Guida per l'amministratore

Catena di approvvigionamento di AWS

Catena di approvvigionamento di AWS: Guida per l'amministratore

Table of Contents

Cos'è Catena di approvvigionamento di AWS?

Catena di approvvigionamento di AWSè un'applicazione di gestione della catena di fornitura basata su cloud che funziona con le soluzioni esistenti come la pianificazione delle risorse aziendali (ERP) e i sistemi di gestione della catena di fornitura. UtilizzandoCatena di approvvigionamento di AWS, puoi connettere ed estrarre i dati relativi all'inventario, alla fornitura e alla domanda dai sistemi ERP o della catena di fornitura esistenti in un unico modello diCatena di approvvigionamento di AWS dati unificato.

Argomenti

Browser Web supportati da Catena di approvvigionamento di AWS

Prima di lavorare conAWS Supply Chain, verifica che il tuo browser sia supportato utilizzando la seguente tabella.

Browser	Versioni supportate
Google Chrome	Ultime tre versioni.
Mozilla Firefox ESR	Le versioni sono supportate fino alla end-of-lifedata di scadenza di Firefox. Per maggiori dettagli, consulta il calendario delle versioni di Firefox ESR.
Mozilla Firefox	Ultime tre versioni.
Microsoft Edge e Edge Chromium	Versione 84 e successive.
Safari	Safari 10 o versioni successive su macOS.

Lingue supportate daCatena di approvvigionamento di AWS

Catena di approvvigionamento di AWS supporta le seguenti lingue:

- Inglese (Stati Uniti)
- Inglese (Regno Unito)
- Tedesco
- Spagnolo
- Francese
- Italiano
- portoghese
- Cinese (semplificato)
- Cinese (tradizionale)
- Giapponese
- Coreano
- Indonesiano

Configurazione di un AWS account

Utilizza questa sezione per creare un AWS account e creare un utente IAM. Per informazioni sulle migliori pratiche per creare un AWS account, consulta Stabilire un AWS ambiente di best practice.

Argomenti

Registrati per un Account AWS

Se non ne hai uno Account AWS, completa i seguenti passaggi per crearne uno.

Per iscriverti a un Account AWS

1. Apri la pagina all'indirizzo https://portal.aws.amazon.com/billing/signup.
2. Segui le istruzioni online.

   Nel corso della procedura di registrazione riceverai una telefonata, durante la quale sarà necessario inserire un codice di verifica attraverso la tastiera del telefono.

   Quando ti iscrivi a un Account AWS, Utente root dell'account AWSviene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come procedura consigliata in materia di sicurezza, assegnate l'accesso amministrativo a un utente e utilizzate solo l'utente root per eseguire attività che richiedono l'accesso da parte dell'utente root.

AWS ti invia un'e-mail di conferma dopo il completamento della procedura di registrazione. È possibile visualizzare l'attività corrente dell'account e gestire l'account in qualsiasi momento accedendo all'indirizzo https://aws.amazon.com/ e selezionando Il mio account.

Crea un utente con accesso amministrativo

Dopo esserti registrato Account AWS, proteggi Utente root dell'account AWS AWS IAM Identity Center, abilita e crea un utente amministrativo in modo da non utilizzare l'utente root per le attività quotidiane.

Proteggi i tuoi Utente root dell'account AWS

1. Accedi AWS Management Consolecome proprietario dell'account scegliendo Utente root e inserendo il tuo indirizzo Account AWS email. Nella pagina successiva, inserisci la password.

   Per informazioni sull'accesso utilizzando un utente root, consulta la pagina Signing in as the root user della Guida per l'utente di Accedi ad AWS .
2. Abilita l'autenticazione a più fattori (MFA) per l'utente root.

   Per istruzioni, consulta Abilitare un dispositivo MFA virtuale per l'utente Account AWS root (console) nella Guida per l'utente IAM.

Crea un utente con accesso amministrativo

1. Abilita Centro identità IAM.

   Per istruzioni, consulta Abilitazione di AWS IAM Identity Center nella Guida per l'utente di AWS IAM Identity Center .
2. In IAM Identity Center, concedi l'accesso amministrativo a un utente.

   Per un tutorial sull'utilizzo di IAM Identity Center directory come fonte di identità, consulta Configurare l'accesso utente con le impostazioni predefinite IAM Identity Center directory nella Guida per l'AWS IAM Identity Center utente.

Accedi come utente con accesso amministrativo

- Per accedere con l'utente IAM Identity Center, utilizza l'URL di accesso che è stato inviato al tuo indirizzo e-mail quando hai creato l'utente IAM Identity Center.

  Per informazioni sull'accesso utilizzando un utente IAM Identity Center, consulta AWS Accedere al portale di accesso nella Guida per l'Accedi ad AWS utente.

Assegna l'accesso ad altri utenti

1. In IAM Identity Center, crea un set di autorizzazioni che segua la migliore pratica di applicazione delle autorizzazioni con privilegi minimi.

Per istruzioni, consulta Creare un set di autorizzazioni nella Guida per l'utente.AWS IAM Identity Center

2. Assegna gli utenti a un gruppo, quindi assegna l'accesso Single Sign-On al gruppo.

   Per istruzioni, consulta Aggiungere gruppi nella Guida per l'utente.AWS IAM Identity Center

Chiusura di un AWS account

Per informazioni su come chiudere un AWS account, consulta Chiusura di un account.

Iniziare con Catena di approvvigionamento di AWS

In questa sezione, puoi imparare a creare un' Catena di approvvigionamento di AWS istanza, concedere ruoli di autorizzazione utente, accedere all'applicazione Catena di approvvigionamento di AWS Web e creare ruoli di autorizzazione utente personalizzati. An Account AWS può avere fino a 10 Catena di approvvigionamento di AWS istanze in stato attivo o in fase di inizializzazione.

Argomenti

Prerequisiti

Prima di creare un' Catena di approvvigionamento di AWS istanza, assicurati di completare i seguenti passaggi:

- Hai creato un Account AWS. Per ulteriori informazioni, consulta Configurazione di un AWS account.

> **Note**
>
> Se non l'hai ancora attivato AWS IAM Identity Center, crea un' AWS organizzazione e attiva IAM Identity Center. Per ulteriori informazioni sulla creazione di un' AWS organizzazione, consulta Creazione di un'organizzazione.

- Attiva IAM Identity Center nello stesso Regione AWS punto in cui desideri creare l' Catena di approvvigionamento di AWS istanza. Catena di approvvigionamento di AWS è supportato solo nelle regioni Stati Uniti orientali (Virginia settentrionale), Stati Uniti occidentali (Oregon), Europa (Francoforte) ed Europa (Irlanda). Per ulteriori informazioni, consulta Abilitazione di IAM Identity Center .

> **Note**
>
> Catena di approvvigionamento di AWS La pianificazione della domanda e la pianificazione dell'offerta non sono supportate nella regione Europa (Irlanda).

> **Note**
>
> Se non hai attivato IAM Identity Center in una regione diversa da quelle elencate qui, non puoi creare un' Catena di approvvigionamento di AWS istanza.

- Puoi creare utenti IAM dalla console AWS Identity and Access Management (IAM). Per ulteriori informazioni, consulta Configurazione di un AWS account.
- Aggiungi gli utenti che devono accedere Catena di approvvigionamento di AWS a IAM Identity Center. Per ulteriori informazioni, consulta Aggiungere utenti in IAM Identity Center. Puoi anche connettere la tua active directory a IAM Identity Center. Per ulteriori informazioni, vedere Connect to a Microsoft AD directory nella Guida per l'AWS IAM Identity Center utente.
- Quando usi Microsoft Active Directory, assicurati che la sincronizzazione con Active Directory sia abilitata.
- È necessario AWS Key Management Service (AWS KMS) per creare un'istanza. Catena di approvvigionamento di AWS lo usa AWS KMS key per crittografare tutti i dati in entrata Catena di approvvigionamento di AWS.

Utilizzo della console di Catena di approvvigionamento di AWS

> **Note**
>
> Se il tuo AWS account è un account membro di un' AWS organizzazione e include una Service Control Policy (SCP), assicurati che l'SCP dell'organizzazione conceda le seguenti autorizzazioni all'account membro. Se le seguenti autorizzazioni non sono incluse nella politica SCP dell'organizzazione, la creazione dell'istanza avrà esito negativo. Catena di approvvigionamento di AWS

Per accedere alla Catena di approvvigionamento di AWS console, è necessario disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle Catena di approvvigionamento di AWS risorse del tuo. Account AWS Se crei una policy basata sull'identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti o ruoli) associate a tale policy.

Non è necessario consentire autorizzazioni minime per la console agli utenti che effettuano chiamate solo verso AWS CLI o l' AWS API. Al contrario, concedi l'accesso solo alle operazioni che corrispondono all'operazione API che stanno cercando di eseguire.

Per garantire che utenti e ruoli possano ancora utilizzare la Catena di approvvigionamento di AWS console, allega anche la policy Catena di approvvigionamento di AWS `ConsoleAccess` o la policy `ReadOnly` AWS gestita alle entità. Per ulteriori informazioni, consulta Aggiunta di autorizzazioni a un utente nella Guida per l'utente IAM.

Le seguenti autorizzazioni sono necessarie all'amministratore della console per creare e aggiornare correttamente Catena di approvvigionamento di AWS le istanze.

```
        {
"Version": "2012-10-17",
"Statement": [
    {
        "Action": "scn:*",
        "Resource": "*",
        "Effect": "Allow"
    },
    {
        "Action": [
```

```
                "s3:GetObject",
                "s3:PutObject",
                "s3:ListBucket",
                "s3:CreateBucket",
                "s3:PutBucketVersioning",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutEncryptionConfiguration",
                "s3:PutBucketPolicy",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketPublicAccessBlock",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutBucketOwnershipControls",
                "s3:PutBucketNotification",
                "s3:PutAccountPublicAccessBlock",
                "s3:PutBucketLogging",
                "s3:PutBucketTagging"
            ],
            "Resource": "arn:aws:s3:::aws-supply-chain-*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "cloudtrail:CreateTrail",
                "cloudtrail:PutEventSelectors",
                "cloudtrail:GetEventSelectors",
                "cloudtrail:StartLogging"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "events:DescribeRule",
                "events:PutRule",
                "events:PutTargets"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "chime:CreateAppInstance",
                "chime:DeleteAppInstance",
```

```
                "chime:PutAppInstanceRetentionSettings",
                "chime:TagResource"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "cloudwatch:PutMetricData",
                "cloudwatch:Describe*",
                "cloudwatch:Get*",
                "cloudwatch:List*"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:CreateOrganization",
                "organizations:EnableAWSServiceAccess"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "kms:CreateGrant",
                "kms:RetireGrant",
                "kms:DescribeKey",
                "kms:ListAliases"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "iam:CreateRole",
                "iam:CreatePolicy",
                "iam:GetRole",
                "iam:PutRolePolicy",
                "iam:AttachRolePolicy",
                "iam:CreateServiceLinkedRole"
            ],
```

```
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "sso:StartPeregrine",
                "sso:DescribeRegisteredRegions",
                "sso:ListDirectoryAssociations",
                "sso:GetPeregrineStatus",
                "sso:GetSSOStatus",
                "sso:ListProfiles",
                "sso:GetProfile",
                "sso:AssociateProfile",
                "sso:AssociateDirectory",
                "sso:RegisterRegion",
                "sso:StartSSO",
                "sso:CreateManagedApplicationInstance",
                "sso:DeleteManagedApplicationInstance",
                "sso:GetManagedApplicationInstance",
                "sso-directory:SearchUsers"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

Creazione di un'istanza

> **Note**
>
> Puoi creare fino a 10 istanze all'interno di un. Account AWS Le 10 istanze includono istanze attive e in fase di inizializzazione. Se hai già attivato IAM Identity Center (successore di AWS Single Sign-On), devi creare l' Catena di approvvigionamento di AWS istanza nella stessa in Regione AWS cui hai attivato IAM Identity Center. Catena di approvvigionamento di AWS non supporta le chiamate IAM Identity Center tra regioni.

Per creare un' Catena di approvvigionamento di AWS istanza, segui questi passaggi.

> **Note**
>
> Solo l' AWS Management Console amministratore può creare un'istanza. L' AWS Management Console amministratore che crea l' Catena di approvvigionamento di AWS istanza deve disporre di tutte le autorizzazioni elencate sottoUtilizzo della console di Catena di approvvigionamento di AWS. Questo amministratore deve invitare un utente IAM come Catena di approvvigionamento di AWS amministratore per la gestione Catena di approvvigionamento di AWS.

1. Apri la Catena di approvvigionamento di AWS console all'indirizzohttps://console.aws.amazon.com/scn/home.
2. Se necessario, modifica Regione AWS. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni sulle regioni, consulta Regioni ed endpoint nella Guida per l'utente IAM. Inoltre, consulta Regioni ed endpoint in. Riferimenti generali di Amazon Web Services

   > **Note**
   >
   > Catena di approvvigionamento di AWS è supportato solo nella regione Stati Uniti orientali (Virginia settentrionale), Stati Uniti occidentali (Oregon), Europa (Francoforte) nella regione Asia Pacifico (Sydney) ed Europa (Irlanda).
   > Catena di approvvigionamento di AWS La pianificazione della domanda e la pianificazione dell'offerta non sono supportate nella regione Europa (Irlanda).

3. Nella Catena di approvvigionamento di AWS dashboard, scegli Crea istanza.
4. Nella pagina delle proprietà dell'istanza, inserisci le seguenti informazioni:
   - AWS Regione: scegli la regione in cui hai attivato IAM Identity Center. Per cambiare la regione, scegli Seleziona una regione dal menu a discesa in alto a destra. Non puoi modificare la regione dopo aver creato l'istanza.
   - Nome: inserisci il nome dell'istanza.
   - (Facoltativo) Descrizione: immettere una descrizione per l'istanza.
5. In AWS KMS Key, inserisci la tua chiave KMS e aggiorna la politica della chiave KMS con quanto segue:

> **Note**
>
> In qualità di amministratore dell'applicazione, quando aggiungi utenti all' Catena di approvvigionamento di AWS istanza, questi hanno accesso a. AWS KMS key Puoi gestire le autorizzazioni utente per aggiungere o rimuovere utenti. Per ulteriori informazioni sulle autorizzazioni degli utenti, consulta. Ruoli di autorizzazione utente

> **Note**
>
> Sostituisci *YourAccountNumber*, *Regione*, *YourInstanceID* e *YourKmsKeyArn*con la tua AWS regione Account AWS, l'ID dell' Catena di approvvigionamento di AWS istanza e la AWS KMS chiave.

