IAM Roles Anywhere integra con l'infrastruttura di certificati esistente?

IAM Roles Anywhere può integrarsi con l'infrastruttura a chiave pubblica (PKI) esistente registrando l'autorità di certificazione (CA) come punto di riferimento della fiducia. Puoi utilizzare la tua CA esistente o AWS Autorità di certificazione privata. Se registrata come trust anchor, la CA emette certificati che possono essere utilizzati per autenticare i carichi di lavoro e ottenere credenziali temporanee. AWS

## Quali sono le migliori pratiche per implementare il privilegio minimo? IAM Roles Anywhere

Le migliori pratiche chiave includono:

- Utilizza gli attributi dei certificati per limitare l'assunzione di ruoli a carichi di lavoro specifici
- Implementa relazioni di fiducia specifiche basate sulle caratteristiche del certificato
- Monitora e registra le ipotesi di ruolo AWS Identity and Access Management (IAM)
- Implementa autorizzazioni di ruolo rigorose in base ai requisiti del carico di lavoro
- Verifica regolarmente le politiche di fiducia per i ruoli, le politiche [basate sull'identità per i ruoli e le politiche](#) dei profili

# Risorse e passaggi successivi

Ora che hai capito come implementare controlli di accesso sicuri utilizzando gli attributi dei certificati con AWS Identity and Access Management Roles Anywhere, prendi in considerazione la possibilità di rivedere le architetture di carico di lavoro ibride esistenti. Identifica i carichi di lavoro che attualmente utilizzano credenziali a lungo termine o richiedono un accesso sicuro a AWS risorse esterne al Cloud AWS. Valuta le opportunità per migliorare la sicurezza implementando l'autenticazione basata su certificati e applicando i controlli di accesso dettagliati descritti in questa guida. Prendi in considerazione l'idea di iniziare con un piccolo proof of concept prima di passare ai carichi di lavoro di produzione. Verifica che gli attributi dei certificati e le politiche di fiducia siano in linea con i requisiti di sicurezza e la struttura organizzativa.

Per nuovi account e carichi di lavoro, incorpora questi consigli fin dalla fase di progettazione. Utilizza le configurazioni e le politiche di esempio fornite in questa guida come base. È possibile adattarle ai casi d'uso specifici mantenendo il principio del privilegio minimo. Se hai bisogno di ulteriore assistenza o hai domande specifiche sull'implementazione IAM Roles Anywhere nel tuo ambiente, contatta il tuo AWS account team o i Servizi AWS professionali.

## Risorse

### AWS Autorità di certificazione privata risorse

- [Procedure ottimali di sicurezza per l'accesso a informazioni private CAs \(AWS Private CA documentazione\) da più account](#)
- [Politiche basate sulle risorse](#) per (documentazione) AWS Private CA
- [Come utilizzarlo per AWS RAM condividere il tuo cross-account ACM Private CA](#) (post sul blog)AWS
- [Come posso condividere la mia ACM Private Certificate Authority con un'altra persona? Account AWS](#) (Centro di AWS conoscenza)

### IAM Roles Anywhere e risorse IAM

- [Il processo IAM Roles Anywhere di firma dell'autenticazione](#) (IAM Roles Anywhere documentazione)
- [IAM Roles Anywhere Credential Helper \(\)](#) GitHub

- [Mappatura degli attributi del certificato](#) (documentazione) IAM Roles Anywhere
- [Mappatura degli attributi e politica di fiducia \(documentazione\)](#) IAM Roles Anywhere
- [Registrazione delle chiamate IAM Roles Anywhere API utilizzando AWS CloudTrail\(documentazione\)](#) IAM Roles Anywhere
- [Visualizzazione dei tag di sessione in CloudTrail](#) (documentazione IAM)



# Appendice: Esempi di politiche relative a profili e ruoli

## Politiche di esempio per l'Applicazione 1

La policy di esempio per Profile 1 consente alcune azioni per Bucket 1 in Amazon Simple Storage Service (Amazon S3):