```
   {
   "Version": "2012-10-17",
   "Statement": [{
           "Sid": "Enable IAM User Permissions",
           "Effect": "Allow",
           "Principal": {
               "AWS": "arn:aws:iam::YourAccountNumber:root"
           },
           "Action": "kms:*",
           "Resource": "*"
       },
       {
           "Sid": "Allow access through SecretManager for all principals in the
account that are authorized to use SecretManager",
           "Effect": "Allow",
           "Principal": {
               "AWS": "*"
           },
           "Action": [
               "kms:Encrypt",
               "kms:Decrypt",
               "kms:ReEncrypt*",
               "kms:GenerateDataKey*",
```

```
                "kms:CreateGrant",
                "kms:DescribeKey",
                "kms:GenerateDataKeyWithoutPlaintext",
                "kms:ReEncryptFrom",
                "kms:ReEncryptTo"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "secretsmanager.Region.amazonaws.com",
                    "kms:CallerAccount": "YourAccountNumber"
                }

            }
        }
    ]
}
```

Se non disponi di una chiave KMS, scegli Crea per accedere alla AWS KMS console, dove puoi creare questa chiave. Usa la precedente politica delle chiavi KMS. Per informazioni dettagliate su come creare le chiavi KMS, consulta Creating keys nella AWS Key Management Service Developer Guide.

Se prevedi di utilizzare una connessione dati S/4 Hana, assicurati che alla chiave KMS che hai fornito sia associato il aws-supply-chain-accesstag con il valore true associato.

6. (Facoltativo) In Tag di istanza, scegli Aggiungi nuovo tag per assegnare un tag all'istanza. Puoi utilizzare questi tag per identificare la tua istanza. Per informazioni sui tag, consulta Creazione di tag.
7. Seleziona Crea istanza.

   La creazione dell' Catena di approvvigionamento di AWS istanza richiede dai 2 ai 3 minuti circa. Una volta creata l'istanza, il campo Stato sulla Catena di approvvigionamento di AWS dashboard viene visualizzato come Attivo.
8. Una volta creata l' Catena di approvvigionamento di AWS istanza, aggiorna la politica KMS per consentire l'accesso Catena di approvvigionamento di AWS alla AWS KMS chiave.

> **Note**
>
> Sostituisci *YourInstanceID* con l'ID dell' Catena di approvvigionamento di AWS istanza. Puoi trovare l'ID dell'istanza nella dashboard della Catena di approvvigionamento di AWS console.

```
        {
    "Sid": "Allow AWS Supply Chain to access the AWS KMS Key",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::YourAccountNumber:role/service-role/scn-instance-
role-YourInstanceID"
    },
    "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:GenerateDataKey"
    ],
    "Resource": "*"
},
{
    "Sid": "Enable ASC to backfill KMS permissions",
    "Effect": "Allow",
    "Principal": {
        "Service": "scn.Region.amazonaws.com"
    },
    "Action": [
        "kms:Encrypt",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "kms:DescribeKey",
        "kms:CreateGrant",
        "kms:RetireGrant"
    ],
    "Resource":"YourKmsKeyArn"
}
```

Abilitazione di IAM Identity Center

Prima di iniziare a utilizzare Catena di approvvigionamento di AWS, devi connetterti a una fonte di identità. Per ulteriori informazioni, consulta la sezione Guida introduttiva a IAM nella IAM User Guide.

Aggiungere utenti in IAM Identity Center

Puoi gestire gli utenti per l' Catena di approvvigionamento di AWS utilizzo del servizio IAM Identity Center. IAM Identity Center è un servizio IAM Identity Center basato sul cloud che semplifica la gestione centralizzata dell'accesso a IAM Identity Center a tutte le tue applicazioni Account AWS e al cloud. Per aggiungere utenti IAM, consulta Creating an IAM user in your AWS account nella IAM User Guide.

Per ulteriori informazioni sulla creazione di gruppi di utenti IAM, consulta Creazione di gruppi di utenti IAM nella Guida per l'utente IAM.

> **Note**
>
> Per aggiungere un utente Catena di approvvigionamento di AWS, gli utenti devono far parte di un gruppo IAM Identity Center.

Scelta del proprietario Catena di approvvigionamento di AWS dell'applicazione

> **Note**
>
> In qualità di amministratore AWS della console, stai scegliendo il proprietario Catena di approvvigionamento di AWS dell'applicazione per gestire l'accesso alle applicazioni Catena di approvvigionamento di AWS Web. Il proprietario Catena di approvvigionamento di AWS dell'applicazione può aggiungere o rimuovere ruoli di autorizzazione utente all'applicazione Catena di approvvigionamento di AWS Web.

Dopo aver creato l'istanza e aver collegato una fonte di identità, segui questi passaggi per scegliere il proprietario Catena di approvvigionamento di AWS dell'applicazione.

1. Nella dashboard della Catena di approvvigionamento di AWS console, in Proprietario dell'applicazione, scegli Assegna proprietario dell'applicazione.
2. In Seleziona il proprietario dell'applicazione, seleziona un utente che agirà come proprietario Catena di approvvigionamento di AWS dell'applicazione. È possibile cercare solo il nome utente e vengono visualizzati gli utenti che corrispondono ai criteri di ricerca.

   Per aggiungere altri utenti, scegli Vai a IAM Identity Center. Per ulteriori informazioni sull'aggiunta di utenti, consulta Aggiungere utenti in IAM Identity Center e per ulteriori informazioni sui ruoli di autorizzazione utente, consultaRuoli di autorizzazione utente.

   > **Note**
   >
   > Puoi aggiungere solo un utente alla volta dalla Catena di approvvigionamento di AWS Console. Non è possibile aggiungere un gruppo come proprietario dell'applicazione in Catena di approvvigionamento di AWS.

3. scegli Invia invito.

   Nella dashboard della Catena di approvvigionamento di AWS console, vedrai l'utente elencato nella sezione Proprietario dell'applicazione.
4. Scegli Gestisci Catena di approvvigionamento di AWS per aggiungere e rimuovere utenti nell'applicazione Catena di approvvigionamento di AWS web.

Assegna gruppi

In qualità di proprietario o Catena di approvvigionamento di AWS amministratore dell'applicazione, puoi aggiungere solo utenti che fanno parte di un gruppo IAM Identity Center. Catena di approvvigionamento di AWS

1. Nella dashboard della Catena di approvvigionamento di AWS console, in Gruppi, scegli Assegna gruppi.

   Viene visualizzata la pagina Gruppi.
2. In Nome gruppo seleziona il gruppo con gli utenti che possono accedere Catena di approvvigionamento di AWS e scegli Assegna.

Vedrai il gruppo che hai elencato in Gruppi nella Catena di approvvigionamento di AWS dashboard.

3. Puoi scegliere Gestisci gruppi per aggiungere un nuovo gruppo in IAM Identity Center. Una volta aggiunto il gruppo in IAM Identity Center, il gruppo verrà elencato nella sezione Nome del gruppo in Catena di approvvigionamento di AWS.

Accesso all'applicazione web AWS Supply Chain

In qualità di Catena di approvvigionamento di AWS amministratore, dovresti aver ricevuto un'e-mail di invito all'applicazione Catena di approvvigionamento di AWS web.

1. Puoi scegliere il link nell'e-mail o nella dashboard della Catena di approvvigionamento di AWS console, in Sottodominio, scegliere l'URL web.

   Viene visualizzata la pagina di accesso all'applicazione Catena di approvvigionamento di AWSWeb.
2. Inserisci le credenziali utente di AWS IAM Identity Center e scegli Accedi.

Accedere Catena di approvvigionamento di AWS per la prima volta

> **Note**
>
> Ti verrà chiesto di completare i profili relativi al tuo account e alla tua organizzazione solo quando effettui il primo accesso.

Dopo aver effettuato l'accesso all'applicazione Catena di approvvigionamento di AWS Web come Catena di approvvigionamento di AWS amministratore, segui questi passaggi per completare la configurazione.

1. Nella pagina Completa il tuo profilo, inserisci il tuo Job Title e il fuso orario. Seleziona Successivo.
2. Nella pagina Aggiungiamo le informazioni sulla tua organizzazione, inserisci il nome dell'organizzazione e scegli la sede centrale. Facoltativamente, puoi aggiungere un logo aziendale. Seleziona Successivo.

3. Nella Catena di approvvigionamento di AWS pagina Configura i colleghi del team, seleziona gli utenti a cui desideri che abbiano accesso all' Catena di approvvigionamento di AWS applicazione web. Scegliere Invite Users (Invita utenti). Per informazioni su come aggiungere utenti a IAM Identity Center, consulta. Aggiungere utenti in IAM Identity Center Per informazioni sui ruoli di autorizzazione Catena di approvvigionamento di AWS degli utenti, consultaRuoli di autorizzazione utente.
4. Se desideri aggiungere utenti in un secondo momento, puoi scegliere Ignora per ora.

   Viene visualizzata la pagina Onboarding completo.
5. Ogni utente che hai aggiunto riceve un messaggio e-mail con un link che rimanda a Catena di approvvigionamento di AWS, oppure puoi scegliere Copia link e inviare il link agli utenti.
6. Scegli Continua alla home page per visualizzare la Catena di approvvigionamento di AWS dashboard.

Aggiornamento del profilo dell'account

Puoi aggiornare il profilo del tuo account in qualsiasi momento sull'applicazione Catena di approvvigionamento di AWS web. Segui questi passaggi per aggiornare l'account.

1. Nella dashboard dell'applicazione Catena di approvvigionamento di AWS Web, dal riquadro di navigazione a sinistra, scegli l'icona Impostazioni.
2. Scegli Profilo dell'account.

   Viene visualizzata la pagina Profilo dell'account.
3. Aggiorna le informazioni sull'account e scegli Salva.

Aggiornamento del profilo dell'organizzazione

Puoi aggiornare il profilo dell'organizzazione in qualsiasi momento sull'applicazione Catena di approvvigionamento di AWS web. Segui questi passaggi per aggiornare il profilo dell'organizzazione.

1. Nella dashboard dell'applicazione Catena di approvvigionamento di AWS web, dal riquadro di navigazione a sinistra, scegli l'icona Impostazioni.
2. Scegli Organizzazione, quindi scegli Profilo dell'organizzazione.

   Viene visualizzata la pagina Profilo dell'organizzazione.

3. Aggiorna il logo dell'organizzazione o l'ubicazione della sede centrale, quindi scegli Salva.

Ruoli di autorizzazione utente

In qualità di Catena di approvvigionamento di AWS amministratore, puoi utilizzare i ruoli di autorizzazione utente predefiniti o creare ruoli di autorizzazione personalizzati. Catena di approvvigionamento di AWS ha i seguenti ruoli di autorizzazione utente predefiniti:

- Amministratore: accesso per creare, visualizzare e gestire tutti i dati e le autorizzazioni degli utenti.
- Analista di dati: accesso per creare, visualizzare e gestire tutte le connessioni dati.
- Inventory Manager: accesso per creare, visualizzare e gestire Insights.
- Planner: accesso per creare, visualizzare e gestire previsioni, sostituzioni e pubblicare piani di domanda.
- Partner Data Manager: accesso per gestire e visualizzare i partner, gestire e visualizzare le richieste di dati e visualizzare i dati sulla sostenibilità.
- Supply Planner: accesso per gestire e visualizzare i piani di fornitura.

> **Note**
>
> In qualità di Catena di approvvigionamento di AWS amministratore, prima di aggiungere utenti, tieni presente quanto segue:
>
> - Ogni ruolo di autorizzazione utente predefinito è definito con un set di autorizzazioni. È possibile aggiungere utenti ai ruoli di autorizzazione utente predefiniti o creare ruoli di autorizzazione personalizzati.
> - A un utente può essere assegnato un solo ruolo di autorizzazione utente.
> - Non è possibile modificare o eliminare i ruoli di autorizzazione utente predefiniti.
> - Quando modifichi un ruolo di autorizzazione personalizzato che hai creato, le autorizzazioni per tutti gli utenti con il ruolo di autorizzazione personalizzato vengono aggiornate.
> - Quando elimini un ruolo di autorizzazione personalizzato che hai creato, tutti gli utenti con il ruolo di autorizzazione personalizzato perderanno l'accesso a Catena di approvvigionamento di AWS.
> - L'aggiunta di gruppi non è supportata in Catena di approvvigionamento di AWS.

Argomenti

Aggiunta di utenti

> **Note**
>
> Prima di aggiungere utenti, assicurati che l'utente faccia parte di un gruppo IAM Identity Center e che il gruppo sia assegnato a Catena di approvvigionamento di AWS.

In qualità di Catena di approvvigionamento di AWS amministratore, puoi aggiungere utenti per accedere all'applicazione Catena di approvvigionamento di AWS web. Segui questi passaggi per aggiungere un utente.

1. Nella Catena di approvvigionamento di AWS dashboard, dal riquadro di navigazione a sinistra, scegli l'icona Impostazioni.
2. Scegli Autorizzazioni, quindi scegli Utenti.

   Viene visualizzata la pagina Gestisci utenti.
3. Scegli Aggiungi nuovo utente.

   Viene visualizzata la pagina Aggiungi utente.
4. Nel menu a discesa Aggiungi utente/i, seleziona l'utente e, in Seleziona ruolo, seleziona il ruolo per l'utente.
5. Scegli Aggiungi.

Aggiornamento delle autorizzazioni degli utenti

È possibile aggiornare il ruolo di autorizzazione utente per gli Catena di approvvigionamento di AWS utenti correnti. Segui questi passaggi per aggiornare il ruolo delle autorizzazioni utente.

1. Nella Catena di approvvigionamento di AWS dashboard, dal riquadro di navigazione a sinistra, scegli l'icona Impostazioni.

2. Scegli Autorizzazioni, quindi scegli Utenti.

   Viene visualizzata la pagina Gestisci utenti.

3. Nella pagina Gestisci utenti, seleziona l'utente o il gruppo per cui desideri aggiornare il ruolo di autorizzazione utente e, dal menu a discesa Ruolo di autorizzazione, seleziona uno dei ruoli di autorizzazione seguenti:

   > **Note**
   >
   > A seconda delle autorizzazioni di ruolo assegnate, la Catena di approvvigionamento di AWS dashboard è personalizzata. Per ulteriori informazioni, consulta Creazione di ruoli di autorizzazione utente personalizzati.

   - Amministratore: accesso per creare, visualizzare e gestire tutti i dati e le autorizzazioni degli utenti.
   - Analista di dati: accesso per creare, visualizzare e gestire tutte le connessioni dati.
   - Inventory Manager: accesso per creare, visualizzare e gestire Insights.
   - Planner: accesso per creare, visualizzare e gestire previsioni, sostituzioni e pubblicare piani di domanda.

4. Selezionare Salva.

Eliminazione di utenti

In qualità di Catena di approvvigionamento di AWS amministratore, puoi eliminare gli utenti dall'applicazione Web. Catena di approvvigionamento di AWS Segui questi passaggi per eliminare gli utenti.

1. Nella Catena di approvvigionamento di AWS dashboard, dal riquadro di navigazione a sinistra, scegli l'icona Impostazioni.
2. Scegli Autorizzazioni, quindi scegli Utenti.

   Viene visualizzata la pagina Gestisci utenti.

3. Nella pagina Gestisci utenti, seleziona l'utente che desideri eliminare e scegli l'icona Elimina.

Creazione di ruoli di autorizzazione utente personalizzati

Oltre ai ruoli di autorizzazione utente predefiniti, puoi creare ruoli di autorizzazione utente personalizzati per includere più ruoli di autorizzazione e aggiungere sedi e prodotti specifici. Segui questi passaggi per creare nuovi ruoli di autorizzazione.

> **Note**
>
> Puoi scegliere i prodotti e le sedi in Accesso alla posizione e Accesso al prodotto solo se l'istanza è connessa a un'origine dati. Ad esempio, puoi creare un utente Admin personalizzato solo per gestire gli avocado nella sede di Seattle o un utente Insight solo per gestire le informazioni sugli avocado nella sede di Seattle.

1. Nella Catena di approvvigionamento di AWS dashboard, dal riquadro di navigazione a sinistra, scegli l'icona Impostazioni. Scegli Autorizzazioni, quindi scegli Ruoli di autorizzazione.

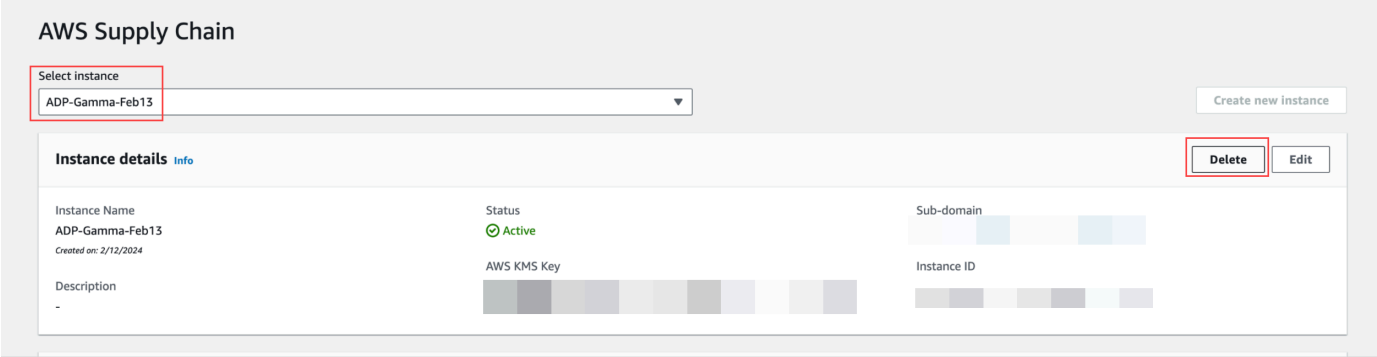
   Viene visualizzata la pagina Ruoli di autorizzazione.
2. Scegli Crea nuovo ruolo.
3. Nella pagina Gestisci ruolo di autorizzazione, in Nome ruolo, inserisci un nome.
4. Sposta il cursore per selezionare il ruolo di autorizzazione dell'utente.
   - Gestisci: l'assegnazione dell'autorizzazione di gestione agli utenti può aggiungere, modificare e gestire informazioni.
   - Visualizza: l'assegnazione dell'autorizzazione alla visualizzazione agli utenti può visualizzare solo le informazioni correnti.
5. In Accesso alla posizione, cerca le regioni mentre digiti nella barra di ricerca e seleziona le regioni.
6. In Accesso al prodotto, cerca i prodotti mentre digiti nella barra di ricerca e seleziona i prodotti.
7. Selezionare Salva.

Eliminazione di un'istanza

Per eliminare un'istanza, procedi nel seguente modo.

> **Note**
>
> Quando elimini un'istanza, le informazioni dal bucket Amazon S3 non vengono eliminate automaticamente.

1. Apri la Catena di approvvigionamento di AWS console all'indirizzo. https://console.aws.amazon.com/scn/home
2. Nella dashboard della Catena di approvvigionamento di AWS console, dal menu a discesa, seleziona l'istanza che desideri eliminare.



3. Scegli Elimina.
4. Nella pagina Elimina Catena di approvvigionamento di AWS istanza, in Conferma, digita **`delete`** per confermare che desideri eliminare l'istanza.
5. Scegli Elimina. L'eliminazione dell'istanza inizia e, una volta eliminata, verrà visualizzato un messaggio di conferma.

Sicurezza in Catena di approvvigionamento di AWS

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di data center e architetture di rete progettati per AWS soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra te e. AWS Il modello di responsabilità condivisa) lo descrive come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che funziona Servizi AWS nel Cloud AWS. AWS fornisce inoltre servizi che è possibile utilizzare in modo sicuro. I revisori di terze parti testano e verificano regolarmente l'efficacia della sicurezza come parte dei programmi di conformità AWS. Per maggiori informazioni sui programmi di conformità applicabili Catena di approvvigionamento di AWS, consulta la sezione AWS Servizi rientranti nell'ambito del programma di conformità AWS .
- Sicurezza nel cloud: Servizio AWS ciò che utilizzi determina la tua responsabilità. Sei responsabile anche di altri fattori, tra cui la sensibilità dei tuoi dati, i tuoi requisiti e le leggi e i regolamenti applicabili.

Questa documentazione ti aiuta a capire come applicare il modello di responsabilità condivisa quando lo usi. Catena di approvvigionamento di AWS I seguenti argomenti mostrano come configurare per Catena di approvvigionamento di AWS soddisfare gli obiettivi di sicurezza e conformità. Imparerai anche a utilizzarne altri Servizi AWS che ti aiutano a monitorare e proteggere Catena di approvvigionamento di AWS le tue risorse.

Argomenti

Protezione dei dati in Catena di approvvigionamento di AWS

Il modello di responsabilità AWS condivisa modello di di si applica alla protezione dei dati in Catena di approvvigionamento di AWS. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. Inoltre, sei responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS che utilizzi. Per ulteriori informazioni sulla privacy dei dati, vedi le Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al Modello di responsabilità condivisa AWS e GDPR nel Blog sulla sicurezza AWS .

Ai fini della protezione dei dati, consigliamo di proteggere Account AWS le credenziali e configurare i singoli utenti con AWS IAM Identity Center or AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Usa SSL/TLS per comunicare con le risorse. AWS È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con. AWS CloudTrail
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-2 per l'accesso AWS tramite un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-2.

Ti consigliamo vivamente di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori o Servizi AWS utilizzi la console, l'API Catena di approvvigionamento di AWS o gli SDK. AWS CLI AWS I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando fornisci un URL a un server esterno, ti suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta al server.

Dati gestiti da Catena di approvvigionamento di AWS

Per limitare i dati a cui possono accedere gli utenti autorizzati di una specifica istanza della catena di AWS fornitura, i dati contenuti all'interno della catena di AWS fornitura sono separati in base all'ID AWS dell'account e all'ID dell'istanza della catena AWS di fornitura.

AWS Supply Chain gestisce una varietà di dati della catena di approvvigionamento, come le informazioni sugli utenti, le informazioni estratte dal connettore dati e i dettagli dell'inventario.

Preferenza di opt-out

Possiamo utilizzare e archiviare i tuoi contenuti elaborati da Catena di approvvigionamento di AWS, come indicato nei Termini del servizio AWS. Se desideri rinunciare all'utilizzo o all' Catena di approvvigionamento di AWS archiviazione dei tuoi contenuti, puoi creare una policy di opt-out in AWS Organizations. Per ulteriori informazioni sulla creazione di una politica di opt-out, consulta la sintassi e gli esempi della policy di opt-out dei servizi AI.

Crittografia a riposo

I dati di contatto classificati come PII, o i dati che rappresentano i contenuti dei clienti archiviati da Catena di approvvigionamento di AWS, vengono crittografati quando sono inattivi (ovvero prima di essere inseriti, archiviati o salvati su un disco) con una chiave limitata nel tempo e specifica per l'istanza. Catena di approvvigionamento di AWS

La crittografia lato server di Amazon S3 viene utilizzata per crittografare tutti i dati della console e delle applicazioni Web con una chiave AWS Key Management Service dati unica per ogni account cliente. Per informazioni su AWS KMS keys, consulta What is? AWS Key Management Service nella Guida per gli AWS Key Management Service sviluppatori.

> **Note**
>
> Catena di approvvigionamento di AWS le funzionalità Supply Planning e N-Tier Visibility non supportano la crittografia data-at-rest con il KMS-CMK fornito.

Crittografia in transito

I dati scambiati con AWS Supply Chain sono protetti durante il transito tra il browser Web dell'utente e AWS Supply Chain utilizzando la crittografia TLS standard del settore.

Gestione delle chiavi

Catena di approvvigionamento di AWS supporta parzialmente KMS-CMK.

Per informazioni sull'aggiornamento della chiave AWS KMS Catena di approvvigionamento di AWS, consulta. Creazione di un'istanza

Riservatezza del traffico Internet

> **Note**
>
> Catena di approvvigionamento di AWS non supporta PrivateLink.

Un endpoint di cloud privato virtuale (VPC) per Catena di approvvigionamento di AWS è un'entità logica all'interno di un VPC che consente la connettività solo a. Catena di approvvigionamento di AWS Il VPC indirizza le richieste Catena di approvvigionamento di AWS e reindirizza le risposte al VPC. Per ulteriori informazioni, consulta VPC Endpoints nella VPC User Guide.

Come utilizza le sovvenzioni Catena di approvvigionamento di AWS in AWS KMS

Catena di approvvigionamento di AWS richiede una concessione per utilizzare la chiave gestita dal cliente.

Catena di approvvigionamento di AWS crea diverse concessioni utilizzando la AWS KMS chiave che viene passata durante l'CreateInstanceoperazione. Catena di approvvigionamento di AWS crea una sovvenzione per tuo conto inviando CreateGrantrichieste a AWS KMS. Le sovvenzioni AWS KMS vengono utilizzate per Catena di approvvigionamento di AWS consentire l'accesso alla AWS KMS chiave in un account cliente.

> **Note**
>
> Catena di approvvigionamento di AWS utilizza il proprio meccanismo di autorizzazione. Una volta aggiunto un utente Catena di approvvigionamento di AWS, non è possibile negare che lo stesso utente utilizzi la AWS KMS politica.

Catena di approvvigionamento di AWS utilizza la concessione per quanto segue:

- Per inviare GenerateDataKeyrichieste AWS KMS di crittografia dei dati archiviati nell'istanza.
- A cui inviare richieste Decrypt per AWS KMS leggere i dati crittografati associati all'istanza.
- Per aggiungere DescribeKeye RetireGrantautorizzazioni per proteggere i tuoi dati quando li invii ad altri AWS servizi come Amazon Forecast. CreateGrant

Puoi revocare l'accesso alla concessione o rimuovere l'accesso del servizio alla chiave gestita dal cliente in qualsiasi momento. Se lo fai, non Catena di approvvigionamento di AWS sarai in grado di accedere a nessuno dei dati crittografati dalla chiave gestita dal cliente, il che influirà sulle operazioni che dipendono da tali dati.

Monitoraggio della crittografia per Catena di approvvigionamento di AWS

Gli esempi seguenti sono AWS CloudTrail eventi per `Encrypt` e `Decrypt` per monitorare le operazioni KMS chiamate Catena di approvvigionamento di AWS ad accedere ai dati crittografati dalla chiave gestita dal cliente: `GenerateDataKey`

Encrypt