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket1",
        "arn:aws:s3:::amzn-s3-demo-bucket1/*"
      ]
    }
  ]
}
```

La policy di esempio per Role 1 consente l'DescribeInstancesazione per un'istanza Amazon Elastic Compute Cloud (Amazon EC2) e consente alcune azioni su Bucket 1 e Bucket 2 in Amazon S3:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances"
      ],
      "Resource": [
        "arn:aws:ec2:us-east-1:123456789012:instance/i-01234567890abcdef"
      ]
    }
  ]
}
```

```

    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "s3:ListAllMyBuckets",
      "s3:ListBucket",
      "s3:GetObject",
      "s3:GetObjectTagging",
      "s3:GetObjectVersion",
      "s3:PutObject",
      "s3:PutObjectAcl",
      "s3:PutObjectLegalHold",
      "s3:PutObjectTagging"
    ],
    "Resource": [
      "arn:aws:s3:::amzn-s3-demo-bucket1",
      "arn:aws:s3:::amzn-s3-demo-bucket1/*",
      "arn:aws:s3:::amzn-s3-demo-bucket2",
      "arn:aws:s3:::amzn-s3-demo-bucket2/*"
    ]
  }
]
}

```

La policy Profile 1 limita le autorizzazioni concesse dalla policy Role 1. Viene applicata alla sessione di ruolo quando il ruolo viene assunto. IAM Roles Anywhere Un'applicazione che presuppone il ruolo 1 ha accesso solo a Bucket 1. Non può accedere a Bucket 2 o eseguire alcuna EC2 azione Amazon perché la policy Profile 1 non concede queste autorizzazioni.

## Politiche di esempio per l'Applicazione 2

La policy di esempio per Profile 2 consente alcune azioni per Bucket 2 in Amazon S3:

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:GetObject",

```

```

        "s3:GetObjectTagging",
        "s3:GetObjectVersion"
    ],
    "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket2",
        "arn:aws:s3:::amzn-s3-demo-bucket2/*"
    ]
}
]
}

```

La policy di esempio per Role 2 consente l'DescribeInstancesazione per un' EC2 istanza Amazon e consente alcune azioni su Bucket 1 e Bucket 2 in Amazon S3:

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances"
      ],
      "Resource": [
        "arn:aws:ec2:us-east-1:567890123456:instance/i-05678901234ghijk"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:PutObjectLegalHold",
        "s3:PutObjectTagging"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket1",
        "arn:aws:s3:::amzn-s3-demo-bucket1/*",
        "arn:aws:s3:::amzn-s3-demo-bucket2",

```

```
    "arn:aws:s3:::amzn-s3-demo-bucket2/*"  
  ]  
}  
]  
}
```

La politica per Profile 2 limita le autorizzazioni concesse da Role 2. Viene applicato alla sessione di ruolo quando il ruolo viene assunto. IAM Roles Anywhere Un'applicazione che presuppone il ruolo 2 ha accesso solo a Bucket 2. Non può accedere a Bucket 1 o eseguire EC2 azioni Amazon perché la policy Profile 2 non concede queste autorizzazioni.

## 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           |
|----------------------------------------|-------------|----------------|
| <a href="#">Pubblicazione iniziale</a> | —           | 14 luglio 2025 |

# 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:

- **Rifattorizzare/riprogettare:** trasferisci un'applicazione e modifica la sua 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 compatibile con Amazon Aurora PostgreSQL.
- **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 a 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 su Microsoft 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

## 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.

## funzione di aggregazione

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 AIOps viene utilizzata nella strategia di AWS migrazione, 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 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 interrompere 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.

### implementazione blu/verde

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, vedere l'indicatore [Implementate break-glass procedures](#) nella guida Well-Architected AWS .

## 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 [Cloud Adoption AWS Framework](#).

## implementazione canaria

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

## CCoE

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.

## crittografia lato client

Crittografia dei dati a livello locale, prima che il destinatario li Servizio AWS riceva.

## Centro di eccellenza 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 gli [CCoE post](#) 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 scalare l'adozione del cloud (ad esempio, creazione di una landing zone, definizione di una CCo E, definizione di un modello operativo)
- Migrazione: migrazione di singole applicazioni
- Reinvenzione: ottimizzazione di prodotti e servizi e innovazione nel cloud

Queste fasi sono state definite da Stephen Orban nel post sul blog The [Journey Toward Cloud-First & the Stages of Adoption on the Enterprise Strategy](#). Cloud AWS [Per informazioni su come si relazionano alla 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 o Bitbucket Cloud. Ogni versione del codice è denominata ramo. In una struttura a microservizi, ogni repository è dedicato a una singola funzionalità. Una singola pipeline CI/CD 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 continua (continuous integration and continuous delivery, 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.