```
            {
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "scn.amazonaws.com"
    },
    "eventTime": "2024-03-06T22:39:32Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Encrypt",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "172.12.34.56"
    "userAgent": "Example/Desktop/1.0 (V1; OS)",
    "requestParameters": {
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
        "keyId": "arn:aws:kms:us-
east-1:123456789:key/1234abcd-11ab-22bc-33ef-123456sample"
    },
    "responseElements": null,
    "requestID": "12a345n4-78a4-8888-0000-a000-6q000yy666rr",
    "eventID": "12a345n4-78a4-8888-0000-a000-6q000yy666rr",
    "readOnly": true,
    "resources": [
```

```
        {
            "accountId": account ID,
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
east-1:123456789:key/1234abcd-11ab-22bc-33ef-123456sample"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "112233445566",
    "sharedEventID": "fdf9ee0f-e43f-4e43-beac-df69067edb8b",
    "eventCategory": "Management"
}
```

GenerateDataKey

```
            {
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "scn.amazonaws.com"
    },
     "eventTime": "2024-03-06T22:39:32Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "172.12.34.56"
    "userAgent": "Example/Desktop/1.0 (V1; OS)",
    "requestParameters": {
        "encryptionContext": {
            "aws:s3:arn": "arn:aws:s3:::test/rawEvent/bf6666c1-111-48aaca-b6b0-
dsadsadsa3432423/noFlowName/scn.data.inboundorder/20240306_223934_536"
        },
        "keyId": "arn:aws:kms:us-
east-1:123456789:key/1234abcd-11ab-22bc-33ef-123456sample",
        "keySpec": "AES_222"
    },
    "responseElements": null,
    "requestID": "12a345n4-78a4-8888-0000-a000-6q000yy666rr",
    "eventID": "12a345n4-78a4-8888-0000-a000-6q000yy666rr",
    "readOnly": true,
```

```
    "resources": [
        {
            "accountId": account ID,
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
east-1:123456789:key/1234abcd-11ab-22bc-33ef-123456sample"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "112233445566",
    "sharedEventID": "fdf9ee0f-e43f-4e43-beac-df69067edb8b",
    "eventCategory": "Management"
}
```

Decrypt

```
            {
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "scn.amazonaws.com"
    },
     "eventTime": "2024-03-06T22:39:32Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "172.12.34.56"
    "userAgent": "Example/Desktop/1.0 (V1; OS)",
    "requestParameters": {
        "keyId": "arn:aws:kms:us-
east-1:123456789:key/1234abcd-11ab-22bc-33ef-123456sample",
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT"
    },
    "responseElements": null,
    "requestID": "12a345n4-78a4-8888-0000-a000-6q000yy666rr",
    "eventID": "12a345n4-78a4-8888-0000-a000-6q000yy666rr",
    "readOnly": true,
    "resources": [
        {
            "accountId": account ID,
```

```
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
east-1:123456789:key/1234abcd-11ab-22bc-33ef-123456sample"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "112233445566",
    "sharedEventID": "fdf9ee0f-e43f-4e43-beac-df69067edb8b",
    "eventCategory": "Management"
}
```

Accesso Catena di approvvigionamento di AWS tramite un endpoint di interfaccia () AWS PrivateLink

Puoi usarlo AWS PrivateLink per creare una connessione privata tra il tuo VPC e. Catena di approvvigionamento di AWS Puoi accedere Catena di approvvigionamento di AWS come se fosse nel tuo VPC, senza l'uso di un gateway Internet, un dispositivo NAT, una connessione VPN o una connessione. AWS Direct Connect Le istanze del tuo VPC non necessitano di indirizzi IP pubblici per accedervi. Catena di approvvigionamento di AWS

Stabilisci questa connessione privata creando un endpoint di interfaccia attivato da AWS PrivateLink. In ciascuna sottorete viene creata un'interfaccia di rete endpoint da abilitare per l'endpoint di interfaccia. Queste sono interfacce di rete gestite dal richiedente che fungono da punto di ingresso per il traffico destinato a Catena di approvvigionamento di AWS.

Per ulteriori informazioni, consulta Access Servizi AWS through AWS PrivateLink nella AWS PrivateLink Guida.

Considerazioni per Catena di approvvigionamento di AWS

Prima di configurare un endpoint di interfaccia per Catena di approvvigionamento di AWS, consulta le considerazioni nella Guida. AWS PrivateLink

Catena di approvvigionamento di AWS supporta l'esecuzione di chiamate a tutte le sue azioni API tramite l'endpoint dell'interfaccia.

Crea un endpoint di interfaccia per Catena di approvvigionamento di AWS

Puoi creare un endpoint di interfaccia per Catena di approvvigionamento di AWS utilizzare la console Amazon VPC o AWS Command Line Interface (). AWS CLI Per ulteriori informazioni, consulta la sezione Creazione di un endpoint di interfaccia nella Guida per l'utente di AWS PrivateLink .

Crea un endpoint di interfaccia per Catena di approvvigionamento di AWS utilizzare il seguente nome di servizio:

```
com.amazonaws.region.scn
```

Se abiliti il DNS privato per l'endpoint dell'interfaccia, puoi effettuare richieste API Catena di approvvigionamento di AWS utilizzando il nome DNS regionale predefinito. Ad esempio, *scn*.*region*.amazonaws.com.

Creazione di una policy dell' endpoint per l'endpoint dell'interfaccia

Una policy dell'endpoint è una risorsa IAM che è possibile allegare all'endpoint dell'interfaccia. La policy predefinita per gli endpoint consente l'accesso completo Catena di approvvigionamento di AWS tramite l'endpoint dell'interfaccia. Per controllare l'accesso consentito Catena di approvvigionamento di AWS dal tuo VPC, collega una policy endpoint personalizzata all'endpoint di interfaccia.

Una policy di endpoint specifica le informazioni riportate di seguito:

- I principali che possono eseguire azioni (utenti IAM Account AWS e ruoli IAM)
- Le azioni che possono essere eseguite
- Le risorse su cui è possibile eseguire le azioni

Per ulteriori informazioni, consulta la sezione Controllo dell'accesso ai servizi con policy di endpoint nella Guida di AWS PrivateLink .

Esempio: policy degli endpoint VPC per le azioni Catena di approvvigionamento di AWS

Di seguito è riportato l'esempio di una policy dell'endpoint personalizzata. Se collegata a un endpoint dell'interfaccia, questa policy concede l'accesso alle operazioni Catena di approvvigionamento di AWS elencate per tutti i principali su tutte le risorse.

```
{
   "Statement": [
      {
         "Principal": "*",
         "Effect": "Allow",
         "Action": [

            "scn:action-1",
            "scn:action-2",
            "scn:action-3"

         ],
         "Resource":"*"
      }
   ]
}
```

IAM per Catena di approvvigionamento di AWS

AWS Identity and Access Management (IAM) è un software Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle AWS risorse. Gli amministratori IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse. Catena di approvvigionamento di AWS IAM è uno Servizio AWS strumento che puoi utilizzare senza costi aggiuntivi.

Argomenti

- Destinatari
- Autenticazione con identità
- Gestione dell'accesso con policy
- Come Catena di approvvigionamento di AWS funziona con IAM
- Esempi di policy basate su identità per Catena di approvvigionamento di AWS
- Risoluzione dei problemi Catena di approvvigionamento di AWS di identità e accesso

Destinatari

Il modo in cui usi AWS Identity and Access Management (IAM) varia a seconda del lavoro che Catena di approvvigionamento di AWS svolgi.

Utente del servizio: se utilizzi il Catena di approvvigionamento di AWS servizio per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzi più Catena di approvvigionamento di AWS funzionalità per svolgere il tuo lavoro, potresti aver bisogno di autorizzazioni aggiuntive. La comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non riesci ad accedere a una funzionalità di Catena di approvvigionamento di AWS, consulta Risoluzione dei problemi Catena di approvvigionamento di AWS di identità e accesso.

Amministratore del servizio: se sei responsabile delle Catena di approvvigionamento di AWS risorse della tua azienda, probabilmente hai pieno accesso a Catena di approvvigionamento di AWS. È tuo compito determinare a quali Catena di approvvigionamento di AWS funzionalità e risorse devono accedere gli utenti del servizio. Devi inviare le richieste all'amministratore IAM per cambiare le autorizzazioni degli utenti del servizio. Esamina le informazioni contenute in questa pagina per comprendere i concetti di base relativi a IAM. Per saperne di più su come la tua azienda può utilizzare IAM con Catena di approvvigionamento di AWS, consultaCome Catena di approvvigionamento di AWS funziona con IAM.

Amministratore IAM: un amministratore IAM potrebbe essere interessato a ottenere dei dettagli su come scrivere policy per gestire l'accesso a Catena di approvvigionamento di AWS. Per visualizzare esempi di policy Catena di approvvigionamento di AWS basate sull'identità che puoi utilizzare in IAM, consulta. Esempi di policy basate su identità per Catena di approvvigionamento di AWS

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi essere autenticato (aver effettuato l' Utente root dell'account AWS accesso AWS) come utente IAM o assumendo un ruolo IAM.

Puoi accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center Gli utenti (IAM Identity Center), l'autenticazione Single Sign-On della tua azienda e le tue credenziali di Google o Facebook sono esempi di identità federate. Se accedi come identità federata, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Quando accedi AWS utilizzando la federazione, assumi indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere al AWS Management Console o al portale di AWS accesso. Per ulteriori informazioni sull'accesso a AWS, vedi Come accedere al tuo Account AWS nella Guida per l'Accedi ad AWS utente.

Se accedi a AWS livello di codice, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le tue richieste utilizzando le tue credenziali. Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sull'utilizzo del metodo consigliato per firmare autonomamente le richieste, consulta Signing AWS API request nella IAM User Guide.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. Ad esempio, ti AWS consiglia di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza del tuo account. Per ulteriori informazioni, consulta Autenticazione a più fattori nella Guida per l'utente di AWS IAM Identity Center e Utilizzo dell'autenticazione a più fattori (MFA) in AWSnella Guida per l'utente IAM.

Account AWS utente root

Quando si crea un account Account AWS, si inizia con un'identità di accesso che ha accesso completo a tutte Servizi AWS le risorse dell'account. Questa identità è denominata utente Account AWS root ed è accessibile effettuando l'accesso con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente root e utilizzale per eseguire le operazioni che solo l'utente root può eseguire. Per un elenco completo delle attività che richiedono l'accesso come utente root, consulta la sezione Attività che richiedono le credenziali dell'utente root nella Guida per l'utente IAM.

Identità federata

Come procedura consigliata, richiedi agli utenti umani, compresi gli utenti che richiedono l'accesso come amministratore, di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente dell'elenco utenti aziendale, di un provider di identità Web AWS Directory Service, della directory Identity Center o di qualsiasi utente che accede utilizzando le Servizi AWS credenziali fornite tramite un'origine di identità. Quando le identità federate accedono Account AWS, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. Puoi creare utenti e gruppi in IAM Identity Center oppure puoi connetterti e sincronizzarti con un set di utenti e gruppi nella tua fonte di identità per utilizzarli su tutte le tue applicazioni. Account AWS Per ulteriori informazioni su IAM Identity Center, consulta Cos'è IAM Identity Center? nella Guida per l'utente di AWS IAM Identity Center .

Utenti e gruppi IAM

Un utente IAM è un'identità interna Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ove possibile, consigliamo di fare affidamento a credenziali temporanee invece di creare utenti IAM con credenziali a lungo termine come le password e le chiavi di accesso. Tuttavia, se si hanno casi d'uso specifici che richiedono credenziali a lungo termine con utenti IAM, si consiglia di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta la pagina Rotazione periodica delle chiavi di accesso per casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente IAM.

Un gruppo IAM è un'identità che specifica un insieme di utenti IAM. Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, è possibile avere un gruppo denominato IAMAdmins e concedere a tale gruppo le autorizzazioni per amministrare le risorse IAM.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta Quando creare un utente IAM (invece di un ruolo) nella Guida per l'utente IAM.

Ruoli IAM

Un ruolo IAM è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. Puoi assumere temporaneamente un ruolo IAM in AWS Management Console cambiando ruolo. Puoi assumere un ruolo chiamando un'operazione AWS CLI o AWS API o utilizzando un URL personalizzato. Per ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta Utilizzo di ruoli IAM nella Guida per l'utente IAM.

I ruoli IAM con credenziali temporanee sono utili nelle seguenti situazioni:

- Accesso utente federato: per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per ulteriori informazioni sulla federazione dei ruoli, consulta Creazione di un ruolo per un provider di identità di terza parte nella Guida per l'utente IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. IAM Identity Center mette in correlazione il set di autorizzazioni con un ruolo in

IAM per controllare a cosa possono accedere le identità dopo l'autenticazione. Per informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .

- Autorizzazioni utente IAM temporanee: un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso multi-account: è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni Servizi AWS, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per conoscere la differenza tra ruoli e politiche basate sulle risorse per l'accesso tra account diversi, consulta Cross Account Resource Access in IAM nella IAM User Guide.
- Accesso tra servizi: alcuni Servizi AWS utilizzano funzionalità in altri. Servizi AWS Ad esempio, quando effettui una chiamata in un servizio, è comune che tale servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
  - Sessioni di accesso diretto (FAS): quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, combinate con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Forward access sessions.
  - Ruolo di servizio: un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire azioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWSnella Guida per l'utente IAM.
  - Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un ruolo IAM per gestire le credenziali temporanee per le applicazioni in esecuzione su un'istanza EC2 e che AWS CLI effettuano richieste API. AWS Ciò è preferibile all'archiviazione delle chiavi di accesso nell'istanza EC2. Per assegnare un AWS ruolo a un'istanza EC2 e renderlo disponibile per tutte le sue applicazioni, crei un profilo di istanza collegato all'istanza. Un profilo dell'istanza contiene il ruolo e consente ai programmi in esecuzione sull'istanza EC2 di ottenere le credenziali temporanee. Per ulteriori informazioni, consulta Utilizzo di un ruolo IAM per concedere autorizzazioni ad applicazioni in esecuzione su istanze di Amazon EC2 nella Guida per l'utente IAM.

Per informazioni sull'utilizzo dei ruoli IAM, consulta Quando creare un ruolo IAM (invece di un utente) nella Guida per l'utente IAM.

Gestione dell'accesso con policy

Puoi controllare l'accesso AWS creando policy e collegandole a AWS identità o risorse. Una policy è un oggetto AWS che, se associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste politiche quando un principale (utente, utente root o sessione di ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle politiche viene archiviata AWS come documenti JSON. Per ulteriori informazioni sulla struttura e sui contenuti dei documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente IAM.

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire operazioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Le policy IAM definiscono le autorizzazioni relative a un'operazione, a prescindere dal metodo utilizzato per eseguirla. Ad esempio, supponiamo di disporre di una policy che consente l'operazione `iam:GetRole`. Un utente con tale policy può ottenere informazioni sul ruolo dall' AWS Management Console AWS CLI, dall'o dall' AWS API.

Policy basate su identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le azioni che utenti e ruoli

possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente IAM.

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono integrate direttamente in un singolo utente, gruppo o ruolo. Le politiche gestite sono politiche autonome che puoi allegare a più utenti, gruppi e ruoli nel tuo Account AWS. Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scelta fra policy gestite e policy inline nella Guida per l'utente IAM.

Policy basate su risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non puoi utilizzare le policy AWS gestite di IAM in una policy basata sulle risorse.

Liste di controllo degli accessi (ACL)

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni per accedere a una risorsa. Le ACL sono simili alle policy basate su risorse, sebbene non utilizzino il formato del documento di policy JSON.

Amazon S3 e Amazon VPC sono esempi di servizi che supportano gli ACL. AWS WAF Per maggiori informazioni sulle ACL, consulta Panoramica delle liste di controllo degli accessi (ACL) nella Guida per gli sviluppatori di Amazon Simple Storage Service.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi e meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai tipi di policy più comuni.

- Limiti delle autorizzazioni: un limite delle autorizzazioni è una funzionalità avanzata nella quale si imposta il numero massimo di autorizzazioni che una policy basata su identità può concedere a

un'entità IAM (utente o ruolo IAM). È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal`sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente IAM.

- Politiche di controllo dei servizi (SCP): le SCP sono politiche JSON che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in. AWS Organizations AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più Account AWS di proprietà dell'azienda. Se abiliti tutte le funzionalità in un'organizzazione, puoi applicare le policy di controllo dei servizi (SCP) a uno o tutti i tuoi account. L'SCP limita le autorizzazioni per le entità negli account dei membri, inclusa ciascuna. Utente root dell'account AWS Per ulteriori informazioni su organizzazioni e policy SCP, consulta la pagina sulle Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations .
- Policy di sessione: le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta Policy di sessione nella Guida per l'utente IAM.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per scoprire come si AWS determina se consentire una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle policy nella IAM User Guide.

Come Catena di approvvigionamento di AWS funziona con IAM

Prima di utilizzare IAM per gestire l'accesso a Catena di approvvigionamento di AWS, scopri con quali funzionalità IAM è disponibile l'uso Catena di approvvigionamento di AWS.

Funzionalità IAM che puoi utilizzare con Catena di approvvigionamento di AWS

Funzionalità IAM	Catena di approvvigionamento di AWS supporto
Policy basate su identità	Sì
Policy basate su risorse	No
Azioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione delle policy	Sì
Credenziali temporanee	Sì
Inoltro delle sessioni di accesso (FAS)	Sì
Ruoli di servizio	Sì
Ruoli collegati al servizio	No

Per avere una panoramica di alto livello su come Catena di approvvigionamento di AWS e altri AWS servizi funzionano con la maggior parte delle funzionalità IAM, consulta AWS i servizi che funzionano con IAM nella IAM User Guide.

Politiche basate sull'identità per Catena di approvvigionamento di AWS

Supporta le policy basate su identità	Sì

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente IAM.

Con le policy basate su identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. Non è possibile specificare l'entità principale in una policy basata sull'identità perché si applica

all'utente o al ruolo a cui è associato. Per informazioni su tutti gli elementi utilizzabili in una policy JSON, consulta Guida di riferimento agli elementi delle policy JSON IAM nella Guida per l'utente di IAM.

Esempi di politiche basate sull'identità per Catena di approvvigionamento di AWS

Per visualizzare esempi di politiche basate sull' Catena di approvvigionamento di AWS identità, vedere. Esempi di policy basate su identità per Catena di approvvigionamento di AWS

Politiche basate sulle risorse all'interno Catena di approvvigionamento di AWS

Supporta le policy basate su risorse	No

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Per consentire l'accesso multi-account, puoi specificare un intero account o entità IAM in un altro account come principale in una policy basata sulle risorse. L'aggiunta di un principale multi-account a una policy basata sulle risorse rappresenta solo una parte della relazione di trust. Quando il principale e la risorsa sono diversi Account AWS, un amministratore IAM dell'account affidabile deve inoltre concedere all'entità principale (utente o ruolo) l'autorizzazione ad accedere alla risorsa. L'autorizzazione viene concessa collegando all'entità una policy basata sull'identità. Tuttavia, se una policy basata su risorse concede l'accesso a un principale nello stesso account, non sono richieste ulteriori policy basate su identità. Per ulteriori informazioni, consulta Cross Account Resource Access in IAM nella IAM User Guide.

Azioni politiche per Catena di approvvigionamento di AWS

Supporta le operazioni di policy	Sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Action`di una policy JSON descrive le azioni che è possibile utilizzare per consentire o negare l'accesso a un criterio. Le azioni politiche in genere hanno lo stesso nome dell'operazione AWS API associata. Ci sono alcune eccezioni, ad esempio le azioni di sola autorizzazione che non hanno un'operazione API corrispondente. Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

Includi le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Le azioni politiche Catena di approvvigionamento di AWS utilizzano il seguente prefisso prima dell'azione:

```
scn
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola.

```
"Action": [
      "scn:action1",
      "scn:action2"
         ]
```

Per visualizzare esempi di politiche Catena di approvvigionamento di AWS basate sull'identità, vedere. Esempi di policy basate su identità per Catena di approvvigionamento di AWS

Risorse politiche per Catena di approvvigionamento di AWS

Supporta le risorse di policy	Sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento JSON `Resource`della policy specifica l'oggetto o gli oggetti ai quali si applica l'operazione. Le istruzioni devono includere un elemento `Resource`o un elemento `NotResource`.

Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). Puoi eseguire questa operazione per azioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le azioni che non supportano le autorizzazioni a livello di risorsa, ad esempio le operazioni di elenco, utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

```
"Resource": "*"
```

Per visualizzare esempi di politiche basate sull' Catena di approvvigionamento di AWS identità, consulta. Esempi di policy basate su identità per Catena di approvvigionamento di AWS

Chiavi relative alle condizioni delle politiche per Catena di approvvigionamento di AWS

Supporta le chiavi di condizione delle policy specifiche del servizio	Sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Condition`(o blocco `Condition`) consente di specificare le condizioni in cui un'istruzione è in vigore. L'elemento `Condition`è facoltativo. Puoi compilare espressioni condizionali che utilizzano operatori di condizione, ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta.

Se specifichi più elementi `Condition`in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione `AND`logica. Se si specificano più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione logica. `OR` Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

Puoi anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, puoi autorizzare un utente IAM ad accedere a una risorsa solo se è stata taggata con il relativo nome utente IAM. Per ulteriori informazioni, consulta Elementi delle policy IAM: variabili e tag nella Guida per l'utente di IAM.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche del servizio. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'utente IAM.

Per visualizzare esempi di politiche Catena di approvvigionamento di AWS basate sull'identità, consulta. Esempi di policy basate su identità per Catena di approvvigionamento di AWS

Utilizzo di credenziali temporanee con Catena di approvvigionamento di AWS

Supporta le credenziali temporanee	Sì

Alcuni Servizi AWS non funzionano quando si accede utilizzando credenziali temporanee. Per ulteriori informazioni, incluse quelle che Servizi AWS funzionano con credenziali temporanee, consulta la sezione relativa alla Servizi AWS compatibilità con IAM nella IAM User Guide.

Stai utilizzando credenziali temporanee se accedi AWS Management Console utilizzando qualsiasi metodo tranne nome utente e password. Ad esempio, quando accedi AWS utilizzando il link Single Sign-On (SSO) della tua azienda, tale processo crea automaticamente credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla console come utente e poi cambi ruolo. Per ulteriori informazioni sullo scambio dei ruoli, consulta Cambio di un ruolo (console) nella Guida per l'utente IAM.

È possibile creare manualmente credenziali temporanee utilizzando l'API or. AWS CLI AWS È quindi possibile utilizzare tali credenziali temporanee per accedere. AWS AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta Credenziali di sicurezza provvisorie in IAM.

Sessioni di accesso diretto per Catena di approvvigionamento di AWS

Supporta l'inoltro delle sessioni di accesso (FAS)	Sì

Quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, in combinazione con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le

richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Inoltro sessioni di accesso.

Ruoli di servizio per Catena di approvvigionamento di AWS

Supporta i ruoli di servizio	Sì

Un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWSnella Guida per l'utente IAM.

> **Warning**
>
> La modifica delle autorizzazioni per un ruolo di servizio potrebbe compromettere la funzionalità. Catena di approvvigionamento di AWS Modifica i ruoli di servizio solo quando viene Catena di approvvigionamento di AWS fornita una guida in tal senso.

Ruoli collegati ai servizi per Catena di approvvigionamento di AWS

Supporta i ruoli collegati ai servizi	No

Un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

Per informazioni dettagliate sulla creazione o la gestione di ruoli collegati ai servizi, consulta Servizi AWS That work with IAM. Trova un servizio nella tabella che include un `Yes` nella colonna Service-linked role (Ruolo collegato ai servizi). Scegli il collegamento Sì per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Esempi di policy basate su identità per Catena di approvvigionamento di AWS

Per impostazione predefinita, gli utenti e i ruoli non sono autorizzati a creare o modificare Catena di approvvigionamento di AWS risorse. Inoltre, non possono eseguire attività utilizzando la Console di gestione AWS, l'interfaccia a riga di comando AWS (AWS CLI) o l'API AWS. Per concedere agli utenti l'autorizzazione a eseguire operazioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Per scoprire come creare una policy basata sull'identità IAM utilizzando questi esempi di documenti di policy JSON, consulta Creating IAM policies nella IAM User Guide.

Argomenti

Best practice per le policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare risorse nel tuo account. Catena di approvvigionamento di AWS Queste azioni possono comportare costi aggiuntivi per l' Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche gestite che concedono le autorizzazioni per molti casi d'uso comuni.AWS Sono disponibili nel tuo. Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta Policy gestite da AWSo Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente IAM.
- Applica le autorizzazioni con privilegio minimo: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. Puoi farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso a operazioni e risorse puoi aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate

utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente IAM.

- Utilizzo di IAM Access Analyzer per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano alla sintassi della policy IAM (JSON) e alle best practice di IAM. IAM Access Analyzer offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per ulteriori informazioni, consulta Convalida delle policy per IAM Access Analyzer nella Guida per l'utente IAM.
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel Account AWS tuo, attiva l'MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta Configurazione dell'accesso alle API protetto con MFA nella Guida per l'utente IAM.

Per maggiori informazioni sulle best practice in IAM, consulta Best practice di sicurezza in IAM nella Guida per l'utente di IAM.

Risoluzione dei problemi Catena di approvvigionamento di AWS di identità e accesso

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con un Catena di approvvigionamento di AWS IAM.

Argomenti

- Non sono autorizzato a eseguire un'azione in Catena di approvvigionamento di AWS
- Non sono autorizzato a eseguire iam: PassRole
- Voglio consentire a persone esterne a me di accedere Account AWS alle mie Catena di approvvigionamento di AWS risorse

Non sono autorizzato a eseguire un'azione in Catena di approvvigionamento di AWS

Se AWS Management Console non sei autorizzato a eseguire un'azione, devi contattare l'amministratore per ricevere assistenza. L'amministratore è la persona da cui si sono ricevuti il nome utente e la password.