## defense-in-depth

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 defense-in-depth approccio potrebbe combinare l'autenticazione a più fattori, la segmentazione della rete e la 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 Workloads 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 il modello del fico strangolatore (Strangler Fig), consulta la sezione [Modernizzazione incrementale dei servizi Web Microsoft ASP.NET \(ASMX\) legacy utilizzando container e il Gateway Amazon API](#).

DOTT.

Vedi [disaster recovery](#).

rilevamento della deriva

Tracciamento delle deviazioni da una configurazione di base. Ad esempio, è possibile AWS CloudFormation utilizzarlo per [rilevare deviazioni nelle risorse di sistema](#) oppure AWS Control Tower per [rilevare cambiamenti nella 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. I sistemi big-endian memorizzano per primo il byte più importante. I sistemi little-endian memorizzano per primo 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 in uno [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. I prompt con pochi passaggi 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 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. FM sono in grado di svolgere 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](#).

# 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 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 alto livello che aiuta a governare le risorse, le politiche e la conformità tra le unità organizzative (). OUs 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 .

# 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 blocco

[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.

#### 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, come 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 in Well-Architected AWS Framework](#).

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. La [AWS Security Reference Architecture](#) consiglia di configurare l'account di rete con funzionalità in entrata, in uscita e di ispezione VPCs 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.

## IIoInternet delle cose industriale (T)

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, vedere [Creazione di una strategia di trasformazione digitale per l'Internet of Things \(IIoT\) industriale](#).

## VPC di ispezione

In un'architettura AWS multi-account, un VPC centralizzato che gestisce le ispezioni del traffico di rete tra VPCs (nello stesso o in modo diverso Regioni AWS), Internet e le reti locali. La [AWS Security Reference Architecture](#) consiglia di configurare l'account di rete con informazioni in entrata, in uscita e di ispezione VPCs 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, vedere 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. LLMs](#)

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](#).

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, consulta [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 machine-to-machine \(M2M\) leggero, basato sul modello di pubblicazione/sottoscrizione, per dispositivi IoT con risorse limitate.](#)

### microservizio

Un servizio piccolo e indipendente che comunica tramite canali ben definiti ed è in genere di proprietà di piccoli team autonomi. APIs 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 attraverso un'interfaccia ben definita utilizzando sistemi leggeri. APIs 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

Team interfunzionali che semplificano la migrazione dei carichi di lavoro attraverso approcci automatizzati e agili. I team di Migration Factory in genere includono addetti alle 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 machine-to-machine (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 Well-Architected AWS Framework.

## tecnologia operativa (OT)

Sistemi hardware e software che interagiscono con l'ambiente fisico per controllare le operazioni, le apparecchiature e le 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 tutti i bucket S3 in generale Regioni AWS, la crittografia lato server con AWS KMS (SSE-KMS) e le richieste dinamiche e dirette al bucket S3.

PUT 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. La [AWS Security Reference Architecture](#) consiglia di configurare l'account di rete con funzionalità in entrata, in uscita e di ispezione VPCs 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 \(vedi politica basata sulle risorse\) 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 `true`. `false`  
`WHERE`

## 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 di ingegneria dei sistemi che tiene conto della privacy durante l'intero processo di sviluppo.

## zone ospitate private

Un contenitore che contiene informazioni su come desideri che Amazon Route 53 risponda alle query DNS per un dominio e i relativi sottodomini all'interno di uno o più VPCs. 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 alle interruzioni o di ripristinarle. [L'elevata disponibilità e il disaster recovery](#) sono considerazioni comuni quando si pianifica la resilienza in Cloud AWS. [Per 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 politica che fornisce il controllo centralizzato sulle autorizzazioni per tutti gli account di un'organizzazione in. AWS Organizations SCPs definire barriere o fissare limiti alle azioni che un amministratore può delegare a utenti o ruoli. È possibile utilizzarli SCPs 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](#).

## 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](#).

## split-and-seed modello

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 [Modernizzazione incrementale dei servizi Web legacy di Microsoft ASP.NET \(ASMX\) mediante container e Gateway Amazon API](#).

## 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

Coppie chiave-valore 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.

## Transit Gateway

Un hub di transito di rete che puoi utilizzare per interconnettere le tue reti VPCs e quelle locali. 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. Per ulteriori informazioni, consulta la guida [Quantificazione dell'incertezza nei sistemi di deep learning](#).



## 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 VPCs che consente di indirizzare il traffico utilizzando 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 query 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.