L'errore di esempio seguente si verifica quando l'utente IAM `mateojackson` prova a utilizzare la console per visualizzare i dettagli relativi a una risorsa *`my-example-widget`* fittizia ma non dispone di autorizzazioni `scn:`*`GetWidget`* fittizie.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 scn:GetWidget on resource: my-example-widget
```

In questo caso, Mateo richiede al suo amministratore di aggiornare le policy per poter accedere alla risorsa *`my-example-widget`* utilizzando l'azione `scn:`*`GetWidget`*.

Non sono autorizzato a eseguire iam: PassRole

Se ricevi un errore che indica che non sei autorizzato a eseguire l'operazione `iam:PassRole`, le tue policy devono essere aggiornate per poter passare un ruolo a Catena di approvvigionamento di AWS.

Alcuni Servizi AWS consentono di passare un ruolo esistente a quel servizio invece di creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

L'errore di esempio seguente si verifica quando un utente IAM denominato `marymajor` cerca di utilizzare la console per eseguire un'operazione in Catena di approvvigionamento di AWS. Tuttavia, l'operazione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per passare il ruolo al servizio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Voglio consentire a persone esterne a me di accedere Account AWS alle mie Catena di approvvigionamento di AWS risorse

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per servizi che supportano policy basate su risorse o liste di controllo degli accessi (ACL), utilizza tali policy per concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se Catena di approvvigionamento di AWS supporta queste funzionalità, consultaCome Catena di approvvigionamento di AWS funziona con IAM.
- Per scoprire come fornire l'accesso alle tue risorse attraverso Account AWS le risorse di tua proprietà, consulta Fornire l'accesso a un utente IAM in un altro Account AWS di tua proprietà nella IAM User Guide.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a soggetti Account AWS di proprietà di terze parti nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (Federazione delle identità) nella Guida per l'utente IAM.
- Per scoprire la differenza tra l'utilizzo di ruoli e politiche basate sulle risorse per l'accesso tra account diversi, consulta Cross Account Resource Access in IAM nella IAM User Guide.

Policy gestite da AWS per Catena di approvvigionamento di AWS

Una policy gestita da AWSè una policy autonoma creata e amministrata da AWS. Le policy gestite da AWSsono progettate per fornire autorizzazioni per molti casi d'uso comuni in modo da poter iniziare ad assegnare autorizzazioni a utenti, gruppi e ruoli.

Ricorda che le policy gestite da AWSpotrebbero non concedere autorizzazioni con privilegi minimi per i tuoi casi d'uso specifici perché possono essere utilizzate da tutti i clienti AWS. Consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente specifiche per i tuoi casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle policy gestite da AWS. Se AWSaggiorna le autorizzazioni definite in una policy gestita da AWS, l'aggiornamento riguarda tutte le identità

principali (utenti, gruppi e ruoli) a cui è collegata la policy. È molto probabile che AWSaggiorni una policy gestita da AWSquando viene lanciato un nuovo Servizio AWSo nuove operazioni API diventano disponibili per i servizi esistenti.

Per ulteriori informazioni, consultare Policy gestite da AWSnella Guida per l'utente di IAM.

AWSpolitica gestita: AWSSupplyChainFederationAdminAccess

AWSSupplyChainFederationAdminAccess fornisce agli utenti Catena di approvvigionamento di AWS federati l'accesso all'Catena di approvvigionamento di AWSapplicazione, incluse le autorizzazioni necessarie per eseguire azioni all'interno dell'Catena di approvvigionamento di AWSapplicazione. La policy fornisce autorizzazioni amministrative per gli utenti e i gruppi di IAM Identity Center ed è associata a un ruolo creato da Catena di approvvigionamento di AWS for you. Non dovresti collegare la AWSSupplyChainFederationAdminAccess policy a nessun'altra entità IAM.

Sebbene questa policy fornisca tutti gli accessi Catena di approvvigionamento di AWS tramite le autorizzazioni scn: *, il Catena di approvvigionamento di AWS ruolo determina le autorizzazioni dell'utente. Il Catena di approvvigionamento di AWS ruolo include solo le autorizzazioni richieste e non dispone delle autorizzazioni per le API di amministrazione.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `Chime`— Fornisce l'accesso per creare o eliminare utenti in Amazon Chime AppInstance; Fornisce l'accesso per gestire il canale, i membri del canale e i moderatori; Fornisce l'accesso per inviare messaggi al canale. Le operazioni di Chime sono limitate alle istanze dell'app contrassegnate con «SCN». InstanceId
- `AWS IAM Identity Center (AWS SSO)`— Fornisce le autorizzazioni necessarie per associare e dissociare i profili utente e i profili di elenco associati all'istanza dell'applicazione IAM Identity Center.
- `AppFlow`— Fornisce l'accesso per creare, aggiornare ed eliminare i profili di connessione; Fornisce l'accesso per creare, aggiornare, eliminare, avviare e interrompere i flussi; Fornisce l'accesso ai tag e rimuove i tag ai flussi e descrive i record di flusso.

- `Amazon S3`— Fornisce l'accesso all'elenco di tutti i bucket. Fornisce GetBucketLocation,, GetBucketPolicy PutObject GetObject, e ListBucket accesso ai bucket con la risorsa arn arn:aws:s3::: -*. aws-supply-chain-data
- `SecretsManager`— Fornisce l'accesso alla creazione di segreti e all'aggiornamento delle politiche segrete.
- `KMS`— Fornisce al AppFlow servizio Amazon l'accesso alle chiavi di elenco e agli alias delle chiavi. Fornisce DescribeKey CreateGrant e ListGrants autorizza le chiavi KMS contrassegnate con key-value aws-suply-chain-access : true; Fornisce l'accesso per creare segreti e aggiornare le politiche segrete.

  Le autorizzazioni (kms:ListKeys, kms:, kms: ListAliases e kms:Decrypt) non sono limitate ad AppFlow Amazon e possono essere concesse a qualsiasi chiave del tuo account. GenerateDataKey AWS KMS

Per visualizzare le autorizzazioni di questa politica, consulta la. AWSSupplyChainFederationAdminAccessAWS Management Console

Aggiornamenti di Catena di approvvigionamento di AWSalle policy gestite da AWS

La tabella seguente elenca i dettagli sugli aggiornamenti alle politiche AWS gestite Catena di approvvigionamento di AWS da quando questo servizio ha iniziato a tenere traccia di queste modifiche. Per gli avvisi automatici sulle modifiche apportate a questa pagina, sottoscrivi il feed RSS nella pagina della cronologia dei documenti di Catena di approvvigionamento di AWS.

Modifica	Description	Data
AWSSupplyChainFederationAdminAccess— Politica aggiornata	Catena di approvvigionamento di AWSha aggiornato la policy gestita per consentire agli utenti federati di accedere alle ListProfileAssociations operazioni in IAM Identity Center.	1 novembre 2023

Modifica	Description	Data
AWSSupplyChainFederationAdminAccess— Politica aggiornata	Catena di approvvigionamento di AWSha aggiornato la politica gestita per consentire agli utenti federati l'accesso PutObject e alle GetObject operazioni sul bucket S3 dedicato con la risorsa arn arn:aws:s3: :aws-supply-chain-data-*.	21 settembre 2023
AWSSupplyChainFederationAdminAccess: nuova policy	Catena di approvvigionamento di AWSha aggiunto una nuova politica per consentire agli utenti federati di accedere all'applicazione. Catena di approvvigionamento di AWS Ciò include le autorizzazioni necessarie per eseguire azioni all'interno dell'Catena di approvvigionamento di AWSapplicazione.	01 marzo 2023
Catena di approvvigionamento di AWS ha iniziato il rilevamento delle modifiche	Catena di approvvigionamento di AWS ha iniziato il rilevamento delle modifiche per le relative policy gestite da AWS.	01 marzo 2023

Convalida della conformità per Catena di approvvigionamento di AWS

Revisori di terze parti valutano la sicurezza e la conformità di Catena di approvvigionamento di AWS come parte di più programmi di conformità di AWS. Questi includono SOC, PCI, FedRAMP, HIPAA e altri.

Per un elenco dei programmi di conformità specifici, consulta AWSServiziServizi AWS che rientrano nell'ambito del programma di conformitàServizi che rientrano nell'ambito del programma di conformitàServizi che rientrano nell'ambito del programma diAWS Per informazioni generali, consulta Programmi per la conformità di AWS.

Puoi scaricare scaricare scaricare scaricare scaricare scaricare scaricare scaricare scaricare scaricareAWS Artifact. Per ulteriori informazioni, consulta Download di report in AWS Artifact.

La tua responsabilità di conformità durante l'utilizzo diCatena di approvvigionamento di AWS è determinata dalla riservatezza dei dati, dagli obiettivi dell'azienda e dalle leggi e normative applicabili. AWSfornisce le seguenti risorse per facilitare la conformità:

- Guide Quick Start su su sicurezza e conformità - Queste guide alla distribuzione illustrano considerazioni relative all'architettura e forniscono procedure per la distribuzione diAWS ambienti di base incentrati sulla sicurezza e sulla conformità.
- Whitepaper sulla progettazione per la sicurezza HIPAA e la conformità: questo whitepaper descrive in che modo le aziende possono utilizzare AWS per creare applicazioni conformi ai requisiti HIPAA.
- Risorse per la conformità AWS: una raccolta di cartelle di lavoro e guide suddivise per settore e area geografica.
- Valutazione delle risorse con le regole nella Guida per gliAWS Config sviluppatori di: questa guida valuta il livello di conformità delle configurazioni delle risorse con pratiche interne, linee guida e regolamenti.
- AWS Security Hub: questoServizio AWS fornisce una visione completa dello stato di sicurezzaAWS all'interno di che consente di verificare la conformità con standard industriali di sicurezza e best practice.

Resilienza in Catena di approvvigionamento di AWS

L'infrastrutturaAWS globale di è basata su zoneRegioni AWS di disponibilità. Regioni AWSfornire più zone di disponibilità fisicamente separate e isolate. Le regioni forniscono reti altamente ridondanti, a bassa latenza e throughput elevato. Con le Zone di disponibilità, è possibile progettare e gestire applicazioni e database che eseguono il failover automatico tra zone di disponibilità senza interruzioni. Le Zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili, rispetto alle infrastrutture a data center singolo o multiplo.

Per ulteriori informazioni sulle Regioni AWS e le zone di disponibilità, consulta Infrastruttura globale di AWS.

Oltre all'infrastruttura globale di AWS, Catena di approvvigionamento di AWS offre numerose funzionalità per supportare la resilienza dei dati e le esigenze di backup.

Registrazione e monitoraggio Catena di approvvigionamento di AWS

La registrazione e il monitoraggio sono una parte importante per mantenere l'affidabilità, la disponibilità e le prestazioni della catena di AWS fornitura e delle altre AWS soluzioni. AWS fornisce lo strumento di AWS CloudTrail monitoraggio per monitorare la catena AWS di fornitura, segnalare quando qualcosa non va e intraprendere azioni automatiche quando necessario.

> **Note**
>
> Le API richiamate solo dalla Catena di approvvigionamento di AWS console vengono acquisite in AWS CloudTrail.

AWS CloudTrail acquisisce le chiamate API e gli eventi correlati effettuati da o per conto del tuo Account AWS e fornisce i file di log a un bucket Simple Storage Service (Amazon S3) specificato. Puoi identificare quali utenti e account hanno richiamato AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute. Puoi visualizzare gli eventi della catena AWS di fornitura su scn.amazonaws.com. Per ulteriori informazioni, consulta la AWS CloudTrail Guida per l'utente.

> **Note**
>
> Tieni presente quanto segue con: Catena di approvvigionamento di AWS
>
> - Quando inviti utenti che non hanno accesso a Catena di approvvigionamento di AWS, questi utenti non ricevono informazioni nelle notifiche che ricevono dall'applicazione web. Gli utenti invitati ricevono una notifica e-mail con un collegamento all'applicazione Web. Possono accedere e visualizzare il contenuto della notifica solo se dispongono delle autorizzazioni utente richieste.
> - Tutti gli utenti con o senza autorizzazioni utente per un particolare Insight possono visualizzare i messaggi di chat di Insights.
> - In qualità di amministratore dell'applicazione, quando aggiungi utenti all' Catena di approvvigionamento di AWS istanza, questi hanno accesso a. AWS KMS key Puoi gestire

le autorizzazioni degli utenti per aggiungere o rimuovere utenti. Per ulteriori informazioni sulle autorizzazioni degli utenti, consulta. Ruoli di autorizzazione utente

Catena di approvvigionamento di AWS eventi relativi ai dati in CloudTrail

Gli eventi di dati forniscono informazioni sulle operazioni delle risorse eseguite su o in una risorsa (ad esempio, lettura o scrittura su un oggetto Amazon S3). Queste operazioni sono definite anche operazioni del piano dei dati. Gli eventi di dati sono spesso attività che interessano volumi elevati di dati. Per impostazione predefinita, CloudTrail non registra gli eventi relativi ai dati. La cronologia CloudTrail degli eventi non registra gli eventi relativi ai dati.

Per gli eventi di dati sono previsti costi aggiuntivi. Per ulteriori informazioni sui CloudTrail prezzi, consulta la sezione AWS CloudTrail Prezzi.

Puoi registrare gli eventi relativi ai dati per i tipi di Catena di approvvigionamento di AWS risorse utilizzando la CloudTrail console o AWS CLI le operazioni CloudTrail dell'API.

- Per registrare gli eventi relativi ai dati utilizzando la CloudTrail console, crea un archivio dati di trail o event per registrare gli eventi relativi ai dati oppure aggiorna un trail o un data store esistente per registrare gli eventi di dati.

  1. Scegli Data events per registrare gli eventi relativi ai dati.
  2. Dall'elenco Tipo di evento Data, scegli il tipo di risorsa per il quale desideri registrare gli eventi relativi ai dati.
  3. Scegli il modello di selettore di registro che desideri utilizzare. Puoi registrare tutti gli eventi relativi ai dati per il tipo di risorsa, registrare tutti `readOnly` gli eventi, registrare tutti `writeOnly` gli eventi o creare un modello di selettore di registro personalizzato per filtrare i `readOnly` campi`eventName`, `eresources.ARN`.
- Per registrare gli eventi relativi ai dati utilizzando il AWS CLI, configura il `--advanced-event-selectors` parametro in modo che il `eventCategory` campo sia uguale `Data` e il `resources.type` campo uguale al valore del tipo di risorsa. È possibile aggiungere condizioni per filtrare i valori dei `resources.ARN` campi `readOnly``eventName`, e.
  - Per configurare un percorso per registrare gli eventi relativi ai dati, esegui il put-event-selectorscomando. Per ulteriori informazioni, vedere Registrazione degli eventi relativi ai dati per i AWS CLI percorsi con.

- Per configurare un Event Data Store per registrare gli eventi di dati, esegui il create-event-data-storecomando per creare un nuovo Event Data Store per registrare gli eventi di dati oppure esegui il update-event-data-storecomando per aggiornare un Event Data Store esistente. Per ulteriori informazioni, vedere Registrazione degli eventi di dati per i data store di eventi con. AWS CLI

*Puoi configurare selettori di eventi avanzati per filtrare `resources.`ARN i campi `eventNamereadOnly`, e per registrare solo gli eventi che ritieni importanti. Per ulteriori informazioni sui campi, consulta AdvancedFieldSelector.

Catena di approvvigionamento di AWS gestione degli eventi in CloudTrail

Gli eventi di gestione forniscono informazioni sulle operazioni di gestione eseguite sulle risorse AWS dell'account. Queste operazioni sono definite anche operazioni del piano di controllo (control-plane). Per impostazione predefinita, CloudTrail registra gli eventi di gestione.

AWS Supply Chain registra tutte le operazioni del piano di controllo CloudTrail come eventi di gestione.

Catena di approvvigionamento di AWS API di applicazioni web

Le API elencate in questa sezione vengono richiamate dalle Catena di approvvigionamento di AWS applicazioni per conto di utenti federati. Queste API non sono visibili nei CloudTrail log e non vengono acquisite nel documento Service Authorization Reference, vedere. Catena di approvvigionamento di AWS L'accesso a queste API è controllato da Catena di approvvigionamento di AWS applicazioni basate sulle autorizzazioni dei ruoli utente federati. Non dovresti cercare di controllare l'accesso a queste API per evitare di interrompere le applicazioni. Catena di approvvigionamento di AWS

Ruoli utente

Le seguenti API vengono utilizzate per gestire utenti, ruoli utente, notifiche utente e messaggi di chat. Catena di approvvigionamento di AWS

```
scn:AddMembersToResourceBasedChat
scn:AssignGalaxyRoleToUser
scn:AssociateUser
scn:BatchGetUsers
scn:BatchMarkNotificationAsDelivered
```

```
scn:CreateRole
scn:DeleteRole
scn:DescribeChatForUser
scn:GetAccessDetailConfig
scn:GetChatPreferencesForUser
scn:GetMessagingSessionConnectionDetails
scn:GetNotificationsPreference
scn:GetOrCreateChimeUser
scn:GetOrCreateResourceBasedChat
scn:GetOrCreateUserBasedChat
scn:GetOrganizationInfo
scn:GetResourceBasedChatArn
scn:GetUserDetails
scn:ListChatMembers
scn:ListChatMessages
scn:ListChatModerators
scn:ListChats
scn:ListRoles
scn:ListUserNotifications
scn:ListUsersWithRole
scn:MarkNotificationAsDelivered
scn:MarkNotificationAsRead
scn:RemoveMemberFromResourceBasedChat
scn:RemoveUser
scn:SearchChimeUsers
scn:SearchUsers
scn:SendChatMessage
scn:SetNotificationsPreference
scn:UpdateChatPreferencesForUser
scn:UpdateChatReadMarker
scn:UpdateOrganizationInfo
scn:UpdateRole
scn:UpdateUser
```

Data lake

Le seguenti API vengono utilizzate per creare e gestire flussi di dati e connessioni nel data lake.

```
scn:CreateConnection
```

```
scn:CreateDataflow
scn:CreateDeleteDataByPartitionJob
scn:CreateExtractFlows
scn:CreatePresignedUrl
scn:CreateSampleParsingJob
scn:CreateSapODataConnection
scn:CreateUpdateDatasetSchemaJob
scn:DeleteConnection
scn:DeleteDataflow
scn:DeleteExtractFlows
scn:DeleteSapODataConnection
scn:describeDatasetGroup
scn:DescribeDataset
scn:DescribeJob
scn:GetConnection
scn:GetCreateExtractFlowsStatus
scn:GetDataflow
scn:ListConnections
scn:ListCustomerFiles
scn:ListDataflows
scn:ListDataflowStats
scn:ListDatasets
scn:UpdateConnection
scn:UpdateDataflow
scn:UpdateExtractFlow
```

Informazioni dettagliate

Le seguenti API vengono utilizzate dall'applicazione Insights per gestire filtri, liste di controllo e visualizzare le modifiche all'inventario.

```
scn:AddModeratorToResourceBasedChat
scn:ComputePostRebalancedQuantities
scn:ComputePostRebalancedQuantitiesV1
scn:CreateInsightFilter
scn:CreateInsightSubscription
scn:DeleteInsightFilter
scn:DeleteInsightSubscription
scn:GetInsightLineItem
```

```
scn:GetInsightSubscription
scn:GetInstanceAttribute
scn:GetInstanceRequiredDatasetAvailabilityStatus
scn:GetKpiData
scn:GetModelEndpointStatus
scn:GetPIVForProduct
scn:GetPIVForSite
scn:GetPIVForSiteAndProduct
scn:GetPIVForSitesAndProducts
scn:GetProducts
scn:GetProductSummaryAggregates
scn:GetSites
scn:GetSiteSummaryAggregates
scn:IsUserAuthorizedForInsightLineItem
scn:ListCustomAttributeValues
scn:ListGeographiesAsGalaxyAdmin
scn:ListInsightFilters
scn:ListInsightLineItems
scn:ListInsightSubscriptions
scn:ListInventoryQuantityAggregates
scn:ListInventoryRisksBySiteAndProduct
scn:ListInventorySummariesBySite
scn:ListPIVProductsBySite
scn:ListProductHierarchiesAsGalaxyAdmin
scn:ListProducts
scn:ListProductsAsGalaxyAdmin
scn:ListSites
scn:ListUsers
scn:PotentiallyComputeThenListRebalancingOptionsForInsightLineItem
scn:RegisterInstanceAttribute
scn:UpdateInsightFilter
scn:UpdateInsightLineItemStatus
scn:UpdateInsightSubscription
scn:UpdateRebalancingOptionStatus
scn:UpdateRebalancingOptionStatusV1
```

Pianificazione della domanda

Le seguenti API vengono utilizzate per creare e gestire previsioni, piani della domanda o cartelle di lavoro. Catena di approvvigionamento di AWS

```
scn:AssociateDatasetWithWorkbook
scn:CreateBaselineForecast
scn:CreateDemandPlan
scn:CreateDemandPlanningCycle
scn:CreateDemandPlanningDatasetExportJob
scn:CreateDerivedForecast
scn:CreateWorkbook
scn:DeleteDemandForecastConfig
scn:DeleteDemandPlanningCycle
scn:DeleteDerivedForecast
scn:DeleteWorkbook
scn:DescribeBaselineForecast
scn:DescribeDemandPlanningCycleAccuracyJob
scn:DescribeDerivedForecast
scn:DescribePlanningCycle
scn:DescribeWorkbook
scn:DisassociatePlanningCycle
scn:GetDemandForecastConfig
scn:GetDemandPlan
scn:GetDemandPlanningCycle
scn:GetDemandPlanningCycleAccuracy
scn:GetDemandPlanningDatasetJob
scn:ListDemandPlans
scn:ListDerivedForecasts
scn:ListForecastingJobs
scn:ListPlanningCycles
scn:ListWorkbooks
scn:PublishDemandPlan
scn:PutDemandForecastConfig
scn:StartDemandPlanningCycleAccuracyJob
scn:StartForecastingJob
scn:UpdateDemandPlan
scn:UpdateDemandPlanningCycleMetadata
scn:UpdateWorkbook
```

Pianificazione dell'offerta

Le seguenti API vengono utilizzate per creare e gestire i piani di approvvigionamento. Catena di approvvigionamento di AWS

```
scn:CreateReplenishmentPipeline
scn:GetReplenishmentPipeline
scn:UpdateReplenishmentPipeline
scn:ListReplenishmentPipelinesByInstance
scn:GetInstanceReplenishmentConfig
scn:CreateBacktest
scn:CreateReplenishmentReviewInstanceConfig
scn:GetReplenishmentReviewInstanceConfig
scn:ListReplenishmentVendors
scn:GetExceptionsSupplyInsightsStatistics
scn:GetPorSupplyInsightsStatistics
scn:GetPlanToPOConversionAnalytics
scn:GetPurchasePlanStatistics
scn:ListPlanExceptions
scn:ListPurchaseOrderRequestLines
scn:UpdatePurchaseOrderRequestLines
scn:ListBomPurchasePlans
scn:ListBomProductionPlans
scn:ListBomTransferPlans
scn:ListBomInsights
scn:ListBomProcesses
scn:ExportBomPlans
scn:GetBomPlanSummary
scn:GetDashboardAnalytics
scn:GetPurchaseOrderRequestExplanation
scn:ListBomSupplyPlan
scn:GetBomPlanRecordDetails
scn:GetBomPlanSummaryAnalytics
scn:ListBomPurchaseOrders
scn:ListBomTransferOrders
scn:ListBomProductionOrders
scn:ExportAllExplodedBoms
scn:ExportBillOfMaterials
scn:ExportInventoryPolicy
scn:ExportProductionProcess
scn:ExportSourcingRule
scn:ExportTransportationLane
scn:ExportVendorLeadTime
scn:ImportBillOfMaterials
scn:ImportInventoryPolicy
scn:ImportProductionProcess
```

```
scn:ImportSourcingRule
scn:ImportTransportationLane
scn:ImportVendorLeadTime
```

Quote per Catena di approvvigionamento di AWS

Hai Account AWS delle quote predefinite, precedentemente denominate limiti, per ciascuno di essi. Servizio AWS Salvo diversa indicazione, ogni quota si applica a una regione specifica. Puoi richiedere di aumentare le quote per le risorse impostate a livello del tuo account. Per ulteriori informazioni sulle quote a livello di account, consulta la tabella seguente.

Per visualizzare le quote per Catena di approvvigionamento di AWS, apri la console Service Quotas. Nel riquadro di navigazione, scegliere Servizi AWS , quindi selezionare Catena di approvvigionamento di AWS.

Per richiedere un aumento delle quote, consultare Richiesta di aumento delle quote nella Guida per l'utente di Service Quotas. Se la quota non è ancora disponibile in Service Quotas, utilizza il modulo di aumento del limite.

La tua Account AWS ha le seguenti quote relative a. Catena di approvvigionamento di AWS

Risorsa	Predefinita	Adattabile
Numero di istanze **Note** Puoi creare fino a 10 istanze all'interno di un account. AWS	10	No
Numero di bucket Amazon S3	100	No
Inviti attivi e in sospeso all'interno di un account AWS	30	Sì
Richieste di dati all'interno di un account AWS	4.000	Sì
Elementi della riga Insights per lista di controllo	1.000	No

Risorsa	Predefinita	Adattabile
Elenchi di controllo di Insights per istanza all'interno di un account AWS	1.000	Sì
Le watchlist di Insights per utente all'interno di un account AWS	100	Sì

Ottenere il supporto amministrativo per Catena di approvvigionamento di AWS

Se in qualità di amministratore hai la necessità di contattare il supporto per Catena di approvvigionamento di AWS, scegli una delle seguenti opzioni:

- Se hai unAWS Support account, vai al Centro Support e invia un ticket.
- Apri AWS Management Consolee scegli AWSSupply Chain, Support, Create case.

È consigliabile fornire le informazioni riportate di seguito:

- L'ID/ARN dell'istanza della catena diAWS fornitura.
- La tuaAWS regione.
- Una descrizione dettagliata del problema.

Cronologia dei documenti per la Catena di approvvigionamento di AWS Administrator Guide

La tabella seguente descrive le versioni della documentazione per Catena di approvvigionamento di AWS.

Modifica	Descrizione	Data
Aggiornamento della politica KMS	È stata aggiornata la politica KMS per consentire l'accesso Catena di approvvigionamento di AWS alla AWS KMS chiave.	18 marzo 2024
PrivateLink supporto	Puoi accedere Catena di approvvigionamento di AWS utilizzando un endpoint di interfaccia (AWS PrivateLink).	26 febbraio 2024
Aggiungere gruppi	Gli utenti devono far parte di un gruppo IAM Identity Center per accedere Catena di approvvigionamento di AWS.	14 novembre 2023
Policy AWS gestita aggiornata	Catena di approvvigionamento di AWS ha aggiornato la policy gestita per consentire agli utenti federati di accedere alle ListProfileAssociations operazioni in IAM Identity Center.	1 novembre 2023
Politica AWS gestita aggiornata	Catena di approvvigionamento di AWS ha aggiornato la policy gestita per consentire agli utenti federati l'accesso alle GetObject operazion i PutObject e sul bucket	21 settembre 2023

	Amazon S3 dedicato con la risorsa arn arn:aws:s3: :aws-supply- chain-data-*.	
Informazioni aggiornate sul supporto delle regioni	Catena di approvvigionamento di AWS La pianificazione della domanda è ora supportat a anche nella regione Asia Pacifico (Sydney).	12 settembre 2023
Usa AWS Console per attivare e disattivare Catena di approvvigionamento di AWS	Catena di approvvigionamento di AWS gli utenti possono ora utilizzare la AWS Console per attivare e disattivare l'utilizzo o Catena di approvvigionamento di AWS l'archiviazione dei tuoi contenuti su AWS Organizat ions.	7 settembre 2023
Informazioni aggiornate sul supporto delle regioni	Catena di approvvigionamento di AWS è ora supportato anche nella regione Asia Pacifico (Sydney) e nella regione Europa (Irlanda).	19 luglio 2023
Informazioni aggiornate su come contattare AWS Support e creare un'istanza	Catena di approvvigionamento di AWS gli utenti possono ora contattare AWS Support per ricevere assistenza e aggiornare i contenuti su come creare un'istanza.	3 aprile 2023

Aggiunta una policy AWS gestita	AWS Supply Chain ha aggiunto una nuova politica per consentire agli utenti federati di accedere all'appli cazione AWS Supply Chain, comprese le autorizzazioni necessarie per eseguire azioni all'interno dell'applicazione AWS Supply Chain.	1 marzo 2023
Versione iniziale	Versione iniziale della Guida per l' Catena di approvvig ionamento di AWS amministr atore.	29 novembre 2022

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.